Phụ lục

ĐỊNH MỨC KINH TẾ - KỸ THUẬT GIÁM SÁT ĐẢM BẢO AN TOÀN THÔNG TIN ĐỐI VỚI HỆ THỐNG HẠ TẦNG KỸ THUẬT DỊCH VỤ CÔNG NGHỆ THÔNG TIN PHỤC VỤ CÔNG TÁC QUẢN LÝ NHÀ NƯỚC THUỘC LĨNH VỰC TÀI NGUYÊN VÀ MÔI TRƯỜNG

(Ban hành kèm theo Quyết định số 7/2026/QĐ-UBND ngày / /2026 của Ủy ban nhân dân thành phố Hà Nội)

Phần I

QUY ĐỊNH CHUNG

1. Cơ sở xây dựng định mức kinh tế - kỹ thuật

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 và Luật số 65/VBHN-VPQH.

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13;

Căn cứ Luật An ninh mạng số 24/2018/QH14;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15;

Căn cứ Nghị định số 204/2004/NĐ-CP ngày 14 tháng 12 năm 2004 của Chính phủ về chế độ tiền lương đối với cán bộ, công chức, viên chức và lực lượng vũ trang;

Căn cứ Nghị định số 117/2016/NĐ-CP ngày 21 tháng 7 năm 2016 của Chính phủ sửa đổi bổ sung một số điều Nghị định số 204/2004/NĐ-CP ngày 14 tháng 12 năm 2004 của Chính phủ về chế độ tiền lương đối với cán bộ, công chức, viên chức và lực lượng vũ trang;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Căn cứ Nghị định số 73/2019/NĐ-CP ngày 05 tháng 9 năm 2019 của Chính phủ về quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước, được sửa đổi, bổ sung bởi Nghị định số 82/2024/NĐ-CP ngày 10 tháng 7 năm 2024.

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông về quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016;

Căn cứ Thông tư số 26/2014/TT-BTNMT ngày 28 tháng 5 năm 2014 của Bộ trưởng Bộ Tài nguyên và Môi trường ban hành Quy trình và Định mức kinh tế - kỹ thuật xây dựng cơ sở dữ liệu tài nguyên và môi trường;

Căn cứ Thông tư số 14/2020/TT-BTNMT ngày 27 tháng 11 năm 2020 của Bộ Tài nguyên và Môi trường ban hành Quy trình và Định mức kinh tế - kỹ thuật xây dựng, duy trì, vận hành hệ thống thông tin ngành tài nguyên và môi trường;

Căn cứ Thông tư số 23/2023/TT-BTC ngày 25/4/2023 của Bộ Tài chính hướng dẫn chế độ quản lý, tính hao mòn, khấu hao tài sản cố định tại cơ quan, tổ chức, đơn vị và tài sản cố định do nhà nước giao cho doanh nghiệp quản lý không tính thành phần vốn nhà nước tại doanh nghiệp;

Căn cứ Nghị quyết số 16/NQ-HĐND ngày 04/7/2023 của HĐND thành phố Hà Nội ban hành Danh mục dịch vụ sự nghiệp công sử dụng ngân sách nhà nước thuộc lĩnh vực tài nguyên và môi trường.

2. Quy định viết tắt

STT	Viết tắt	Tiếng Anh	Giải nghĩa tiếng Việt
1.	ATTT	Information Security	An toàn thông tin
2.	CVE	Common Vulnerabilities and Exposures	Danh mục lỗ hổng bảo mật chuẩn quốc tế
3.	Patch Management	Patch Management	Quản lý bản vá hệ thống
4.	IDS/IPS	Intrusion Detection/Prevention System	Hệ thống phát hiện/ngăn chặn xâm nhập
5.	DoS/DDoS	Denial of Service / Distributed Denial of Service	Tấn công từ chối dịch vụ
6.	Pentest	Penetration Testing	Kiểm thử xâm nhập
7.	SQLi	SQL Injection	Kỹ thuật tấn công chèn lệnh SQL
8.	XSS	Cross-Site Scripting	Kỹ thuật tấn công chèn mã script
9.	RCE	Remote Code Execution	Khai thác thực thi mã từ xa
10.	OWASP Top 10	OWASP Top 10	10 lỗ hổng bảo mật web phổ biến nhất
11.	CWE	Common Weakness Enumeration	Danh mục các điểm yếu phần mềm
12.	AD	Active Directory	Dịch vụ quản lý tài khoản/máy tính của Microsoft
13.	RBAC	Role-Based Access Control	Mô hình phân quyền dựa trên vai trò
14.	UBA	User Behavior Analytics	Phân tích hành vi người dùng
15.	AuthN	Authentication	Xác thực người dùng

STT	Viết tắt	Tiếng Anh	Giải nghĩa tiếng Việt
16.	MFA	Multi-Factor Authentication	Xác thực đa yếu tố
17.	IAM	Identity and Access Management	Quản lý danh tính và quyền truy cập
18.	SIEM	Security Information and Event Management	Hệ thống quản lý sự kiện và thông tin bảo mật
19.	SOAR	Security Orchestration, Automation, and Response	Tự động hóa điều phối và ứng phó sự cố bảo mật
20.	DLP	Data Loss Prevention	Ngăn chặn thất thoát dữ liệu
21.	AV	Anti-Virus	Phần mềm chống virus
22.	EDR	Endpoint Detection & Response	Phát hiện và phản hồi sự cố trên thiết bị đầu cuối
23.	WAF	Web Application Firewall	Tường lửa ứng dụng web
24.	Wazuh	Wazuh	Nền tảng SIEM mã nguồn mở
25.	OSSEC	OSSEC	Hệ thống phát hiện xâm nhập mã nguồn mở
26.	Splunk	Splunk	Công cụ SIEM thương mại
27.	QRadar	IBM QRadar	Giải pháp SIEM của IBM
28.	ELK Stack	Elasticsearch, Logstash, Kibana	Bộ công cụ thu thập và phân tích log
29.	ArcSight	ArcSight	Giải pháp quản lý log và bảo mật
30.	Datadog	Datadog	Nền tảng giám sát và bảo mật hệ thống
31.	OpenVAS	Open Vulnerability Assessment System	Công cụ quét lỗ hổng mã nguồn mở
32.	Nessus	Nessus	Công cụ quét lỗ hổng phổ biến
33.	QualysGuard	QualysGuard	Giải pháp quét lỗ hổng thương mại
34.	Snort	Snort	Hệ thống IDS/IPS mã nguồn mở
35.	Suricata	Suricata	Công cụ IDS/IPS mã nguồn mở
36.	ModSecurity	ModSecurity	Tường lửa ứng dụng web mã nguồn mở
37.	OWASP ZAP	OWASP Zed Attack Proxy	Công cụ kiểm thử bảo mật web miễn phí

STT	Viết tắt	Tiếng Anh	Giải nghĩa tiếng Việt
38.	Burp Suite Pro	Burp Suite Professional	Công cụ pentest ứng dụng web thương mại
39.	SonarQube	SonarQube	Công cụ phân tích mã nguồn và tìm lỗ hổng
40.	Checkmarx	Checkmarx	Giải pháp kiểm tra bảo mật ứng dụng
41.	Veracode	Veracode	Nền tảng kiểm thử bảo mật ứng dụng
42.	pgAudit	PostgreSQL Audit Extension	Công cụ ghi log giám sát CSDL PostgreSQL
43.	MySQL Audit	MySQL Audit Plugin	Công cụ ghi log giám sát MySQL
44.	IBM Guardium	IBM Guardium	Giải pháp bảo mật và giám sát CSDL
45.	Imperva	Imperva	Công cụ bảo mật CSDL thương mại
46.	Bacula	Bacula	Công cụ quản lý sao lưu mã nguồn mở
47.	Amanda	Amanda	Giải pháp sao lưu mã nguồn mở
48.	Veeam	Veeam	Phần mềm sao lưu dữ liệu thương mại
49.	Commvault	Commvault	Giải pháp quản trị sao lưu dữ liệu
50.	Varonis	Varonis	Giải pháp giám sát và bảo mật dữ liệu
51.	Okta	Okta	Giải pháp quản lý danh tính & MFA
52.	Ping Identity	Ping Identity	Nền tảng quản lý truy cập và danh tính
53.	CloudTrail	AWS CloudTrail	Dịch vụ ghi log hoạt động của AWS
54.	Prisma Cloud	Prisma Cloud	Nền tảng bảo mật đa đám mây
55.	ScoutSuite	ScoutSuite	Công cụ kiểm tra cấu hình bảo mật Cloud
56.	Prowler	Prowler	Công cụ kiểm tra cấu hình AWS
57.	ntopng	ntopng	Công cụ phân tích lưu lượng mạng
58.	Zeek (Bro)	Zeek (Bro)	Công cụ phân tích lưu lượng

STT	Viết tắt	Tiếng Anh	Giải nghĩa tiếng Việt
			mạng
59.	Arbor	Arbor Networks	Giải pháp chống DDoS
60.	Darktrace	Darktrace	Nền tảng AI an ninh mạng
61.	RSA Archer	RSA Archer	Giải pháp quản trị rủi ro và tuân thủ
62.	ServiceNow GRC	ServiceNow Governance, Risk, Compliance	Giải pháp quản trị rủi ro, tuân thủ
63.	ISO/IEC 27001	ISO/IEC 27001	Tiêu chuẩn hệ thống quản lý an toàn thông tin
64.	ISO/IEC 27002	ISO/IEC 27002	Hướng dẫn áp dụng kiểm soát ATTT
65.	ISO/IEC 27035	ISO/IEC 27035	Tiêu chuẩn quản lý sự cố an toàn thông tin
66.	ISO/IEC 27017	ISO/IEC 27017	Hướng dẫn bảo mật cho dịch vụ Cloud
67.	ISO/IEC 27018	ISO/IEC 27018	Bảo vệ dữ liệu cá nhân trong môi trường Cloud

3. Giải thích từ ngữ

Trong văn bản này, các từ ngữ dưới đây được hiểu như sau:

a) Hệ thống phần cứng công nghệ thông tin là tập hợp hạ tầng phần cứng vật lý các thiết bị công nghệ thông tin bao gồm:

- Hệ thống máy chủ.

- Hệ thống thiết bị mạng.

- Hệ thống thiết bị lưu trữ, sao lưu dữ liệu.

- Hệ thống cáp mạng.

- Hệ thống thiết bị hội nghị truyền hình.

- Hệ thống thoại IP.

b) Phần mềm hệ thống là phần mềm quản lý điều hành thiết bị phần cứng công nghệ thông tin, các phần mềm phục vụ quản lý người dùng và quản lý các quá trình truy cập của người dùng và các quá trình đòi hỏi cần quản lý trong quá trình khai thác, bao gồm:

- Dịch vụ DNS, WINS, LDAP, Directory, Proxy, Cluster, DHCP, CA, Radius, NMS,... và tương đương.

- Phần mềm quản lý, giám sát mạng.

- Phần mềm dò quét lỗ hổng an ninh mạng, website.

- Phần mềm sao lưu, phục hồi.

- Phần mềm giám sát mạng không dây.

- Phần mềm hỗ trợ người dùng.

- Phần mềm thu thập và phân tích logs.

- Phần mềm tường lửa, phòng chống tấn công mạng, QoS.

- Phần mềm cân bằng tải.

- Phần mềm chống tấn công từ chối dịch vụ.

- Phần mềm quản lý máy chủ ảo hóa.

- Phần mềm mạng riêng ảo VPN.

- Phần mềm xử lý dữ liệu không gian (Arc GIS, MapInfo,…).

- Phần mềm hệ quản trị cơ sở dữ liệu (Oracle, Microsoft SQL Server,…).

- Phần mềm nguồn mở.

PHẦN II
QUY TRÌNH KỸ THUẬT GIÁM SÁT ĐẢM BẢO AN TOÀN THÔNG TIN ĐỐI VỚI HỆ THỐNG HẠ TẦNG KỸ THUẬT DỊCH VỤ CÔNG NGHỆ THÔNG TIN

I. Quy trình giám sát đảm bảo an toàn thông tin cho thiết bị mạng (tường lửa - firewall, IDS/IPS, router, switch)

1. Các bước thực hiện

1.1. Chuẩn bị và thiết lập

- Lập sơ đồ mạng và danh mục thiết bị (CMDB).

- Chuẩn hóa cấu hình log: bật syslog/CEF/JSON, định nghĩa mức log.

- Thiết lập kênh thu tập trung (syslog-ng, rsyslog, Logstash) kết nối với SIEM.

- Thiết lập AAA (TACACS+/RADIUS), tăng cường bảo mật SSH, quản lý mật khẩu/khóa.

1.2. Thu thập và vận hành

- Thu log: ACL hits, VPN, firewall accept/deny, cảnh báo IDS/IPS, thay đổi định tuyến.

- Giám sát hiệu năng thiết bị: CPU, RAM, lỗi cổng mạng, gián đoạn kết nối.

- Giám sát NetFlow/sFlow/IPFIX để phát hiện lưu lượng bất thường.

- Giám sát tuân thủ cấu hình, backup định kỳ, phát hiện thay đổi trái phép.

- Cảnh báo theo ngưỡng và đối chiếu IOC từ nguồn tình báo mối đe dọa.

1.3. Phân tích và tương quan (SIEM/SOC)

- Xây dựng quy tắc tương quan

- Thực hiện phân loại cảnh báo (triage), tìm kiếm mối đe dọa (threat hunting).

1.4. Xác minh và ứng cứu ban đầu

- Xác minh nguồn gốc (MAC, p-rt, VLAN), capture gói tin (pcap).

- Biện pháp ban đầu: chặn IP/ASN, cô lập cổng, thay đổi rule trên firewall.

- Ghi lại chuỗi thời gian sự kiện phục vụ điều tra (f-rensic, IS-/IEC 27035).

1.5. Bảo mật dữ liệu giám sát

- Mã hóa kênh l-g (TLS), lưu vết truy cập.

- Chính sách lưu giữ: l-g chi tiết 90-180 ngày, bản tóm tắt 1-3 năm.

1.6. Đánh giá và cải tiến

- Rà soát quy tắc, chữ ký, ngưỡng hàng tháng/quý.

- Diễn tập ứng cứu (tablet-p, kiểm thử xâm nhập).

2. Sản phẩm

(1). Báo cáo hàng ngày: số lượng cảnh báo, sự kiện quan trọng, thiết bị ngừng hoạt động (theo Mẫu TBM.01).

(2). Báo cáo hàng tuần: mức sử dụng băng thông, tình trạng backup cấu hình (theo Mẫu TBM.02).

(3). Báo cáo sự cố (theo ISO/IEC 27035): chuỗi thời gian, nguyên nhân gốc, biện pháp xử lý (theo Mẫu TBM.03).

(4). Báo cáo hàng tháng: xu hướng tấn công, IOC, baseline lưu lượng (theo Mẫu TBM.04).

(5). Báo cáo tuân thủ cấu hình, audit log (theo Mẫu TBM.05).

(6). Chỉ số đo lường (KPI): thời gian phát hiện (MTTD), thời gian xử lý (MTTR), tỷ lệ cảnh báo sai (false positives), tỷ lệ thiết bị gửi log (theo Mẫu TBM.06).

(Chi tiết tại Phụ lục 1 kèm theo)

II. Quy trình giám sát đảm bảo an toàn thông tin cho hạ tầng ảo hóa (cloud, virtualization)

1. Các bước thực hiện

1.1. Chuẩn bị và thiết lập

- Kiểm kê host, VM, container, tài nguyên đám mây.

- Bật log gốc (AWS CloudTrail, VPC Flow Logs, Azure Monitor, GCP Audit Logs).

- Cấu hình audit log cho API call, snapshot, migration, thay đổi IAM.

- Quét lỗ hổng image, áp dụng chính sách registry.

1.2. Thu thập và giám sát

- Log API: thay đổi quyền, tạo khóa truy cập, thay đổi bucket công khai.

- Giám sát lưu lượng mạng trong nội bộ đám mây (flow logs).

- Giám sát RBAC trong Kubernetes, hoạt động container.

1.3 Phân tích và xử lý

- Tạo IAM key mới + xuất dữ liệu lớn → cảnh báo.

- Vô hiệu hóa key, cô lập namespace, chặn bucket.

1.4 Bảo mật dữ liệu

- Mã hóa log, lưu giữ theo quy định (GDPR, pháp luật Việt Nam).

- Thực hiện quản lý bảo mật đám mây (CSPM).

2. Sản phẩm

(1). Báo cáo hàng ngày: sự kiện truy cập IAM, thay đổi cấu hình cloud, cảnh báo bảo mật container/VM (theo Mẫu AH.01).

(2). Báo cáo hàng tuần: trạng thái tài nguyên cloud (CPU, storage, network), nhật ký audit API, tình trạng backup snapshot (theo Mẫu AH.02).

(3). Báo cáo sự cố: chi tiết sự kiện vi phạm quyền truy cập, rò rỉ dữ liệu, hành vi bất thường trên VM/container, biện pháp khắc phục (theo Mẫu AH.03).

(4). Báo cáo hàng tháng: xu hướng tấn công trên hạ tầng ảo hóa, phân tích sử dụng IAM key, thống kê thay đổi cấu hình và baseline bảo mật (theo Mẫu AH.04).

(5) Báo cáo tuân thủ: đánh giá chính sách bảo mật cloud (CIS Benchmark, ISO/IEC 27017), kiểm tra lưu giữ log và mã hóa dữ liệu (theo Mẫu AH.05).

(6). Chỉ số đo lường (KPI): Thời gian phát hiện và xử lý sự cố (MTTD, MTTR); Tỷ lệ sự kiện bất thường được phân tích tự động (automation rate); Số lượng tài nguyên tuân thủ baseline bảo mật (% compliant); Tỷ lệ VM/container gửi log đầy đủ (theo Mẫu AH.06).

(Chi tiết tại Phụ lục 2 kèm theo)

III. Quy trình giám sát đảm bảo an toàn thông tin cho máy chủ (hệ điều hành windows, linux)

1. Các bước thực hiện

1.1. Chuẩn bị và thiết lập

- Kiểm kê hệ điều hành, phiên bản, bản vá, vai trò.

- Tăng cường bảo mật (hardening) theo chuẩn CIS.

- Bật audit logging: syslog (Linux), Windows Event Forwarding, audit DB.

1.2. Thu thập và giám sát

- Log: đăng nhập thành công/thất bại, sử dụng sudo, lỗi kernel.
- Log DB: truy vấn lỗi, thay đổi cấu trúc, xuất dữ liệu.
- Giám sát CPU, RAM, I/O, số lượng kết nối.

1.3. Phân tích và xác minh

- Tương quan: nhiều lần đăng nhập thất bại trên nhiều server → tấn công ngang.
- Kích hoạt điều tra forensic (memory dump, snapshot).

1.4. Ứng cứu ban đầu

- Cô lập server, vô hiệu hóa tài khoản, thay đổi mật khẩu.
- Tạo snapshot để lưu bằng chứng.

1.5. Bảo mật dữ liệu

- Mã hóa log khi lưu trữ, kiểm soát truy cập.
- Chính sách lưu giữ log.

1.6. Đánh giá định kỳ

Quét lỗ hổng, lập lịch vá lỗi, báo cáo thay đổi cấu hình

2. Sản phẩm

(1). Báo cáo hàng ngày: đăng nhập bất thường, lỗi hệ thống, dịch vụ dừng đột ngột, thay đổi quyền hoặc nhóm người dùng (theo Mẫu HĐH.01).

(2). Báo cáo hàng tuần: tình trạng CPU/RAM/I/O, số lượng kết nối, trạng thái bản vá và dịch vụ quan trọng (theo Mẫu HĐH.02).

(3). Báo cáo sự cố: chi tiết sự kiện xâm nhập, lỗi bảo mật, kết quả forensic (log, memory dump, snapshot), biện pháp khắc phục (theo Mẫu HĐH.03).

(4) Báo cáo hàng tháng: thống kê xu hướng sự cố, mức độ tuân thủ hardening, tỷ lệ máy chủ đã vá đầy đủ, thay đổi cấu hình bảo mật (theo Mẫu HĐH.04).

(5). Báo cáo tuân thủ: đối chiếu chuẩn CIS, NIST, ISO/IEC 27001; kiểm tra chính sách quản lý tài khoản, lưu trữ và mã hóa log (theo Mẫu HĐH.05).

(6). Chỉ số đo lường (KPI): Thời gian phát hiện và xử lý sự cố (MTTD, MTTR); Tỷ lệ máy chủ cập nhật bản vá đúng hạn; Số lượng cảnh báo sai (false positives); Tỷ lệ máy chủ gửi log và tuân thủ baseline bảo mật (theo Mẫu HĐH.06).

(Chi tiết tại Phụ lục 3 kèm theo)

IV. Quy trình giám sát đảm bảo an toàn thông tin cho ứng dụng (web, erp, crm, api, email)

1. Các bước thực hiện

1.1. Chuẩn bị và thiết lập

- Kiểm kê danh mục ứng dụng, phiên bản, môi trường triển khai (dev/test/prod).

- Bật log truy cập, xác thực, lỗi ứng dụng, giao dịch API.

- Cấu hình tường lửa ứng dụng web (WAF), DLP, bảo vệ API gateway.

1.2. Thu thập và giám sát

- Thu thập log request/response, API usage, cảnh báo từ WAF và IDS.

- Giám sát truy cập bất thường, tần suất POST/GET cao, lỗi 4xx/5xx, email spam/phishing.

- Giám sát hành vi giao dịch nghi ngờ (fraud detection, brute force, SQLi, XSS).

1.3. Phân tích và tương quan

- Tương quan WAF block + login thất bại hàng loạt → tấn công brute force.

- Phân tích chuỗi request để phát hiện khai thác API hoặc rò rỉ dữ liệu.

- Kết hợp log ứng dụng và hệ thống xác thực (SSO/AD) để xác minh người dùng.

1.4. Ứng cứu ban đầu

- Giới hạn tốc độ, tạm khóa tài khoản, reset mật khẩu.

- Vá nóng (hotfix), cập nhật chữ ký WAF, chặn IP/ASN tấn công.

- Thông báo sự cố và ghi nhận bằng chứng phục vụ điều tra.

1.5. Bảo mật dữ liệu log

- Che giấu hoặc ẩn danh dữ liệu cá nhân (PII) trong log.

- Mã hóa log khi lưu trữ, kiểm soát quyền truy cập và chính sách lưu giữ.

1.6. Đánh giá và cải tiến

- Kiểm thử xâm nhập định kỳ, rà soát quy tắc WAF và API policy.

- Cập nhật baseline an toàn ứng dụng và đào tạo đội ngũ vận hành.

2. Sản phẩm

(1). Báo cáo hàng ngày: số lượng truy cập, lỗi ứng dụng, cảnh báo WAF/API, đăng nhập bất thường (theo Mẫu UD.01).

(2). Báo cáo hàng tuần: trạng thái hoạt động ứng dụng, hiệu suất API, tỷ lệ lỗi và phản hồi chậm (theo Mẫu UD.02).

(3). Báo cáo sự cố: chi tiết khai thác lỗ hổng, tấn công brute force, phishing, rò rỉ dữ liệu; biện pháp xử lý (theo Mẫu UD.03).

(4). Báo cáo hàng tháng: thống kê xu hướng tấn công, hiệu quả quy tắc WAF, tỷ lệ giao dịch nghi ngờ, đánh giá bảo mật API (theo Mẫu UD.04).

(5). Báo cáo tuân thủ: đối chiếu OWASP Top 10, ISO/IEC 27034, GDPR (nếu có), kiểm tra chính sách PII và mã hóa log (theo Mẫu UD.05).

(6). Chỉ số đo lường (KPI): MTTD/MTTR (thời gian phát hiện và khắc phục); Số lượng lỗ hổng được vá đúng hạn; Tỷ lệ cảnh báo đúng (true positives); Tỷ lệ log ứng dụng được thu thập và phân tích đầy đủ (theo Mẫu UD.06).

(Chi tiết tại Phụ lục 4 kèm theo)

V. Quy trình giám sát đảm bảo an toàn thông tin cho cơ sở dữ liệu

1. Các bước thực hiện

1.1. Chuẩn bị và thiết lập

- Kiểm kê hệ quản trị cơ sở dữ liệu (DBMS), phiên bản, vai trò, và người quản trị.

- Bật audit log, query log, slow query log.

- Cấu hình giám sát kết nối, phân quyền, thay đổi cấu trúc bảng/lược đồ.

- Áp dụng hardening theo chuẩn CIS/OWASP Database Security.

1.2. Thu thập và giám sát

- Thu thập log truy cập, đăng nhập, truy vấn lỗi, hành vi thao tác dữ liệu (INSERT/UPDATE/DELETE).

- Giám sát thay đổi quyền truy cập, tạo tài khoản mới, hoặc cấp quyền DBA.

- Theo dõi hiệu năng DB: CPU, I/O, deadlock, kết nối bất thường.

- Giám sát backup/restore, lịch trình và trạng thái sao lưu.

1.3. Phân tích và tương quan

- Tương quan các hành vi bất thường: DROP table + đăng nhập ngoài giờ + truy cập từ IP lạ.

- Phát hiện truy vấn khối lượng lớn hoặc quét dữ liệu nhạy cảm (data exfiltration).

- Đối chiếu nhật ký DB với log ứng dụng và hệ điều hành để xác minh hành vi.

1.4. Ứng cứu ban đầu

- Cô lập tài khoản nghi ngờ, thu hồi quyền truy cập, khóa session đang hoạt động.

- Khôi phục dữ liệu từ bản sao lưu, ghi nhận log phục vụ điều tra.

- Vá lỗi hoặc điều chỉnh cấu hình bảo mật (role, GRANT/REVOKE).

1.5. Bảo mật dữ liệu và log

- Mã hóa dữ liệu nhạy cảm (at rest, in transit), ẩn danh dữ liệu khi test.

- Mã hóa log, kiểm soát quyền truy cập, lưu trữ an toàn và tuân thủ chính sách retention.

1.6. Đánh giá và cải tiến

- Rà soát quyền tài khoản, kiểm tra chính sách backup và mã hóa định kỳ.

- Kiểm thử xâm nhập database, cập nhật baseline bảo mật.

2. Sản phẩm

(1). Báo cáo hàng ngày: đăng nhập bất thường, truy vấn lỗi, thay đổi cấu trúc hoặc quyền truy cập (theo Mẫu CSDL.01).

(2). Báo cáo hàng tuần: tình trạng hiệu năng DB, lịch backup/restore, log audit (theo Mẫu CSDL.02).

(3). Báo cáo sự cố: chi tiết truy vấn phá hoại (DROP/DELETE), rò rỉ dữ liệu, biện pháp khôi phục (theo Mẫu CSDL.03).

(4). Báo cáo hàng tháng: xu hướng truy cập, thay đổi quyền, thống kê hiệu năng, kiểm tra tuân thủ chính sách lưu trữ (theo Mẫu CSDL.04).

(5). Báo cáo tuân thủ: đối chiếu chuẩn bảo mật cơ sở dữ liệu (CIS Benchmark, ISO/IEC 27001, PCI DSS), đánh giá trạng thái mã hóa và quản lý quyền (theo Mẫu CSDL.05).

(6). Chỉ số đo lường (KPI): Thời gian phát hiện và xử lý sự cố (MTTD, MTTR); Tỷ lệ backup thành công và khôi phục thử nghiệm; Tỷ lệ phát hiện truy vấn bất thường; Tỷ lệ cơ sở dữ liệu tuân thủ baseline bảo mật và mã hóa (theo Mẫu CSDL.06).

(Chi tiết tại Phụ lục 5 kèm theo)

VI. Quy trình giám sát đảm bảo an toàn thông tin cho người dùng

1. Các bước thực hiện

1.1. Chuẩn bị và thiết lập

- Kiểm kê danh sách tài khoản người dùng, vai trò, nhóm, và các đặc quyền.

- Thiết lập hệ thống quản lý danh tính và truy cập (IAM) và bật audit log cho các sự kiện xác thực (Active Directory/SSO).

- Cấu hình giám sát truy cập từ xa (VPN, VDI) và các dịch vụ chia sẻ tài nguyên.

- Áp dụng chính sách mật khẩu và xác thực đa yếu tố (MFA).

1.2. Thu thập và giám sát

- Thu thập log đăng nhập/đăng xuất thành công/thất bại, thay đổi mật khẩu, thay đổi vai trò.

- Giám sát đăng nhập bất thường (từ IP lạ, ngoài giờ hành chính, tốc độ di chuyển không thể lý giải).

- Giám sát hành vi người dùng đặc quyền (Admin, Root, DBA) trong việc truy cập tài nguyên.

- Thu thập log truy cập vào dữ liệu nhạy cảm (qua DLP, file share audit).

1.3. Phân tích và tương quan

- Xây dựng baseline hành vi cho từng nhóm người dùng (giờ làm việc, tài nguyên truy cập, khối lượng download/upload).

- Tương quan đăng nhập thành công bất thường + truy cập tệp nhạy cảm + download khối lượng lớn → rò rỉ dữ liệu nội bộ.

- Phân tích chuỗi sự kiện để phát hiện tấn công chiếm quyền tài khoản (account takeover).

1.4. Ứng cứu ban đầu

- Vô hiệu hóa hoặc tạm khóa tài khoản bị chiếm quyền.

- Buộc đăng xuất (force logoff) và reset mật khẩu cho người dùng.

- Cô lập thiết bị đầu cuối của người dùng có hành vi bất thường.

- Thông báo và phối hợp với phòng ban nhân sự/quản lý để xác minh.

1.5. Bảo mật dữ liệu và log

- Đảm bảo log xác thực được mã hóa và lưu trữ an toàn, tách biệt khỏi log hệ thống.

- Tuân thủ chính sách lưu giữ log theo quy định pháp luật.

- Thực hiện ẩn danh (anonymization) hoặc che giấu (masking) thông tin nhận dạng cá nhân (PII) trong log.

1.6. Đánh giá và cải tiến

- Rà soát định kỳ các tài khoản không hoạt động (idle accounts) và đặc quyền.

- Thực hiện các chiến dịch kiểm tra phishing và đào tạo nhận thức bảo mật cho người dùng.

- Cập nhật baseline hành vi UEBA dựa trên các sự cố đã xảy ra.

2. Sản phẩm

(1). Báo cáo hàng ngày: Đăng nhập bất thường (khác vị trí, ngoài giờ), thất bại đăng nhập/MFA liên tục, thay đổi mật khẩu/đặc quyền người dùng (theo Mẫu USER.01).

(2). Báo cáo hàng tuần: Thống kê hành vi người dùng đặc quyền, tổng hợp truy cập dữ liệu nhạy cảm, trạng thái xác thực MFA/SSO, tài khoản không hoạt động (theo Mẫu USER.02).

(3). Báo cáo sự cố: Chi tiết sự kiện chiếm quyền tài khoản, vi phạm chính sách truy cập, rò rỉ dữ liệu nội bộ do người dùng; biện pháp khắc phục (theo Mẫu USER.03).

(4). Báo cáo hàng tháng: Xu hướng hành vi bất thường (UEBA), đánh giá tài khoản đặc quyền, thống kê kết quả kiểm tra phishing, rà soát tài khoản không hoạt động (theo Mẫu USER.04).

(5). Báo cáo tuân thủ: Đối chiếu chính sách IAM với ISO/IEC 27001 (A.9, A.11), NIST CSF; kiểm tra việc áp dụng MFA, và chính sách quản lý mật khẩu (theo Mẫu USER.05).

(6). Chỉ số đo lường (KPI): Thời gian phát hiện và xử lý sự cố (MTTD, MTTR); Tỷ lệ tài khoản có MFA; Tỷ lệ người dùng vi phạm chính sách mật khẩu; Tỷ lệ hành vi bất thường được UEBA phát hiện chính xác (theo Mẫu USER.06).

(Chi tiết tại Phụ lục 6 kèm theo)

VII. Quy trình giám sát đảm bảo an toàn thông tin cho toàn bộ hệ thống (SOC - Trung tâm điều hành an ninh mạng)

1. Các bước thực hiện

1.1. Chuẩn bị và thiết lập

- Triển khai và cấu hình hệ thống SIEM/SOAR, tích hợp log từ các nguồn: mạng, máy chủ, ứng dụng, cơ sở dữ liệu, endpoint, cloud.

- Xây dựng thư viện tình huống (use-case library) theo mô hình MITRE ATT&CK.

- Xác định ngưỡng cảnh báo, mức độ ưu tiên (severity), quy trình phân quyền xử lý.

1.2. Giám sát và phân tích

- Giám sát liên tục 24/7 các sự kiện an ninh trên toàn hệ thống.

- Thực hiện phân loại (triage), làm giàu dữ liệu (enrichment), tương quan cảnh báo (correlation).

- Phát hiện hành vi tấn công (brute force, phishing, privilege escalation, lateral movement).

1.3. Ứng cứu và xử lý sự cố

- Thực hiện playbook phản ứng: DDoS, ransomware, khai thác lỗ hổng, lạm dụng đặc quyền.

- Kích hoạt quy trình escalation đến đội chuyên trách, cô lập hệ thống hoặc tài khoản nghi ngờ.

- Ghi nhận và lưu trữ toàn bộ chuỗi sự kiện phục vụ điều tra.

1.4. Săn tìm mối đe dọa

- Phân tích hành vi ẩn, IOC, log lịch sử để phát hiện tấn công chưa được cảnh báo.

- Sử dụng nguồn threat intelligence nội bộ và bên thứ ba (MISP, VirusTotal, AlienVault OTX).

- Cập nhật danh sách IOC, YARA rule, pattern nhận diện tấn công mới.

1.5. Rà soát và cải tiến

- Thực hiện đánh giá sau sự cố (post-incident review), cập nhật quy tắc SIEM và playbook.

- Đánh giá năng lực phản ứng của đội SOC, đề xuất đào tạo và nâng cấp công cụ.

- Báo cáo định kỳ kết quả vận hành và cải thiện khả năng phát hiện.

2. Sản phẩm

(1). Báo cáo hàng ngày: số lượng cảnh báo, sự kiện nghi ngờ, tình trạng thiết bị/nguồn log, hành vi đáng chú ý (theo Mẫu SOC.01).

(2). Báo cáo hàng tuần: thống kê mức độ cảnh báo, top 10 mối đe dọa, hiệu quả quy tắc phát hiện, tình trạng phản ứng sự cố (theo Mẫu SOC.02).

(3). Báo cáo sự cố: chi tiết chuỗi sự kiện, phân tích nguyên nhân gốc (root cause), tác động và biện pháp khắc phục theo ISO/IEC 27035 (theo Mẫu SOC.03).

(4). Báo cáo hàng tháng: xu hướng tấn công, thống kê IOC, hiệu quả threat hunting, tỷ lệ cảnh báo chính xác (theo Mẫu SOC.04).

(5) Báo cáo tuân thủ: đối chiếu tiêu chuẩn vận hành SOC (ISO/IEC 27035, NIST 800-61, MITRE ATT&CK), kiểm tra đầy đủ nguồn log (theo Mẫu SOC.05).

(6). Chỉ số đo lường (KPI): MTTD, MTTR (thời gian phát hiện và xử lý); Tỷ lệ cảnh báo chính xác (true positive rate); Số lượng sự cố được phát hiện chủ động qua threat hunting; Tỷ lệ hệ thống/thiết bị gửi log đầy đủ về SIEM (theo Mẫu SOC.06).

(Chi tiết tại Phụ lục 7 kèm theo)

PHẦN III
ĐỊNH MỨC KINH TẾ - KỸ THUẬT GIÁM SÁT ĐẢM BẢO AN TOÀN THÔNG TIN ĐỐI VỚI HỆ THỐNG HẠ TẦNG KỸ THUẬT DỊCH VỤ CÔNG NGHỆ THÔNG TIN

CHƯƠNG I
GIÁM SÁT ĐẢM BẢO AN TOÀN THÔNG TIN CHO THIẾT BỊ MẠNG (TƯỜNG LỬA - FIREWALL, IDS/IPS, ROUTER, SWITCH)

I. Chuẩn bị và thiết lập

1. Định mức lao động

1.1. Nội dung công việc

a) Lập sơ đồ mạng và danh mục thiết bị (CMDB).

b) Chuẩn hóa cấu hình log: bật syslog/CEF/JSON, định nghĩa mức log.

c) Thiết lập kênh thu tập trung (syslog-ng, rsyslog, Logstash) kết nối với SIEM.

d) Thiết lập AAA (TACACS+/RADIUS), tăng cường bảo mật SSH, quản lý mật khẩu/khóa.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Giải thích	Điểm tối đa	Quy tắc tính điểm
1	Số lượng thiết bị/host cần giám sát (m)	Tổng số thiết bị mạng, máy chủ, endpoint phải thu log	40	$m \leq 50 \rightarrow 10$ $50 < m \leq 200 \rightarrow 25$ $m > 200 \rightarrow 40$
2	Số lượng hệ thống log/ứng dụng khác loại	Độ đa dạng nguồn log (Firewall, Web, DB, AD, Cloud...)	15	≤3 loại → 5 4-6 loại → 10 >6 loại → 15
3	Mức độ phức tạp cấu trúc mạng	Số vùng mạng (LAN, DMZ, Cloud, VPN, OT…)	30	≤3 vùng → 10 4-6 vùng → 20 > 6 vùng → 30
4	Yêu cầu tuân thủ và tiêu chuẩn bảo mật	Có yêu cầu ISO 27001, NIST, hay quy định chuyên ngành	15	Không yêu cầu → 0 Yêu cầu nội bộ → 10 Yêu cầu theo chuẩn quốc tế → 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm	Ký hiệu
1	Dễ	$K \leq 50$	KK1
2	Trung bình	$50 < K < 80$	KK2
3	Khó	$K \geq 80$	KK3

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Lập sơ đồ mạng và danh mục thiết bị (CMDB)		2		2
2	Chuẩn hóa cấu hình log (syslog/CEF/JSON, định nghĩa mức log)		1	1	2
3	Thiết lập kênh thu tập trung (syslog-ng, rsyslog, Logstash, SIEM)		1	1	2
4	Thiết lập AAA (TACACS+/RADIUS), bảo mật SSH, quản lý mật khẩu/khóa	1	1		2

1.4. Định mức

Công nhóm/ĐVT

STT	Danh mục công việc	Đơn vị tính	KK1	KK2	KK3
`	Lập sơ đồ mạng và danh mục thiết bị (CMDB)	Hệ thống	1,8	2,3	3,1
2	Chuẩn hóa cấu hình log (syslog/CEF/JSON, định nghĩa mức log)	Thiết bị	2,5	3,2	4,1
3	Thiết lập kênh thu tập trung (syslog-ng, rsyslog, Logstash)	Nguồn log	3,0	3,8	5,0
4	Thiết lập AAA, bảo mật SSH, quản lý mật khẩu/khóa	Thiết bị	2,0	2,6	3,4

2. Định mức thiết bị

Ca/01 hệ thống

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Lập sơ đồ mạng và danh mục thiết bị (CMDB)	Chuẩn hóa cấu hình log (syslog/CEF/JSON, định nghĩa mức log)	Thiết lập kênh thu tập trung (syslog-ng, rsyslog, Logstash)	Thiết lập AAA, bảo mật SSH, quản lý mật khẩu/khóa
1	Máy tính để bàn	Bộ	60	4,027	4,027	24,160	24,160
2	Máy in laser	Cái	60	-	-		
3	Điều hoà nhiệt độ	Cái	96	0,705	0,705	4,228	4,228
4	Máy photocopy	Cái	96	-	-	-	-
5	Điện năng (kw)	kW		15,644	15,644	93,862	93,862

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 hệ thống

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Lập sơ đồ mạng và danh mục thiết bị (CMDB)	Chuẩn hóa cấu hình log (syslog/CEF/JSON, định nghĩa mức log)	Thiết lập kênh thu tập trung (syslog-ng, rsyslog, Logstash)	Thiết lập AAA, bảo mật SSH, quản lý mật khẩu/khóa
1	Ghế	Cái	96	5,033	5,033	30,200	30,200
2	Bàn làm việc	Cái	96	5,033	5,033	30,200	30,200
3	Quạt trần 0,1 kW	Cái	60	0,881	0,881	5,285	5,285
4	Đèn neon 0,04 kW	Bộ	36	2,517	2,517	15,100	15,100
5	Điện năng (kw)	kW		1,586	1,586	9,513	9,513

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Lập sơ đồ mạng và danh mục thiết bị (CMDB)	Chuẩn hóa cấu hình log (syslog/CEF/JSON, định nghĩa mức log)	Thiết lập kênh thu tập trung (syslog-ng, rsyslog, Logstash)	Thiết lập AAA, bảo mật SSH, quản lý mật khẩu/khóa
1	Giấy in A4	Gram	-	-	-	-
2	Mực in laser	Hộp	-	-	-	-
3	Mực máy photocopy	Hộp	-	-	-	-
4	Cặp để tài liệu	Cái	-	-	-	-

II. Thu thập và vận hành

1. Định mức lao động

1.1. Nội dung công việc

a) Thu log: ACL hits, VPN, firewall accept/deny, cảnh báo IDS/IPS, thay đổi định tuyến.

b) Giám sát hiệu năng thiết bị: CPU, RAM, lỗi cổng mạng, gián đoạn kết nối.

c) Giám sát NetFlow/sFlow/IPFIX để phát hiện lưu lượng bất thường.

d) Giám sát tuân thủ cấu hình, backup định kỳ, phát hiện thay đổi trái phép.

đ) Cảnh báo theo ngưỡng và đối chiếu IOC từ nguồn tình báo mối đe dọa.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Giải thích	Điểm tối đa	Quy tắc tính điểm
1	Số lượng thiết bị/nguồn log cần giám sát (m)	Tổng số firewall, router, switch, server, ứng dụng, endpoint gửi log	40	$m \leq 100 \rightarrow 10$ $100 < m \leq 300 \rightarrow 25$ $m > 300 \rightarrow 40$
2	Tốc độ tạo log trung bình (log/s)	Lưu lượng log ảnh hưởng trực tiếp đến công suất thu thập & xử lý	15	≤1.000 log/s → 5 1.000-10.000 → 10 >10.000 → 15
3	Độ phức tạp cảnh báo & phân loại sự kiện	Số rule/alert, mức độ liên kết, tương quan IOC	30	≤200 rule → 10 200-500 → 20 >500 → 30
4	Yêu cầu trực giám & thời gian phản ứng (SLA)	Có SOC 24/7, yêu cầu phản ứng nhanh hoặc định kỳ	15	Ca hành chính → 5 2 ca/ngày → 10 24/7 → 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm	Ký hiệu
1	Dễ	$K \leq 50$	KK1
2	Trung bình	$50 < K < 80$	KK2
3	Khó	$K \geq 80$	KK3

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Thu log: ACL hits, VPN, firewall accept/ deny, cảnh báo IDS/IPS, thay đổi định tuyến		2		2
2	Giám sát hiệu năng thiết bị: CPU, RAM, lỗi cổng mạng, gián đoạn kết nối		1	1	2
3	Giám sát NetFlow/sFlow/IPFIX để phát hiện lưu lượng bất thường		1	1	2
4	Giám sát tuân thủ cấu hình, backup định kỳ, phát hiện thay đổi trái phép		1	1	2
5	Cảnh báo theo ngưỡng và đối chiếu IOC từ nguồn tình báo mối đe dọa	1	1		2

1.4. Định mức

STT	Danh mục công việc	Đơn vị tính	KK1	KK2	KK3
1	Thu log: ACL hits, VPN, firewall accept/ deny, IDS/IPS alert, thay đổi định tuyến	Nguồn log	1,8	2,3	3,0
2	Giám sát hiệu năng thiết bị: CPU, RAM, lỗi cổng, gián đoạn kết nối	Thiết bị	2,4	3,0	3,9
3	Giám sát NetFlow/sFlow/IPFIX, phát hiện lưu lượng bất thường	Hệ thống	3,2	4,0	5,3
4	Giám sát tuân thủ cấu hình, backup, phát hiện thay đổi trái phép	Thiết bị	2,2	2,8	3,6
5	Cảnh báo theo ngưỡng và đối chiếu IOC từ nguồn tình báo mối đe dọa	Nguồn log	3,0	3,8	5,0

2. Định mức thiết bị

Ca/01 thiết bị

STT	Thiết bị	ĐVT	Công suất (Kw)	Thu log: ACL hits, VPN, firewall accept/deny, IDS/IPS alert, thay đổi định tuyến	Giám sát hiệu năng thiết bị: CPU, RAM, lỗi cổng, gián đoạn kết nối	Giám sát NetFlow/ sFlow/IP FIX, phát hiện lưu lượng bất thường	Giám sát tuân thủ cấu hình, backup, phát hiện thay đổi trái phép	Cảnh báo theo ngưỡng và đối chiếu IOC từ nguồn tình báo mối đe dọa
1	Máy tính để bàn	Cái	0,4	0,033	0,067	0,067	0,2	0,1
2	Máy in laser	Cái	0,6	0	0	0	0	0
3	Điều hoà nhiệt độ	Cái	2,2	0,006	0,011	0,011	0,034	0,017
4	Điện năng	Kw		0,215	0,43	0,43	1,291	0,646

3. Định mức dụng cụ

Ca/01 thiết bị

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Thu log: ACL hits, VPN, firewall accept/deny, IDS/IPS alert, thay đổi định tuyến	Giám sát hiệu năng thiết bị: CPU, RAM, lỗi cổng, gián đoạn kết nối	Giám sát NetFlow/ sFlow/IP FIX, phát hiện lưu lượng bất thường	Giám sát tuân thủ cấu hình, backup, phát hiện thay đổi trái phép	Cảnh báo theo ngưỡng và đối chiếu IOC từ nguồn tình báo mối đe dọa
1	Ghế	Cái	96	0,067	0,2	0,1	0,2	0,4
2	Bàn làm việc	Cái	96	0,067	0,2	0,1	0,2	0,4
3	Quạt trần	Cái	96	0,012	0,035	0,018	0,035	0,07
4	Đèn neon	Bộ	24	0,033	0,1	0,05	0,1	0,2
5	Điện năng	kW		0,021	0,063	0,031	0,063	0,126
6	Đồng hồ đo điện vạn năng	Cái	60	0	0	0	0	0
7	Máy hút bụi	Cái	60	0	0	0	0	0

4. Định mức vật liệu

STT	Nội dung	ĐVT	Thu log: ACL hits, VPN, firewall accept/deny, IDS/IPS alert, thay đổi định tuyến	Giám sát hiệu năng thiết bị: CPU, RAM, lỗi cổng, gián đoạn kết nối	Giám sát NetFlow/sFlow/IPFIX, phát hiện lưu lượng bất thường	Giám sát tuân thủ cấu hình, backup, phát hiện thay đổi trái phép	Cảnh báo theo ngưỡng và đối chiếu IOC từ nguồn tình báo mối đe dọa
1	Giấy in A4	Gram	-	-	-	0,01	0,01
2	Mực in laser	Hộp	-	-	-	0,002	0,002

III. Phân tích & tương quan (SIEM/SOC)

1. Định mức lao động

1.1. Nội dung công việc

a) Xây dựng quy tắc tương quan.

b) Thực hiện phân loại cảnh báo (triage), săn tìm mối đe dọa (threat hunting).

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Giải thích	Điểm tối đa	Quy tắc tính điểm
1	Số lượng nguồn log/hệ thống đầu vào (m)	Số lượng nguồn dữ liệu được đưa vào SIEM để tương quan	40	m ≤ 50 → 10 50 < m ≤ 200 → 25m > 200 → 40
2	Số lượng quy tắc tương quan cần xây dựng /bảo trì	Mức độ đa dạng và phức tạp của rule	15	≤50 rule → 5 50-150 → 10 >150 → 15
3	Độ phức tạp mô hình tấn công và phân tích hành vi	Cần mô hình hóa chuỗi hành vi (kill chain), mapping MITRE ATT&CK	30	Chỉ theo signature đơn → 10 Có mapping MITRE → 20 Có hành vi đa tầng (multi-step correlation) → 30
4	Nguồn dữ liệu threat intelligence và IOC tích hợp	Số lượng nguồn và mức độ cập nhật	15	Không có → 0 1-2 nguồn → 10 ≥3 nguồn tự động cập nhật → 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm	Ký hiệu
1	Dễ	K ≤ 50	KK1
2	Trung bình	50 < K < 80	KK2
3	Khó	K ≥ 80	KK3

1.3. Định biên

STT	Danh mục công việc	KS3	KS4	Nhóm
1	Xây dựng quy tắc tương quan	1	1	2
2	Thực hiện phân loại cảnh báo (triage), săn tìm mối đe dọa (threat hunting)	1	1	2

1.4. Định mức

STT	Danh mục công việc	Đơn vị tính	KK1	KK2	KK3
1	Xây dựng quy tắc tương quan	Rule	2,0	2,8	3,8
2	Thực hiện phân loại cảnh báo (triage), săn tìm mối đe dọa (threat hunting)	Phiên làm việc	3,0	3,9	5,2

2. Định mức thiết bị

Ca/01 Phiên làm việc

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Xây dựng quy tắc tương quan	Thực hiện phân loại cảnh báo (triage), săn tìm mối đe dọa (threat hunting)
1	Máy tính để bàn	Bộ	60	0,080	0,160
2	Máy in laser	Cái	60	0,002	
3	Điều hoà nhiệt độ	Cái	96	0,014	0,028
4	Điện năng (kw)	kW		0,313	0,622

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 Phiên làm việc

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Xây dựng quy tắc tương quan	Thực hiện phân loại cảnh báo (triage), săn tìm mối đe dọa (threat hunting)
1	Ghế	Cái	96	0,100	0,200
2	Bàn làm việc	Cái	96	0,100	0,200
3	Quạt trần 0,1 kW	Cái	60	0,018	0,035
4	Đèn neon 0,04 kW	Bộ	36	0,050	0,100
5	Điện năng (kw)	kW		0,032	0,063

Ghi chú: Mức dụng cụ trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Xây dựng quy tắc tương quan	Thực hiện phân loại cảnh báo (triage), săn tìm mối đe dọa (threat hunting)
1	Giấy in A4	Gram	-	0,0040
2	Mực in laser	Hộp	-	0,0011
3	Cặp để tài liệu	Cái	-	0,0040

IV. Xác minh & ứng cứu ban đầu

1. Định mức lao động

1.1. Nội dung công việc

a) Xác minh nguồn gốc (MAC, port, VLAN), capture gói tin (pcap).

b) Biện pháp ban đầu: chặn IP/ASN, cô lập cổng, thay đổi rule trên firewall.

c) Ghi lại chuỗi thời gian sự kiện phục vụ điều tra (forensic, ISO/IEC 27035).

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng thiết bị mạng trong phạm vi giám sát và xử lý sự cố	40	≤10: 10	10–50: 25	>50: 40
2	Mức độ phân tán hệ thống mạng (site, VLAN, DMZ, chi nhánh)	20	1 site hoặc VLAN: 5	2–3 site hoặc VLAN: 10	Nhiều vùng mạng, DMZ hoặc kết nối liên vùng: 20
3	Mức độ phức tạp trong cấu hình và chính sách bảo mật	25	Cấu hình đơn giản, rule ít: 5	Có nhiều rule, ACL trung bình: 15	ACL/NAT phức tạp, nhiều rule và nhóm chính sách: 25
4	Mức độ hỗ trợ công cụ giám sát và quản lý tập trung	15	Có SIEM/NMS tích hợp: 5	Có syslog nhưng không đồng bộ: 10	Không có quản lý tập trung, thao tác thủ công: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Xác minh nguồn gốc (MAC, port, VLAN), capture gói tin (pcap)	1	1		2

2	Biện pháp ban đầu: chặn IP/ASN, cô lập cổng, thay đổi rule trên firewall		2	1	3
3	Ghi lại chuỗi thời gian sự kiện phục vụ điều tra (forensic, ISO/IEC 27035)		1	1	2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Xác minh nguồn gốc (MAC, port, VLAN), capture gói tin (pcap)	Sự cố	1,4	1,9	2,6
2	Biện pháp ban đầu: chặn IP/ASN, cô lập cổng, thay đổi rule trên firewall	Sự cố	1,8	2,6	3,5
3	Ghi lại chuỗi thời gian sự kiện phục vụ điều tra (forensic, ISO/IEC 27035)	Sự cố	1,5	2,2	3,1

2. Định mức thiết bị

Ca/01 sự cố

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Xác minh nguồn gốc (MAC, port, VLAN), capture gói tin (pcap)	Biện pháp ban đầu: chặn IP/ASN, cô lập cổng, thay đổi rule firewall	Ghi lại chuỗi thời gian sự kiện (forensic, ISO/IEC 27035)
1	Máy tính để bàn	Bộ	60	0,480	2,880	0,240
2	Máy in laser	Cái	60			
3	Điều hoà nhiệt độ	Cái	96	0,084	0,504	0,042
4	Máy photocopy	Cái	96	-	-	-
5	Điện năng (kw)	kW		1,865	11,189	0,932

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 sự cố

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Xác minh nguồn gốc (MAC, port, VLAN), capture gói tin (pcap)	Biện pháp ban đầu: chặn IP/ASN, cô lập cổng, thay đổi rule firewall	Ghi lại chuỗi thời gian sự kiện (forensic, ISO/IEC 27035)
1	Ghế	Cái	96	0,600	3,600	0,300
2	Bàn làm việc	Cái	96	0,600	3,600	0,300
3	Quạt trần 0,1 kW	Cái	60	0,105	0,630	0,053
4	Đèn neon 0,04 kW	Bộ	36	0,300	1,800	0,150
5	Điện năng (kw)	kW		0,189	1,134	0,095

Ghi chú: Mức dụng cụ trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Xác minh nguồn gốc (MAC, port, VLAN), capture gói tin (pcap)	Biện pháp ban đầu: chặn IP/ASN, cô lập cổng, thay đổi rule firewall	Ghi lại chuỗi thời gian sự kiện (forensic, ISO/IEC 27035)
1	Giấy in A4	Gram	-	-	-
2	Mực in laser	Hộp	-	-	-
3	Mực máy photocopy	Hộp	-	-	-
4	Cặp để tài liệu	Cái	-	-	-

V. Bảo mật dữ liệu giám sát

1. Định mức lao động

1.1. Nội dung công việc

a) Mã hóa kênh log (TLS), lưu vết truy cập.

b) Chính sách lưu giữ: log chi tiết 90-180 ngày, log tóm tắt 1-3 năm.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng thiết bị mạng gửi log (firewall, IDS/IPS, router, switch)	40	≤10: 10	10–50: 25	>50: 40
2	Kiến trúc truyền log và mã hóa (tập trung, phân tán, multi-site)	20	Truyền nội bộ 1 site: 5	2–3 site: 10	Nhiều vùng mạng/DMZ/cloud: 20
3	Mức độ tuân thủ chuẩn bảo mật dữ liệu log (TLS, ISO/IEC 27035, 27001)	25	TLS mặc định, lưu log nội bộ: 5	Có tuân thủ cơ bản: 15	Yêu cầu nghiêm ngặt theo chuẩn ISO/CIS: 25
4	Mức độ phức tạp trong lưu trữ và chính sách retention	15	Lưu log 1–3 tháng, không phân tầng: 5	Lưu 6–12 tháng, có nén hoặc tóm tắt: 10	Lưu nhiều năm, phân cấp dữ liệu, có backup ngoại vi: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Mã hóa kênh log (TLS), lưu vết truy cập	1	1		2
2	Chính sách lưu giữ: log chi tiết 90–180 ngày, log tóm tắt 1–3 năm		2	1	3

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Mã hóa kênh log (TLS), lưu vết truy cập	Thiết bị	1,5	2,1	2,9
2	Chính sách lưu giữ: log chi tiết 90–180 ngày, log tóm tắt 1–3 năm	Hệ thống	1,8	2,6	3,5

2. Định mức thiết bị

Ca/01 thiết bị

STT	Vật tư, thiết bị	ĐVT	Thời hạn (tháng)	Mã hóa kênh log (TLS), lưu vết truy cập	Chính sách lưu giữ
1	Máy tính để bàn	Bộ	60	0,160	2,400
2	Máy in laser	Cái	60		
3	Điều hoà nhiệt độ	Cái	96	0,028	0,420
4	Máy photocopy	Cái	96	-	-
5	Điện năng (kw)	kW		0,622	9,324

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 thiết bị

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Mã hóa kênh log (TLS), lưu vết truy cập	Chính sách lưu giữ
1	Ghế	Cái	96	0,200	3,000
2	Bàn làm việc	Cái	96	0,200	3,000
3	Quạt trần 0,1 kW	Cái	60	0,035	0,525
4	Đèn neon 0,04 kW	Bộ	36	0,100	1,500
5	Điện năng (kw)	kW		0,063	0,945

Ghi chú: Mức dụng cụ trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Mã hóa kênh log (TLS), lưu vết truy cập	Chính sách lưu giữ
1	Giấy in A4	Gram	-	-
2	Mực in laser	Hộp	-	-
3	Mực máy photocopy	Hộp	-	-
4	Cặp để tài liệu	Cái	-	-

VI. Đánh giá và cải tiến

1. Định mức lao động

1.1. Nội dung công việc

a) Rà soát quy tắc, chữ ký, ngưỡng hàng tháng/quý.

b) Diễn tập ứng cứu (tabletop, kiểm thử xâm nhập).

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng thiết bị mạng giám sát	40	≤10: 10	10–50: 25	>50: 40
2	Mức độ phân tán hệ thống	20	1 mạng nội bộ: 5	2–3 mạng con: 10	Nhiều vùng/DMZ/cloud: 20
3	Mức độ tùy biến cấu hình & quy tắc ATTT	25	Áp dụng rule/chữ ký chuẩn: 5	Điều chỉnh nhẹ: 15	Quy tắc tùy biến chuyên sâu: 25
4	Tích hợp hệ thống giám sát tập trung	15	Có SIEM/log tập trung: 5	Có syslog rời rạc: 10	Chưa có hệ thống, cần triển khai mới: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Rà soát quy tắc, chữ ký, ngưỡng hàng tháng/quý	1	1		2
2	Diễn tập ứng cứu (tabletop, kiểm thử xâm nhập)		2	1	3

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Rà soát quy tắc, chữ ký, ngưỡng hàng tháng/quý	Thiết bị	1,4	2,0	2,8
2	Diễn tập ứng cứu (tabletop, kiểm thử xâm nhập)	Buổi diễn tập	3,0	4,2	5,8

2. Định mức thiết bị

Ca/01 thiết bị

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Rà soát quy tắc, chữ ký, ngưỡng hàng tháng/quý	Diễn tập ứng cứu (tabletop, kiểm thử xâm nhập)
1	Máy tính để bàn	Bộ	60	0,005	0,032
2	Máy in laser	Cái	60		
3	Điều hoà nhiệt độ	Cái	96	0,001	0,006
4	Máy photocopy	Cái	96	-	-
5	Điện năng (kw)	kW		0,021	0,124

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 thiết bị

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Rà soát quy tắc, chữ ký, ngưỡng hàng tháng/quý	Diễn tập ứng cứu (tabletop, kiểm thử xâm nhập)
1	Ghế	Cái	96	0,007	0,040
2	Bàn làm việc	Cái	96	0,007	0,040
3	Quạt trần 0,1 kW	Cái	60	0,001	0,007
4	Đèn neon 0,04 kW	Bộ	36	0,003	0,020
5	Điện năng (kw)	kW		0,002	0,013

Ghi chú: Mức dụng cụ trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Rà soát quy tắc, chữ ký, ngưỡng hàng tháng/quý	Diễn tập ứng cứu (tabletop, kiểm thử xâm nhập)
1	Giấy in A4	Gram	-	-
2	Mực in laser	Hộp	-	-
3	Mực máy photocopy	Hộp	-	-
4	Cặp để tài liệu	Cái	-	-

CHƯƠNG II
ĐỊNH MỨC GIÁM SÁT ĐẢM BẢO AN TOÀN THÔNG TIN CHO HẠ TẦNG ẢO HÓA (CLOUD, VIRTUALIZATION)

I. Chuẩn bị và thiết lập

1. Định mức lao động

1.1. Nội dung công việc

a) Kiểm kê host, VM, container, tài nguyên đám mây.

b) Bật log gốc (AWS CloudTrail, VPC Flow Logs, Azure Monitor, GCP Audit Logs).

c) Cấu hình audit log cho API call, snapshot, migration, thay đổi IAM.

d) Quét lỗ hổng image, áp dụng chính sách registry.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng host/VM/container giám sát	40	≤20: 10	20–100: 25	>100: 40
2	Mức độ phân tán hạ tầng đám mây	20	1 nền tảng (AWS hoặc Azure hoặc GCP…): 5	2 nền tảng: 10	≥3 nền tảng/hybrid cloud: 20
3	Mức độ tùy biến chính sách log/audit	25	Áp dụng theo chuẩn nhà cung cấp (AWS/Azure/GCP…): 5	Có điều chỉnh nhẹ (bổ sung rule riêng): 15	Chính sách riêng biệt, tuỳ chỉnh sâu IAM/API: 25
4	Tích hợp công cụ giám sát và cảnh báo tập trung	15	Đã có SIEM/central log: 5	Có collector riêng từng nền tảng: 10	Chưa có, cần triển khai mới: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Kiểm kê host, VM, container, tài nguyên đám mây	1	1		2
2	Bật log gốc (AWS CloudTrail, VPC Flow Logs, Azure Monitor, GCP Audit Logs)		2		2
3	Cấu hình audit log cho API call, snapshot, migration, thay đổi IAM		2	1	3
4	Quét lỗ hổng image, áp dụng chính sách registry		1	1	2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Kiểm kê host, VM, container, tài nguyên đám mây	Hệ thống	1,5	2,1	3,0
2	Bật log gốc (AWS CloudTrail, VPC Flow Logs, Azure Monitor, GCP… Audit Logs)	Nền tảng	1,8	2,5	3,4
3	Cấu hình audit log cho API call, snapshot, migration, thay đổi IAM	Nền tảng	2,0	2,8	3,8
4	Quét lỗ hổng image, áp dụng chính sách registry	Kho image	2,2	3,0	4,0

2. Định mức thiết bị

Bảng số 03: Ca/01 hệ thống

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Kiểm kê host, VM, container, tài nguyên cloud	Bật log gốc (CloudTrail, Azure Monitor, GCP Audit Logs…)	Cấu hình audit log cho API call, snapshot, IAM	Quét lỗ hổng image, áp dụng chính sách registry
1	Máy tính để bàn	Bộ	60	4,027	4,027	24,160	24,160
2	Máy in laser	Cái	60	-	-	-	-

3	Điều hoà nhiệt độ	Cái	96	0,705	0,705	4,228	4,228
4	Máy photocopy	Cái	96	-	-	-	-
5	Điện năng (kw)	kW		15,644	15,644	93,862	93,862

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Bảng số 03: Ca/01 hệ thống

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Kiểm kê host, VM, container, tài nguyên cloud	Bật log gốc (CloudTrail, Azure Monitor, GCP Audit Logs…)	Cấu hình audit log cho API call, snapshot, IAM	Quét lỗ hổng image, áp dụng chính sách registry
1	Ghế	Cái	96	5,033	5,033	30,200	30,200
2	Bàn làm việc	Cái	96	5,033	5,033	30,200	30,200
3	Quạt trần 0,1 kW	Cái	60	0,881	0,881	5,285	5,285
4	Đèn neon 0,04 kW	Bộ	36	2,517	2,517	15,100	15,100
5	Điện năng (kw)	kW		1,586	1,586	9,513	9,513

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Kiểm kê host, VM, container, tài nguyên cloud	Bật log gốc (CloudTrail, Azure Monitor, GCP Audit Logs…)	Cấu hình audit log cho API call, snapshot, IAM	Quét lỗ hổng image, áp dụng chính sách registry
1	Giấy in A4	Gram	-	-	-	-
2	Mực in laser	Hộp	-	-	-	-
3	Mực máy photocopy	Hộp	-	-	-	-
4	Cặp để tài liệu	Cái	-	-	-	-

II. Thu thập và giám sát

1. Định mức lao động

1.1. Nội dung công việc

a) Log API: thay đổi quyền, tạo khóa truy cập, thay đổi bucket công khai.

b) Giám sát lưu lượng mạng trong nội bộ đám mây (flow logs).

c) Giám sát RBAC trong Kubernetes, hoạt động container.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng nền tảng cloud hoặc cụm ảo hóa cần giám sát	40	1 nền tảng: 10	2 nền tảng: 25	≥3 nền tảng/hybrid cloud: 40
2	Mức độ phân tán vùng mạng và dịch vụ	20	1 vùng mạng (1 VPC/cluster): 5	2–5 vùng: 10	>5 vùng hoặc multi-region: 20
3	Mức độ tùy biến chính sách log và quyền	25	Áp dụng theo chuẩn cloud/k8s gốc: 5	Có điều chỉnh nhẹ (custom rule RBAC, IAM): 15	Chính sách riêng biệt, nhiều namespace, multi-tenant: 25
4	Mức độ tích hợp giám sát và cảnh báo tập trung	15	Đã có SIEM hoặc log collector tập trung: 5	Có log riêng lẻ từng cụm: 10	Chưa có, cần thiết lập mới hoàn toàn: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Log API: thay đổi quyền, tạo khóa truy cập, thay đổi bucket công khai		2		2
2	Giám sát lưu lượng mạng trong nội bộ đám mây (flow logs)	1	1		2
3	Giám sát RBAC trong Kubernetes, hoạt động container		1	1	2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Log API: thay đổi quyền, tạo khóa truy cập, thay đổi bucket công khai	Nền tảng	1,6	2,2	3,0
2	Giám sát lưu lượng mạng trong nội bộ đám mây (flow logs)	Hệ thống	1,8	2,5	3,4
3	Giám sát RBAC trong Kubernetes, hoạt động container	Cụm	2,0	2,8	3,8

2. Định mức thiết bị

Ca/01 hệ thống

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Log API: thay đổi quyền, tạo khóa truy cập, thay đổi bucket công khai	Giám sát lưu lượng mạng trong nội bộ đám mây (Flow Logs)	Giám sát RBAC trong Kubernetes, hoạt động container
1	Máy tính để bàn	Bộ	60	4,027	4,027	24,160
2	Máy in laser	Cái	60	-	-	
3	Điều hoà nhiệt độ	Cái	96	0,705	0,705	4,228
4	Máy photocopy	Cái	96	-	-	-
5	Điện năng (kw)	kW		15,644	15,644	93,862

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 hệ thống

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Log API: thay đổi quyền, tạo khóa truy cập, thay đổi bucket công khai	Giám sát lưu lượng mạng trong nội bộ đám mây (Flow Logs)	Giám sát RBAC trong Kubernetes, hoạt động container
1	Ghế	Cái	96	5,033	5,033	30,200
2	Bàn làm việc	Cái	96	5,033	5,033	30,200
3	Quạt trần 0,1 kW	Cái	60	0,881	0,881	5,285
4	Đèn neon 0,04 kW	Bộ	36	2,517	2,517	15,100
5	Điện năng (kw)	kW		1,586	1,586	9,513

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Log API: thay đổi quyền, tạo khóa truy cập, thay đổi bucket công khai	Giám sát lưu lượng mạng trong nội bộ đám mây (Flow Logs)	Giám sát RBAC trong Kubernetes, hoạt động container
1	Giấy in A4	Gram	-	-	-
2	Mực in laser	Hộp	-	-	-
3	Mực máy photocopy	Hộp	-	-	-
4	Cặp để tài liệu	Cái	-	-	-

III. Phân tích và xử lý

1. Định mức lao động

1.1. Nội dung công việc

a) Tạo IAM key mới + xuất dữ liệu lớn → cảnh báo.

b) Vô hiệu hóa key, cô lập namespace, chặn bucket.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng nền tảng cloud hoặc cụm ảo hóa cần giám sát	40	1 nền tảng: 10	2 nền tảng: 25	≥3 nền tảng hoặc hybrid cloud: 40
2	Mức độ phân tán tài nguyên và chính sách truy cập	20	1 vùng mạng/tenant: 5	2–5 vùng hoặc tenant: 10	>5 vùng hoặc multi-region: 20
3	Mức độ tùy biến chính sách IAM và cảnh báo	25	Áp dụng theo chuẩn IAM mặc định: 5	Có điều chỉnh cảnh báo hoặc custom policy: 15	Chính sách IAM, alert rule riêng biệt, đa tài khoản: 25
4	Tích hợp hệ thống cảnh báo và cô lập tự động	15	Có sẵn SIEM hoặc CloudWatch/ Stackdriver: 5	Có script bán tự động: 10	Chưa có, cần triển khai cơ chế mới: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS3	KS4	Nhóm
1	Tạo IAM key mới + xuất dữ liệu lớn → cảnh báo	2		2
2	Vô hiệu hóa key, cô lập namespace, chặn bucket	1	1	2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Tạo IAM key mới + xuất dữ liệu lớn → cảnh báo	Nền tảng	1,8	2,5	3,4
2	Vô hiệu hóa key, cô lập namespace, chặn bucket	Sự cố	2,0	2,8	3,8

2. Định mức thiết bị

Ca/01 nền tảng

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Tạo IAM key mới + xuất dữ liệu lớn → cảnh báo	Vô hiệu hóa key, cô lập namespace, chặn bucket
1	Máy tính để bàn	Bộ	60	0,080	0,160
2	Máy in laser	Cái	60	0,002	
3	Điều hoà nhiệt độ	Cái	96	0,014	0,028
4	Máy photocopy	Cái	96	0,002	-
5	Điện năng (kw)	kW		0,313	0,622

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 nền tảng

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Tạo IAM key mới + xuất dữ liệu lớn → cảnh báo	Vô hiệu hóa key, cô lập namespace, chặn bucket
1	Ghế	Cái	96	0,100	0,200
2	Bàn làm việc	Cái	96	0,100	0,200
3	Quạt trần 0,1 kW	Cái	60	0,018	0,035
4	Đèn neon 0,04 kW	Bộ	36	0,050	0,100
5	Điện năng (kw)	kW		0,032	0,063

Ghi chú: Mức dụng cụ trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Tạo IAM key mới + xuất dữ liệu lớn → cảnh báo	Vô hiệu hóa key, cô lập namespace, chặn bucket
1	Giấy in A4	Gram	-	0,0040
2	Mực in laser	Hộp	-	0,0011
3	Mực máy photocopy	Hộp	-	0,0011
4	Cặp để tài liệu	Cái	-	0,0040

IV. Bảo mật dữ liệu

1. Định mức lao động

1.1. Nội dung công việc

a) Mã hóa log, lưu giữ theo quy định (GDPR, pháp luật Việt Nam).

b) Thực hiện quản lý bảo mật đám mây (CSPM).

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	**Các yếu tố ảnh hưởng**	**Điểm tối đa**	**Mức thấp**	**Mức trung bình**	**Mức cao**
1	Số lượng nền tảng cloud/hypervisor cần giám sát	35	1 nền tảng (ví dụ: VMware hoặc AWS): 10	2–3 nền tảng: 25	>3 nền tảng (multi-cloud, hybrid): 35
2	Mức độ phân tán và tích hợp lưu trữ log	25	Lưu log nội bộ, tập trung: 10	Lưu log nhiều vùng, có forwarding: 15	Lưu log phân tán nhiều khu vực, cần mã hóa đầu cuối: 25
3	Mức độ yêu cầu tuân thủ pháp lý và tiêu chuẩn quốc tế	25	Tuân thủ nội bộ cơ bản: 10	Tuân thủ pháp luật Việt Nam: 15	Tuân thủ đồng thời GDPR + Việt Nam + ISO 27001: 25
4	Mức độ phức tạp chính sách CSPM và automation	15	Chính sách mặc định của cloud provider: 5	Có tùy chỉnh rule CSPM: 10	Tự động hóa kiểm tra chính sách đa cloud: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Mã hóa log, lưu giữ theo quy định (GDPR, pháp luật Việt Nam)	1	1		2
2	Thực hiện quản lý bảo mật đám mây (CSPM)		2	1	3

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Mã hóa log, lưu giữ theo quy định (GDPR, pháp luật Việt Nam)	Nền tảng	1,8	2,4	3,2
2	Thực hiện quản lý bảo mật đám mây (CSPM)	Nền tảng	2,0	2,8	3,8

2. Định mức thiết bị

Ca/01 nền tảng

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Mã hóa log, lưu giữ theo quy định (GDPR, pháp luật Việt Nam)	Thực hiện quản lý bảo mật đám mây (CSPM)
1	Máy tính để bàn	Bộ	60	0,080	0,160
2	Máy in laser	Cái	60	0,002	
3	Điều hoà nhiệt độ	Cái	96	0,014	0,028
4	Máy photocopy	Cái	96	0,002	-
5	Điện năng (kw)	kW		0,313	0,622

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 nền tảng

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Mã hóa log, lưu giữ theo quy định (GDPR, pháp luật Việt Nam)	Thực hiện quản lý bảo mật đám mây (CSPM)
1	Ghế	Cái	96	0,100	0,200
2	Bàn làm việc	Cái	96	0,100	0,200
3	Quạt trần 0,1 kW	Cái	60	0,018	0,035
4	Đèn neon 0,04 kW	Bộ	36	0,050	0,100
5	Điện năng (kw)	kW		0,032	0,063

Ghi chú: Mức dụng cụ trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Mã hóa log, lưu giữ theo quy định (GDPR, pháp luật Việt Nam)	Thực hiện quản lý bảo mật đám mây (CSPM)
1	Giấy in A4	Gram	-	0,0040
2	Mực in laser	Hộp	-	0,0011
3	Mực máy photocopy	Hộp	-	0,0011
4	Cặp để tài liệu	Cái	-	0,0040

CHƯƠNG III
ĐỊNH MỨC GIÁM SÁT ĐẢM BẢO AN TOÀN THÔNG TIN CHO MÁY CHỦ (HỆ ĐIỀU HÀNH WINDOWS, LINUX)

I. Chuẩn bị và thiết lập

1. Định mức lao động

1.1. Nội dung công việc

a) Kiểm kê hệ điều hành, phiên bản, bản vá, vai trò.

b) Tăng cường bảo mật (hardening) theo chuẩn CIS.

c) Bật audit logging: syslog (Linux), Windows Event Forwarding, audit DB.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng máy chủ giám sát	40	≤10: 10	10-50: 25	>50: 40
2	Mức độ phân tán hệ thống	20	Nội bộ 1 mạng: 5	2-3 mạng con: 10	Nhiều vùng/DMZ/cloud: 20
3	Mức độ tùy biến chính sách bảo mật	25	Áp dụng chuẩn CIS gốc: 5	Có điều chỉnh nhẹ: 15	Chính sách riêng biệt: 25
4	Tích hợp công cụ giám sát tập trung	15	Có sẵn SIEM/log tập trung: 5	Có syslog riêng lẻ: 10	Chưa có hệ thống, cần triển khai mới: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Kiểm kê hệ điều hành, phiên bản, bản vá, vai trò	1	1		2
2	Tăng cường bảo mật (hardening) theo chuẩn CIS		2	1	3
3	Bật audit logging (syslog, WEF, audit DB)		2		2
4	Triển khai giám sát tính toàn vẹn tệp (File Integrity Monitoring)		1	1	2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Kiểm kê hệ điều hành, phiên bản, bản vá, vai trò	Máy chủ	1,2	1,6	2,2
2	Tăng cường bảo mật (hardening) theo chuẩn CIS	Máy chủ	1,8	2,5	3,5
3	Bật audit logging (syslog, WEF, audit DB)	Máy chủ	1,6	2,2	3,0
4	Triển khai giám sát tính toàn vẹn tệp (File Integrity Monitoring)	Máy chủ	2,0	2,8	3,8

2. Định mức thiết bị

Ca/01 máy chủ

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Kiểm kê hệ điều hành, phiên bản, bản vá, vai trò	Tăng cường bảo mật (hardening) theo chuẩn CIS	Bật audit logging (syslog, WEF, audit DB)	Triển khai giám sát tính toàn vẹn tệp (File Integrity Monitoring)
1	Máy tính để bàn	Bộ	60	4,027	4,027	24,160	24,160
2	Máy in laser	Cái	60	-	-		
3	Điều hoà nhiệt độ	Cái	96	0,705	0,705	4,228	4,228
4	Máy photocopy	Cái	96	-	-	-	-
5	Điện năng (kw)	kW		15,644	15,644	93,862	93,862

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 máy chủ

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Kiểm kê hệ điều hành, phiên bản, bản vá, vai trò	Tăng cường bảo mật (hardening) theo chuẩn CIS	Bật audit logging (syslog, WEF, audit DB)	Triển khai giám sát tính toàn vẹn tệp (File Integrity Monitoring)
1	Ghế	Cái	96	5,033	5,033	30,200	30,200
2	Bàn làm việc	Cái	96	5,033	5,033	30,200	30,200
3	Quạt trần 0,1 kW	Cái	60	0,881	0,881	5,285	5,285
4	Đèn neon 0,04 kW	Bộ	36	2,517	2,517	15,100	15,100
5	Điện năng (kw)	kW		1,586	1,586	9,513	9,513

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Kiểm kê hệ điều hành, phiên bản, bản vá, vai trò	Tăng cường bảo mật (hardening) theo chuẩn CIS	Bật audit logging (syslog, WEF, audit DB)	Triển khai giám sát tính toàn vẹn tệp (File Integrity Monitoring)
1	Giấy in A4	Gram	-	-	-	-
2	Mực in laser	Hộp	-	-	-	-
3	Mực máy photocopy	Hộp	-	-	-	-
4	Cặp để tài liệu	Cái	-	-	-	-

II. Thu thập và giám sát

1. Định mức lao động

1.1. Nội dung công việc

a) Log: đăng nhập thành công/thất bại, sử dụng sudo, lỗi kernel.

b) Log DB: truy vấn lỗi, thay đổi cấu trúc, xuất dữ liệu.

c) Giám sát CPU, RAM, I/O, số lượng kết nối.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng máy chủ cần giám sát	40	≤10: 10	10-50: 25	>50: 40
2	Đa dạng loại log và nguồn log	25	1-2 loại: 10	3-5 loại: 15	>5 loại: 25
3	Mức độ phức tạp xử lý & lọc log	20	Ghi nhận thô: 5	Có rule đơn giản: 10	Có parser phức tạp: 20
4	Hình thức thu thập & lưu trữ log	15	Qua syslog tập trung: 5	Qua agent cục bộ: 10	Kết hợp SIEM/agent/cloud API: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm	Ký hiệu
1	Dễ	K ≤ 50	KK1
2	Trung bình	50 < K < 80	KK2
3	Khó	K ≥ 80	KK3

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Log: đăng nhập thành công/thất bại, sử dụng sudo, lỗi kernel	1	1		2
2	Log DB: truy vấn lỗi, thay đổi cấu trúc, xuất dữ liệu		1	1	2
3	Giám sát CPU, RAM, I/O, số lượng kết nối	1	1		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK 1	KK 2	KK 3
1	Log: đăng nhập thành công/thất bại, sử dụng sudo, lỗi kernel	Máy chủ	1,4	1,9	2,6
2	Log DB: truy vấn lỗi, thay đổi cấu trúc, xuất dữ liệu	Máy chủ	1,8	2,4	3,2
3	Giám sát CPU, RAM, I/O, số lượng kết nối	Máy chủ	1,2	1,8	2,4

2. Định mức thiết bị

Ca/01 máy chủ

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Log: đăng nhập thành công/thất bại, sử dụng sudo, lỗi kernel	Log DB: truy vấn lỗi, thay đổi cấu trúc, xuất dữ liệu	Giám sát CPU, RAM, I/O, số lượng kết nối
1	Máy tính để bàn	Bộ	60	4,027	4,027	24,160
2	Máy in laser	Cái	60	-	-	
3	Điều hoà nhiệt độ	Cái	96	0,705	0,705	4,228
4	Máy photocopy	Cái	96	-	-	-
5	Điện năng (kw)	kW		15,644	15,644	93,862

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 máy chủ

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Log: đăng nhập thành công/thất bại, sử dụng sudo, lỗi kernel	Log DB: truy vấn lỗi, thay đổi cấu trúc, xuất dữ liệu	Giám sát CPU, RAM, I/O, số lượng kết nối
1	Ghế	Cái	96	5,033	5,033	30,200
2	Bàn làm việc	Cái	96	5,033	5,033	30,200
3	Quạt trần 0,1 kW	Cái	60	0,881	0,881	5,285
4	Đèn neon 0,04 kW	Bộ	36	2,517	2,517	15,100
5	Điện năng (kw)	kW		1,586	1,586	9,513

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Log: đăng nhập thành công/thất bại, sử dụng sudo, lỗi kernel	Log DB: truy vấn lỗi, thay đổi cấu trúc, xuất dữ liệu	Giám sát CPU, RAM, I/O, số lượng kết nối
1	Giấy in A4	Gram	-	-	-
2	Mực in laser	Hộp	-	-	-
3	Mực máy photocopy	Hộp	-	-	-
4	Cặp để tài liệu	Cái	-	-	-

III. Phân tích và xác minh

1. Định mức lao động

1.1. Nội dung công việc

a) Tương quan: nhiều lần đăng nhập thất bại trên nhiều server → tấn công ngang.

b) Kích hoạt điều tra forensic (memory dump, snapshot).

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Giải thích ý nghĩa	Điểm tối đa
1	Số lượng máy chủ được giám sát	Tổng số máy chủ cần giám sát, ảnh hưởng khối lượng dữ liệu log cần phân tích	30
2	Số lượng sự kiện bảo mật cần phân tích (log alert, failed login, policy change…)	Quy mô dữ liệu log và mức độ phức tạp trong lọc, tương quan	25
3	Mức độ tích hợp và tương quan sự kiện giữa nhiều hệ điều hành / mạng	Phản ánh mức khó khi phải so khớp log giữa Windows-Linux-AD-Firewall…	25
4	Yêu cầu kỹ thuật điều tra số (Forensic)	Có cần thực hiện memory dump, snapshot, phục hồi log, khôi phục chuỗi sự kiện	20
	Tổng cộng		**100**

Tính điểm theo các yếu tố ảnh hưởng:

STT	Các yếu tố ảnh hưởng	Mức chi tiết	Điểm
1	Số lượng máy chủ được giám sát	$m \leq 10 \rightarrow 10$; $10 < m < 30 \rightarrow 20$; $m \geq 30 \rightarrow 30$	30
2	Số lượng sự kiện bảo mật cần phân tích	$m \leq 1.000 \rightarrow 10$; $1.000 < m < 5.000 \rightarrow 15$; $m \geq 5.000 \rightarrow 25$	25
3	Mức độ tích hợp & tương quan đa nền tảng	Chỉ 1 HĐH → 10 ; 2 HĐH → 20 ; ≥3 HĐH (Windows + Linux + thiết bị mạng) → 25	25
4	Yêu cầu kỹ thuật điều tra số (Forensic)	Không yêu cầu → 0 ; Dump/snapshot cơ bản → 10 ; Phân tích sâu (memory, timeline, recovery) → 20	20

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm	Ký hiệu
1	Dễ	$K \leq 50$	KK1
2	Trung bình	$50 < K < 80$	KK2
3	Khó	$K \geq 80$	KK3

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Tương quan: nhiều lần đăng nhập thất bại trên nhiều server → tấn công ngang	1	1		2
2	Kích hoạt điều tra forensic (memory dump, snapshot)		1	1	2

1.4. Định mức

STT	Danh mục công việc	Đơn vị tính (ĐVT)	KK 1	KK 2	KK 3
1	Tương quan: nhiều lần đăng nhập thất bại trên nhiều server → tấn công ngang	Sự kiện (đợt phân tích)	2,0	2,6	3,4
2	Kích hoạt điều tra forensic (memory dump, snapshot)	Phiên điều tra	3,0	3,8	5,2

2. Định mức thiết bị

Ca/01 đợt

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Tương quan: nhiều lần đăng nhập thất bại trên nhiều server → tấn công ngang	Kích hoạt điều tra forensic (memory dump, snapshot)
1	Máy tính để bàn	Bộ	60	0,080	0,160
2	Máy in laser	Cái	60	0,002	
3	Điều hoà nhiệt độ	Cái	96	0,014	0,028
4	Máy photocopy	Cái	96	0,002	-
5	Điện năng (kw)	kW		0,313	0,622

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 đợt

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Tương quan: nhiều lần đăng nhập thất bại trên nhiều server → tấn công ngang	Kích hoạt điều tra forensic (memory dump, snapshot)
1	Ghế	Cái	96	0,100	0,200
2	Bàn làm việc	Cái	96	0,100	0,200

3	Quạt trần 0,1 kW	Cái	60	0,018	0,035
4	Đèn neon 0,04 kW	Bộ	36	0,050	0,100
5	Điện năng (kw)	kW		0,032	0,063

Ghi chú: Mức dụng cụ trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Tương quan: nhiều lần đăng nhập thất bại trên nhiều server → tấn công ngang	Kích hoạt điều tra forensic (memory dump, snapshot)
1	Giấy in A4	Gram	-	0,0040
2	Mực in laser	Hộp	-	0,0011
3	Mực máy photocopy	Hộp	-	0,0011
4	Cặp để tài liệu	Cái	-	0,0040

IV. Ứng cứu ban đầu

1. Định mức lao động

1.1. Nội dung công việc

a) Cô lập server, vô hiệu hóa tài khoản, thay đổi mật khẩu.

b) Tạo snapshot để lưu bằng chứng.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	**Các yếu tố ảnh hưởng**	**Giải thích ý nghĩa**	**Điểm tối đa**
1	Số lượng máy chủ bị ảnh hưởng	Quy mô sự cố cần cô lập hoặc xử lý	30
2	Mức độ nghiêm trọng của sự cố (phá hoại, lây lan, truy cập trái phép)	Ảnh hưởng tới quy trình ứng cứu và khối lượng thao tác	25
3	Phạm vi và tính kết nối của hệ thống (mạng nội bộ, DMZ, cloud)	Độ phức tạp khi cô lập hoặc thay đổi quyền truy cập	25
4	Yêu cầu lưu trữ bằng chứng (snapshot, forensic)	Có yêu cầu snapshot, ghi log, backup bằng chứng để phục vụ điều tra	20
Tổng cộng			**100**

Tính điểm theo các yếu tố ảnh hưởng:

STT	Các yếu tố ảnh hưởng	Mức chi tiết	Điểm
1	Số lượng máy chủ bị ảnh hưởng	$m \leq 5 \rightarrow 10$; $5 < m < 20 \rightarrow 20$; $m \geq 20 \rightarrow 30$	30
2	Mức độ nghiêm trọng của sự cố	Mức thấp (tài khoản đơn lẻ) → 10 ; Trung bình (nhiều tài khoản, chưa lan truyền) → 15 ; Cao (xâm nhập, mã độc, lan truyền) → 25	25
3	Phạm vi và tính kết nối của hệ thống	Một mạng nội bộ → 10 ; Có DMZ hoặc VPN kết nối ngoài → 20 ; Nhiều môi trường (on-prem + cloud) → 25	25
4	Yêu cầu lưu trữ bằng chứng (snapshot, forensic)	Không yêu cầu → 0 ; Snapshot cơ bản → 10 ; Snapshot + forensic chi tiết → 20	20

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm	Ký hiệu
1	Dễ	$K \leq 50$	KK1
2	Trung bình	$50 < K < 80$	KK2
3	Khó	$K \geq 80$	KK3

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Cô lập server, vô hiệu hóa tài khoản, thay đổi mật khẩu	1	1		2
2	Tạo snapshot để lưu bằng chứng		1	1	2

1.4. Định mức

STT	Danh mục công việc	Đơn vị tính (ĐVT)	KK1	KK2	KK3
1	Cô lập server, vô hiệu hóa tài khoản, thay đổi mật khẩu	Sự cố (máy chủ)	2,0	2,6	3,4
2	Tạo snapshot để lưu bằng chứng	Máy chủ	2,6	3,2	4,2

2. Định mức thiết bị

Ca/01 máy chủ

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Cô lập server, vô hiệu hóa tài khoản, thay đổi mật khẩu	Tạo snapshot để lưu bằng chứng
1	Máy tính để bàn	Bộ	60	0,480	2,880
2	Máy in laser	Cái	60		
3	Điều hoà nhiệt độ	Cái	96	0,084	0,504
4	Máy photocopy	Cái	96	-	-
5	Điện năng (kw)	kW		1,865	11,189

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 máy chủ

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Cô lập server, vô hiệu hóa tài khoản, thay đổi mật khẩu	Tạo snapshot để lưu bằng chứng
1	Ghế	Cái	96	0,600	3,600
2	Bàn làm việc	Cái	96	0,600	3,600
3	Quạt trần 0,1 kW	Cái	60	0,105	0,630
4	Đèn neon 0,04 kW	Bộ	36	0,300	1,800
5	Điện năng (kw)	kW		0,189	1,134

Ghi chú: Mức dụng cụ trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Cô lập server, vô hiệu hóa tài khoản, thay đổi mật khẩu	Tạo snapshot để lưu bằng chứng
1	Giấy in A4	Gram	-	-
2	Mực in laser	Hộp	-	-
3	Mực máy photocopy	Hộp	-	-
4	Cặp để tài liệu	Cái	-	-

V. Bảo mật dữ liệu

1. Định mức lao động

1.1. Nội dung công việc

a) Mã hóa log khi lưu trữ, kiểm soát truy cập.

b) Chính sách lưu giữ log.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Giải thích ý nghĩa	Điểm tối đa
1	Số lượng máy chủ cần bảo mật log	Phản ánh khối lượng dữ liệu log và phạm vi quản lý	30
2	Cấp độ mã hóa và tiêu chuẩn bảo mật áp dụng	Mức độ phức tạp khi thiết lập, duy trì và kiểm tra mã hóa	25
3	Hệ thống kiểm soát truy cập (ACL, RBAC, LDAP, AD, IAM)	Mức độ phức tạp trong quản lý quyền truy cập log và dữ liệu	25
4	Yêu cầu về chính sách lưu giữ log	Thời gian lưu, mức độ chi tiết log, khả năng truy xuất khi cần điều tra	20
	Tổng cộng		**100**

Tính điểm theo các yếu tố ảnh hưởng:

STT	Các yếu tố ảnh hưởng	Mức chi tiết	Điểm
1	Số lượng máy chủ cần bảo mật log	$m \leq 5 \rightarrow 10$; $5 < m < 20 \rightarrow 20$; $m \geq 20 \rightarrow 30$	30
2	Cấp độ mã hóa & tiêu chuẩn bảo mật	Cơ bản (AES128, nội bộ) → 10 ; Trung bình (AES256, TLS) → 15 ; Cao (FIPS, PKI, HSM, chứng thực đa tầng) → 25	25
3	Hệ thống kiểm soát truy cập	Cơ bản (local user) → 10 ; Trung bình (RBAC nội bộ) → 15 ; Cao (AD/LDAP + IAM tập trung) → 25	25
4	Yêu cầu về chính sách lưu giữ log	≤ 90 ngày → 10 ; 90-180 ngày → 15 ; > 180 ngày hoặc chi tiết nhiều mức → 20	20

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm	Ký hiệu
1	Dễ	K ≤ 50	KK1
2	Trung bình	50 < K < 80	KK2
3	Khó	K ≥ 80	KK3

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Mã hóa log khi lưu trữ, kiểm soát truy cập	1	1		2
2	Chính sách lưu giữ log		1	1	2

1.4. Định mức

STT	Danh mục công việc	Đơn vị tính (ĐVT)	KK1	KK2	KK3
1	Mã hóa log khi lưu trữ, kiểm soát truy cập	Máy chủ	2,0	2,6	3,4
2	Chính sách lưu giữ log	Hệ thống	2,4	3,0	3,9

2. Định mức thiết bị

Ca/01 máy chủ

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Mã hóa log khi lưu trữ, kiểm soát truy cập	Chính sách lưu giữ log
1	Máy tính để bàn	Bộ	60	0,080	0,160
2	Máy in laser	Cái	60	0,002	
3	Điều hoà nhiệt độ	Cái	96	0,014	0,028
4	Máy photocopy	Cái	96	0,002	-
5	Điện năng (kw)	kW		0,313	0,622

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 máy chủ

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Mã hóa log khi lưu trữ, kiểm soát truy cập	Chính sách lưu giữ log
1	Ghế	Cái	96	0,100	0,200
2	Bàn làm việc	Cái	96	0,100	0,200
3	Quạt trần 0,1 kW	Cái	60	0,018	0,035
4	Đèn neon 0,04 kW	Bộ	36	0,050	0,100
5	Điện năng (kw)	kW		0,032	0,063

Ghi chú: Mức dụng cụ trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Mã hóa log khi lưu trữ, kiểm soát truy cập	Chính sách lưu giữ log
1	Giấy in A4	Gram	-	0,0040
2	Mực in laser	Hộp	-	0,0011
3	Mực máy photocopy	Hộp	-	0,0011
4	Cặp để tài liệu	Cái	-	0,0040

VI. Đánh giá định kỳ

1. Định mức lao động

1.1. Nội dung công việc

Quét lỗ hổng, lập lịch vá lỗi, báo cáo thay đổi cấu hình

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	**Các yếu tố ảnh hưởng**	**Giải thích ý nghĩa**	**Điểm tối đa**
1	Số lượng máy chủ cần quét và đánh giá	Phản ánh khối lượng công việc cần quét, kiểm tra và tổng hợp	30
2	Mức độ phức tạp của hệ điều hành và dịch vụ đang chạy	Đa dạng nền tảng và ứng dụng khiến việc quét và đánh giá khó hơn	25
3	Chu kỳ đánh giá và yêu cầu lập lịch vá lỗi	Độ thường xuyên và tính chính xác trong quản lý lịch trình vá lỗi	25
4	Mức độ chi tiết của báo cáo thay đổi cấu hình	Ảnh hưởng khối lượng phân tích, so sánh và ghi nhận kết quả	20
	Tổng cộng		**100**

Tính điểm theo các yếu tố ảnh hưởng:

STT	Các yếu tố ảnh hưởng	Mức chi tiết	Điểm
1	Số lượng máy chủ cần quét và đánh giá	m ≤ 10 → 10 ; 10 < m < 30 → 20 ; m ≥ 30 → 30	30
2	Mức độ phức tạp của HĐH và dịch vụ	HĐH đồng nhất (chỉ Windows hoặc Linux) → 10 ; 2 loại HĐH → 15 ; Hỗn hợp + nhiều dịch vụ (DB, Web, AD, Mail) → 25	25
3	Chu kỳ đánh giá & lập lịch vá lỗi	Hàng quý → 10 ; Hàng tháng → 15 ; Hàng tuần / liên tục → 25	25
4	Mức độ chi tiết báo cáo cấu hình	Chỉ tổng hợp thay đổi chính → 10 ; Có log chi tiết theo file/service → 15 ; Có đối chiếu baseline tự động → 20	20

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm	Ký hiệu
1	Dễ	K ≤ 50	KK1
2	Trung bình	50 < K < 80	KK2
3	Khó	K ≥ 80	KK3

1.3. Định biên

STT	Danh mục công việc	KS 2	KS 3	KS 4	Nhóm
1	Quét lỗ hổng, lập lịch vá lỗi, báo cáo thay đổi cấu hình	1	1	1	3

1.4. Định mức

STT	Danh mục công việc	Đơn vị tính (ĐVT)	KK 1	KK 2	KK 3
1	Quét lỗ hổng, lập lịch vá lỗi, báo cáo thay đổi cấu hình	Máy chủ	2,4	3,0	3,9

2. Định mức thiết bị

Ca/01 máy chủ

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Quét lỗ hổng, lập lịch vá lỗi, báo cáo thay đổi cấu hình
1	Máy tính để bàn	Bộ	60	0,005
2	Máy in laser	Cái	60	
3	Điều hoà nhiệt độ	Cái	96	0,001
4	Máy photocopy	Cái	96	-
5	Điện năng (kw)	kW		0,021

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 máy chủ

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Quét lỗ hổng, lập lịch vá lỗi, báo cáo thay đổi cấu hình
1	Ghế	Cái	96	0,007
2	Bàn làm việc	Cái	96	0,007
3	Quạt trần 0,1 kW	Cái	60	0,001
4	Đèn neon 0,04 kW	Bộ	36	0,003
5	Điện năng (kw)	kW		0,002

Ghi chú: Mức dụng cụ trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Quét lỗ hổng, lập lịch vá lỗi, báo cáo thay đổi cấu hình
1	Giấy in A4	Gram	-
2	Mực in laser	Hộp	-
3	Mực máy photocopy	Hộp	-
4	Cặp để tài liệu	Cái	-

CHƯƠNG IV
ĐỊNH MỨC GIÁM SÁT ĐẢM BẢO AN TOÀN THÔNG TIN CHO ỨNG DỤNG (WEB, ERP, CRM, API, EMAIL)

I. Chuẩn bị và thiết lập

1. Định mức lao động

1.1. Nội dung công việc

a) Kiểm kê danh mục ứng dụng, phiên bản, môi trường triển khai (dev/test/prod).

b) Bật log truy cập, xác thực, lỗi ứng dụng, giao dịch API.

c) Cấu hình tường lửa ứng dụng web (WAF), DLP, bảo vệ API gateway.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng ứng dụng giám sát	40	≤5: 10	5–20: 25	>20: 40
2	Mức độ phân tán môi trường triển khai	20	Một môi trường: 5	2–3 môi trường: 10	>3 môi trường (multi-cloud): 20
3	Mức độ tùy biến cấu hình bảo mật	25	Dùng chính sách chuẩn: 5	Có tùy chỉnh nhẹ: 15	Cấu hình riêng cho từng ứng dụng: 25
4	Hệ thống quản lý log tập trung	15	Có SIEM/log tập trung: 5	Có log riêng lẻ: 10	Chưa có, cần tích hợp mới: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Kiểm kê danh mục ứng dụng, phiên bản, môi trường triển khai (dev/test/prod)	1	1		2
2	Bật log truy cập, xác thực, lỗi ứng dụng, giao dịch API		2	1	3
3	Cấu hình tường lửa ứng dụng web (WAF), DLP, bảo vệ API gateway		2	1	3

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Kiểm kê danh mục ứng dụng, phiên bản, môi trường triển khai (dev/test/prod)	Ứng dụng	1,5	2,0	2,8
2	Bật log truy cập, xác thực, lỗi ứng dụng, giao dịch API	Ứng dụng	2,0	2,8	3,8
3	Cấu hình tường lửa ứng dụng web (WAF), DLP, bảo vệ API gateway	Ứng dụng	2,2	3,0	4,0

2. Định mức thiết bị

Ca/01 thiết bị

STT	Thiết bị	ĐVT	Công suất (Kw)	Kiểm kê danh mục ứng dụng, phiên bản, môi trường triển khai (dev/test/prod)	Bật log truy cập, xác thực, lỗi ứng dụng, giao dịch API	Cấu hình tường lửa ứng dụng web (WAF), DLP, bảo vệ API gateway
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,6
2	Máy in laser	Cái	0,6	0	0,053	0,053
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,101
4	Điện năng	Kw		1,3	6,2	4,2

3. Định mức dụng cụ

Ca/01 thiết bị

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Kiểm kê danh mục ứng dụng, phiên bản, môi trường triển khai (dev/test/prod)	Bật log truy cập, xác thực, lỗi ứng dụng, giao dịch API	Cấu hình tường lửa ứng dụng web (WAF), DLP, bảo vệ API gateway
1	Ghế	Cái	96	0,2	1,2	0,6
2	Bàn làm việc	Cái	96	0,2	1,2	0,6
3	Quạt trần	Cái	96	0,035	0,21	0,105
4	Đèn neon	Bộ	24	0,1	0,6	0,3
5	Điện năng	kW		0,06	0,38	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Kiểm kê danh mục ứng dụng, phiên bản, môi trường triển khai (dev/test/prod)	Bật log truy cập, xác thực, lỗi ứng dụng, giao dịch API	Cấu hình tường lửa ứng dụng web (WAF), DLP, bảo vệ API gateway
1	Giấy in A4	Gram		0,015	0,003
2	Mực in laser	Hộp		0,015	0,003

II. Thu thập và giám sát

1. Định mức lao động

1.1. Nội dung công việc

a) Thu thập log request/response, API usage, cảnh báo từ WAF và IDS.

b) Giám sát truy cập bất thường, tần suất POST/GET cao, lỗi 4xx/5xx, email spam/phishing.

c) Giám sát hành vi giao dịch nghi ngờ (fraud detection, brute force, SQLi, XSS).

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	**Các yếu tố ảnh hưởng**	**Điểm tối đa**	**Mức thấp**	**Mức trung bình**	**Mức cao**
1	Số lượng nguồn log	40	≤5: 10	5–20: 25	>20: 40

2	Mức độ tự động hóa giám sát	20	Có dashboard sẵn: 5	Giám sát bán tự động: 10	Thủ công hoặc cần script mới: 20
3	Tích hợp công cụ cảnh báo	25	Có sẵn: 5	Cần cấu hình lại: 15	Tích hợp mới: 25
4	Khối lượng cảnh báo/ngày	15	<100: 5	100–500: 10	>500: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Thu thập log request/response, API usage, cảnh báo từ WAF và IDS	1	1		2
2	Giám sát truy cập bất thường, tần suất POST/GET cao, lỗi 4xx/5xx, email spam/phishing		2		2
3	Giám sát hành vi giao dịch nghi ngờ (fraud detection, brute force, SQLi, XSS)		1	1	2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Thu thập log request/response, API usage, cảnh báo từ WAF và IDS	Ứng dụng	1,6	2,2	3,0
2	Giám sát truy cập bất thường, tần suất POST/GET cao, lỗi 4xx/5xx, email spam/phishing	Ứng dụng	1,8	2,5	3,4
3	Giám sát hành vi giao dịch nghi ngờ (fraud detection, brute force, SQLi, XSS)	Ứng dụng	2,0	2,8	3,8

2. Định mức thiết bị

Ca/01 thiết bị

STT	Thiết bị	ĐVT	Công suất (Kw)	Thu thập log request/response, API usage, cảnh báo từ WAF và IDS	Giám sát truy cập bất thường, tần suất POST/GET cao, lỗi 4xx/5xx, email spam/phishing	Giám sát hành vi giao dịch nghi ngờ (fraud detection, brute force, SQLi, XSS)
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,6
2	Máy in laser	Cái	0,6	0	0,053	0,053
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,101
4	Điện năng	Kw		1,3	6,2	4,2

3. Định mức dụng cụ

Ca/01 thiết bị

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Thu thập log request/response, API usage, cảnh báo từ WAF và IDS	Giám sát truy cập bất thường, tần suất POST/GET cao, lỗi 4xx/5xx, email spam/phishing	Giám sát hành vi giao dịch nghi ngờ (fraud detection, brute force, SQLi, XSS)
1	Ghế	Cái	96	0,2	1,2	0,6
2	Bàn làm việc	Cái	96	0,2	1,2	0,6
3	Quạt trần	Cái	96	0,035	0,21	0,105
4	Đèn neon	Bộ	24	0,1	0,6	0,3
5	Điện năng	kW		0,06	0,38	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Thu thập log request/response, API usage, cảnh báo từ WAF và IDS	Giám sát truy cập bất thường, tần suất POST/GET cao, lỗi 4xx/5xx, email spam/phishing	Giám sát hành vi giao dịch nghi ngờ (fraud detection, brute force, SQLi, XSS)
1	Giấy in A4	Gram		0,015	0,003
2	Mực in laser	Hộp		0,015	0,003

III. Phân tích và tương quan

1. Định mức lao động

1.1. Nội dung công việc

a) Tương quan WAF block + login thất bại hàng loạt → tấn công brute force.

b) Phân tích chuỗi request để phát hiện khai thác API hoặc rò rỉ dữ liệu.

c) Kết hợp log ứng dụng và hệ thống xác thực (SSO/AD) để xác minh người dùng.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Yếu tố	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng nguồn log tương quan	40	≤3: 10	4–8: 25	>8: 40
2	Tự động hóa phân tích	25	Có SIEM rule sẵn: 5	Tùy chỉnh rule: 15	Viết rule mới: 25
3	Khối lượng log/ngày	20	<1GB: 5	1–10GB: 10	>10GB: 20
4	Độ phức tạp hành vi nghi ngờ	15	Đơn giản: 5	Trung bình: 10	Đa dạng/chuỗi tấn công: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

STT	Công việc	KS3	KS4	Nhóm
1	Tương quan WAF block + login thất bại hàng loạt → tấn công brute force	2		2
2	Phân tích chuỗi request để phát hiện khai thác API hoặc rò rỉ dữ liệu	1	1	2
3	Kết hợp log ứng dụng và hệ thống xác thực (SSO/AD) để xác minh người dùng	2		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Tương quan WAF block + login thất bại hàng loạt → tấn công brute force	Ứng dụng	1,8	2,6	3,6
2	Phân tích chuỗi request để phát hiện khai thác API hoặc rò rỉ dữ liệu	Ứng dụng	2,2	3,0	4,0
3	Kết hợp log ứng dụng và hệ thống xác thực (SSO/AD) để xác minh người dùng	Ứng dụng	1,6	2,2	3,0

2. Định mức thiết bị

Ca/01 Ứng dụng

STT	Thiết bị	ĐVT	Công suất (Kw)	Tương quan WAF block + login thất bại hàng loạt → tấn công brute force	Phân tích chuỗi request để phát hiện khai thác API hoặc rò rỉ dữ liệu	Kết hợp log ứng dụng và hệ thống xác thực (SSO/AD) để xác minh người dùng
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,6
2	Máy in laser	Cái	0,6	0	0,053	0,053
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,101
4	Điện năng	Kw		1,3	6,2	4,2

3. Định mức dụng cụ

Ca/01 Ứng dụng

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Tương quan WAF block + login thất bại hàng loạt → tấn công brute force	Phân tích chuỗi request để phát hiện khai thác API hoặc rò rỉ dữ liệu	Kết hợp log ứng dụng và hệ thống xác thực (SSO/AD) để xác minh người dùng
1	Ghế	Cái	96	0,2	1,2	0,6
2	Bàn làm việc	Cái	96	0,2	1,2	0,6
3	Quạt trần	Cái	96	0,035	0,21	0,105
4	Đèn neon	Bộ	24	0,1	0,6	0,3
5	Điện năng	kW		0,06	0,38	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Tương quan WAF block + login thất bại hàng loạt → tấn công brute force	Phân tích chuỗi request để phát hiện khai thác API hoặc rò rỉ dữ liệu	Kết hợp log ứng dụng và hệ thống xác thực (SSO/AD) để xác minh người dùng
1	Giấy in A4	Gram		0,015	0,003
2	Mực in laser	Hộp		0,015	0,003

IV. Ứng cứu ban đầu

1. Định mức lao động

1.1. Nội dung công việc

a) Giới hạn tốc độ, tạm khóa tài khoản, reset mật khẩu.

b) Vá nóng (hotfix), cập nhật chữ ký WAF, chặn IP/ASN tấn công.

c) Thông báo sự cố và ghi nhận bằng chứng phục vụ điều tra.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	**Các yếu tố ảnh hưởng**	**Điểm tối đa**	**Mức thấp**	**Mức trung bình**	**Mức cao**
1	Số lượng ứng dụng hoặc dịch vụ bị ảnh hưởng	40	≤5: 10	6–15: 25	>15: 40
2	Mức độ phức tạp của sự cố	25	Lỗi đơn giản, xác định được nguyên nhân: 10	Có dấu hiệu tấn công đa lớp: 20	Liên quan nhiều tầng (ứng dụng, mạng, API): 25
3	Mức độ sẵn sàng của công cụ ứng cứu (SIEM, SOAR, WAF, EDR)	20	Có hệ thống tự động hóa hoàn chỉnh: 5	Có bán tự động (SOAR bán phần): 10	Chủ yếu thủ công: 20
4	Quy mô đội ngũ và quy trình phối hợp	15	Có quy trình, đội chuyên trách: 5	Có quy trình bán chính thức: 10	Chưa có quy trình, phối hợp thủ công: 15

Phân loại khó khăn

STT	**Mức độ khó khăn**	**Khoảng điểm (K)**
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

Bảng số 01:

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Giới hạn tốc độ, tạm khóa tài khoản, reset mật khẩu	1	1		2
2	Vá nóng (hotfix), cập nhật chữ ký WAF, chặn IP/ASN tấn công		2	1	3
3	Thông báo sự cố và ghi nhận bằng chứng phục vụ điều tra		2		2

1.4. Định mức

Bảng số 02:

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Giới hạn tốc độ, tạm khóa tài khoản, reset mật khẩu	Ứng dụng	1,2	1,8	2,6
2	Vá nóng (hotfix), cập nhật chữ ký WAF, chặn IP/ASN tấn công	Ứng dụng	1,6	2,4	3,2
3	Thông báo sự cố và ghi nhận bằng chứng phục vụ điều tra	Sự cố	1,4	2,0	2,8

2. Định mức thiết bị

Ca/01 Ứng dụng

STT	Thiết bị	ĐVT	Công suất (Kw)	Giới hạn tốc độ, tạm khóa tài khoản, reset mật khẩu	Vá nóng (hotfix), cập nhật chữ ký WAF, chặn IP/ASN tấn công	Thông báo sự cố và ghi nhận bằng chứng phục vụ điều tra
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,6
2	Máy in laser	Cái	0,6	0	0,053	0,053
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,101
4	Điện năng	Kw		1,3	6,2	4,2

3. Định mức dụng cụ

Ca/01 Ứng dụng

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Giới hạn tốc độ, tạm khóa tài khoản, reset mật khẩu	Vá nóng (hotfix), cập nhật chữ ký WAF, chặn IP/ASN tấn công	Thông báo sự cố và ghi nhận bằng chứng phục vụ điều tra
1	Ghế	Cái	96	0,2	1,2	0,6
2	Bàn làm việc	Cái	96	0,2	1,2	0,6
3	Quạt trần	Cái	96	0,035	0,21	0,105
4	Đèn neon	Bộ	24	0,1	0,6	0,3
5	Điện năng	kW		0,06	0,38	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Giới hạn tốc độ, tạm khóa tài khoản, reset mật khẩu	Vá nóng (hotfix), cập nhật chữ ký WAF, chặn IP/ASN tấn công	Thông báo sự cố và ghi nhận bằng chứng phục vụ điều tra
1	Giấy in A4	Gram		0,015	0,003
2	Mực in laser	Hộp		0,015	0,003

V. Bảo mật dữ liệu log

1. Định mức lao động

1.1. Nội dung công việc

a) Che giấu hoặc ẩn danh dữ liệu cá nhân (PII) trong log.

b) Mã hóa log khi lưu trữ, kiểm soát quyền truy cập và chính sách lưu giữ.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	**Các yếu tố ảnh hưởng**	**Điểm tối đa**	**Mức thấp**	**Mức trung bình**	**Mức cao**
1	Số lượng nguồn log cần xử lý	40	≤5 nguồn: 10	6–15 nguồn: 25	>15 nguồn: 40
2	Mức độ nhạy cảm của dữ liệu log (PII, tài chính, giao dịch)	25	Chủ yếu dữ liệu kỹ thuật: 10	Có dữ liệu người dùng/PII: 20	Bao gồm dữ liệu nhạy cảm nhiều loại: 25

3	Mức độ tự động hóa công cụ xử lý log (SIEM, DLP, Masking Tool)	20	Có công cụ tự động đầy đủ: 5	Có công cụ bán tự động: 10	Xử lý thủ công: 20
4	Chính sách kiểm soát truy cập và lưu giữ log	15	Có chính sách, phân quyền rõ ràng: 5	Có nhưng chưa đồng bộ: 10	Chưa có hoặc quản lý thủ công: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Che giấu hoặc ẩn danh dữ liệu cá nhân (PII) trong log	1	1		2
2	Mã hóa log khi lưu trữ, kiểm soát quyền truy cập và chính sách lưu giữ		2	1	3

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Che giấu hoặc ẩn danh dữ liệu cá nhân (PII) trong log	Hệ thống	1,4	2,0	2,8
2	Mã hóa log khi lưu trữ, kiểm soát quyền truy cập và chính sách lưu giữ	Hệ thống	1,8	2,6	3,6

2. Định mức thiết bị

Ca/01 hệ thống

STT	Thiết bị	ĐVT	Công suất (Kw)	Che giấu hoặc ẩn danh dữ liệu cá nhân (PII) trong log	Mã hóa log khi lưu trữ, kiểm soát quyền truy cập và chính sách lưu giữ
1	Máy tính để bàn	Cái	0,4	0,1	0,6
2	Máy in laser	Cái	0,6	0	0

3	Điều hoà nhiệt độ	Cái	2,2	0,02	0,05
4	Điện năng	Kw		0,6	2,9

3. Định mức dụng cụ

Ca/01 hệ thống

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Che giấu hoặc ẩn danh dữ liệu cá nhân (PII) trong log	Mã hóa log khi lưu trữ, kiểm soát quyền truy cập và chính sách lưu giữ
1	Ghế	Cái	96	0,1	0,6
2	Bàn làm việc	Cái	96	0,1	0,6
3	Quạt trần	Cái	96	0,02	0,11
4	Đèn neon	Bộ	24	0,05	0,3
5	Điện năng	kW		0,03	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Ghi nhận sự cố	Che giấu hoặc ẩn danh dữ liệu cá nhân (PII) trong log	Mã hóa log khi lưu trữ, kiểm soát quyền truy cập và chính sách lưu giữ
1	Giấy in A4	Gram	0	0	0,02
2	Mực in laser	Hộp	0	0	0,003

VI. Đánh giá và cải tiến

1. Định mức lao động

1.1. Nội dung công việc

a) Kiểm thử xâm nhập định kỳ, rà soát quy tắc WAF và API policy.

b) Cập nhật baseline an toàn ứng dụng và đào tạo đội ngũ vận hành.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	**Các yếu tố ảnh hưởng**	**Điểm tối đa**	**Mức thấp**	**Mức trung bình**	**Mức cao**
1	Số lượng ứng dụng, API, hoặc dịch vụ cần kiểm thử	40	≤5: 10	6–15: 25	>15: 40
2	Mức độ phức tạp của hệ thống (liên kết SSO, tích hợp bên thứ ba, multi-tenant)	25	Độc lập, không tích hợp: 10	Có tích hợp nội bộ: 20	Liên kết nhiều hệ thống ngoài: 25

3	Mức độ trưởng thành của chính sách WAF và baseline an toàn	20	Có sẵn baseline chuẩn, cập nhật định kỳ: 5	Có baseline nhưng chưa cập nhật thường xuyên: 10	Chưa có baseline, cần xây dựng mới: 20
4	Mức độ sẵn sàng và năng lực đội ngũ vận hành	15	Có đội chuyên trách, được đào tạo đầy đủ: 5	Có kinh nghiệm cơ bản: 10	Cần đào tạo hoặc hỗ trợ bên ngoài: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Kiểm thử xâm nhập định kỳ, rà soát quy tắc WAF và API policy		2	1	3
2	Cập nhật baseline an toàn ứng dụng và đào tạo đội ngũ vận hành	1	1		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Kiểm thử xâm nhập định kỳ, rà soát quy tắc WAF và API policy	Ứng dụng	2,0	2,8	3,8
2	Cập nhật baseline an toàn ứng dụng và đào tạo đội ngũ vận hành	Hệ thống	1,4	2,0	2,8

2. Định mức thiết bị

Ca/01 hệ thống

STT	Thiết bị	ĐVT	Công suất (Kw)	Kiểm thử xâm nhập định kỳ, rà soát quy tắc WAF và API policy	Cập nhật baseline an toàn ứng dụng và đào tạo đội ngũ vận hành
1	Máy tính để bàn	Cái	0,4	0,1	0,6
2	Máy in laser	Cái	0,6	0	0
3	Điều hoà nhiệt độ	Cái	2,2	0,02	0,05
4	Điện năng	Kw		0,6	2,9

3. Định mức dụng cụ

Ca/01 hệ thống

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Kiểm thử xâm nhập định kỳ, rà soát quy tắc WAF và API policy	Cập nhật baseline an toàn ứng dụng và đào tạo đội ngũ vận hành
1	Ghế	Cái	96	0,1	0,6
2	Bàn làm việc	Cái	96	0,1	0,6
3	Quạt trần	Cái	96	0,02	0,11
4	Đèn neon	Bộ	24	0,05	0,3
5	Điện năng	kW		0,03	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Ghi nhận sự cố	Kiểm thử xâm nhập định kỳ, rà soát quy tắc WAF và API policy	Cập nhật baseline an toàn ứng dụng và đào tạo đội ngũ vận hành
1	Giấy in A4	Gram	0	0	0,02
2	Mực in laser	Hộp	0	0	0,003

CHƯƠNG V
ĐỊNH MỨC GIÁM SÁT ĐẢM BẢO AN TOÀN THÔNG TIN CHO CƠ SỞ DỮ LIỆU

I. Chuẩn bị và thiết lập

1. Định mức lao động

1.1. Nội dung công việc

a) Kiểm kê hệ quản trị cơ sở dữ liệu (DBMS), phiên bản, vai trò, và người quản trị.

b) Bật audit log, query log, slow query log.

c) Cấu hình giám sát kết nối, phân quyền, thay đổi cấu trúc bảng/lược đồ.

d) Áp dụng hardening theo chuẩn CIS/OWASP Database Security.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng cơ sở dữ liệu giám sát	40	≤5: 10	6–20: 25	>20: 40
2	Mức độ phân tán hệ thống (các máy chủ DB)	20	Tập trung 1 máy chủ: 5	2–3 máy chủ: 10	Phân tán nhiều vùng/cluster/ cloud: 20
3	Mức độ tùy biến chính sách bảo mật DB	25	Áp dụng chuẩn CIS/OWASP gốc: 5	Có điều chỉnh nhẹ: 15	Chính sách riêng biệt theo từng DB: 25
4	Mức độ tích hợp giám sát với SIEM/log tập trung	15	Có sẵn SIEM/log tập trung: 5	Có log forwarding riêng lẻ: 10	Chưa có, cần triển khai mới: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Kiểm kê hệ quản trị cơ sở dữ liệu (DBMS), phiên bản, vai trò, và người quản trị	1	1		2
2	Bật audit log, query log, slow query log		2		2
3	Cấu hình giám sát kết nối, phân quyền, thay đổi cấu trúc bảng/lược đồ		2	1	3
4	Áp dụng hardening theo chuẩn CIS/OWASP Database Security		1	1	2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Kiểm kê hệ quản trị cơ sở dữ liệu (DBMS), phiên bản, vai trò, và người quản trị	CSDL	1,4	1,9	2,5
2	Bật audit log, query log, slow query log	CSDL	1,6	2,2	3,0
3	Cấu hình giám sát kết nối, phân quyền, thay đổi cấu trúc bảng/lược đồ	CSDL	1,8	2,5	3,5
4	Áp dụng hardening theo chuẩn CIS/OWASP Database Security	CSDL	2,0	2,8	3,8

2. Định mức thiết bị

Ca/01 CSDL

STT	Thiết bị	ĐVT	Công suất (Kw)	Kiểm kê hệ quản trị cơ sở dữ liệu (DBMS), phiên bản, vai trò, và người quản trị	Bật audit log, query log, slow query log	Cấu hình giám sát kết nối, phân quyền, thay đổi cấu trúc bảng/lược đồ	Áp dụng hardening theo chuẩn CIS/OWASP Database Security
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,1	0,05
2	Máy in laser	Cái	0,6	0,018	0	0	0,004
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,017	0,008
4	Điện năng	Kw		1,409	5,889	0,646	0,352

3. Định mức dụng cụ

Ca/01 CSDL

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Kiểm kê hệ quản trị cơ sở dữ liệu (DBMS), phiên bản, vai trò, và người quản trị	Bật audit log, query log, slow query log	Cấu hình giám sát kết nối, phân quyền, thay đổi cấu trúc bảng/lược đồ	Áp dụng hardening theo chuẩn CIS/OWASP Database Security
1	Ghế	Cái	96	0,2	1,2	0,1	0,05
2	Bàn làm việc	Cái	96	0,2	1,2	0,1	0,05
3	Quạt trần	Cái	96	0,035	0,21	0,02	0,018
4	Đèn neon	Bộ	24	0,1	0,6	0,05	0,025
5	Điện năng	kW		0,063	0,378	0,032	0,016

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Kiểm kê hệ quản trị cơ sở dữ liệu (DBMS), phiên bản, vai trò, và người quản trị	Bật audit log, query log, slow query log	Cấu hình giám sát kết nối, phân quyền, thay đổi cấu trúc bảng/lược đồ	Áp dụng hardening theo chuẩn CIS/OWASP Database Security
1	Giấy in A4	Gram	0,015	0	0	0,015
2	Mực in laser	Hộp	0,003	0	0	0,003

II. Thu thập và giám sát

1. Định mức lao động

1.1. Nội dung công việc

a) Thu thập log truy cập, đăng nhập, truy vấn lỗi, hành vi thao tác dữ liệu (INSERT/UPDATE/DELETE).

b) Giám sát thay đổi quyền truy cập, tạo tài khoản mới, hoặc cấp quyền DBA.

c) Theo dõi hiệu năng DB: CPU, I/O, deadlock, kết nối bất thường.

d) Giám sát backup/restore, lịch trình và trạng thái sao lưu.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng cơ sở dữ liệu cần giám sát	40	≤5: 10	6–20: 25	>20: 40
2	Mức độ phân tán của hệ thống log (máy chủ, node, cluster)	20	Tập trung 1 máy chủ: 5	2–3 node: 10	Nhiều node/cluster/cloud: 20
3	Mức độ phức tạp của cấu trúc log và sự kiện giám sát	25	Log tiêu chuẩn dễ phân tách: 5	Có nhiều định dạng khác nhau: 15	Log không chuẩn, nhiều hệ DB: 25
4	Tích hợp với hệ thống SIEM hoặc công cụ phân tích tập trung	15	Có sẵn tích hợp SIEM: 5	Có log forwarding riêng lẻ: 10	Chưa có, cần triển khai mới: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Thu thập log truy cập, đăng nhập, truy vấn lỗi, hành vi thao tác dữ liệu (INSERT/UPDATE/DELETE)	1	1		2
2	Giám sát thay đổi quyền truy cập, tạo tài khoản mới, hoặc cấp quyền DBA		2	1	3
3	Theo dõi hiệu năng DB: CPU, I/O, deadlock, kết nối bất thường		2		2
4	Giám sát backup/restore, lịch trình và trạng thái sao lưu		1	1	2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Thu thập log truy cập, đăng nhập, truy vấn lỗi, hành vi thao tác dữ liệu (INSERT/UPDATE/DELETE)	CSDL	1,5	2,1	2,8

2	Giám sát thay đổi quyền truy cập, tạo tài khoản mới, hoặc cấp quyền DBA	CSDL	1,8	2,5	3,4
3	Theo dõi hiệu năng DB: CPU, I/O, deadlock, kết nối bất thường	CSDL	1,6	2,3	3,0
4	Giám sát backup/restore, lịch trình và trạng thái sao lưu	CSDL	1,4	2,0	2,7

2. Định mức thiết bị

Ca/01 CSDL

STT	Thiết bị	ĐVT	Công suất (Kw)	Thu thập log truy cập, đăng nhập, truy vấn lỗi, hành vi thao tác dữ liệu (INSERT/UPDATE/DELETE)	Giám sát thay đổi quyền truy cập, tạo tài khoản mới, hoặc cấp quyền DBA	Theo dõi hiệu năng DB: CPU, I/O, deadlock, kết nối bất thường	Giám sát backup/restore, lịch trình và trạng thái sao lưu
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,1	0,05
2	Máy in laser	Cái	0,6	0,018	0	0	0,004
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,017	0,008
4	Điện năng	Kw		1,409	5,889	0,646	0,352

3. Định mức dụng cụ

Ca/01 CSDL

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Thu thập log truy cập, đăng nhập, truy vấn lỗi, hành vi thao tác dữ liệu (INSERT/UPDATE/DELETE)	Giám sát thay đổi quyền truy cập, tạo tài khoản mới, hoặc cấp quyền DBA	Theo dõi hiệu năng DB: CPU, I/O, deadlock, kết nối bất thường	Giám sát backup/restore, lịch trình và trạng thái sao lưu
1	Ghế	Cái	96	0,2	1,2	0,1	0,05
2	Bàn làm việc	Cái	96	0,2	1,2	0,1	0,05
3	Quạt trần	Cái	96	0,035	0,21	0,02	0,018
4	Đèn neon	Bộ	24	0,1	0,6	0,05	0,025
5	Điện năng	kW		0,063	0,378	0,032	0,016

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Thu thập log truy cập, đăng nhập, truy vấn lỗi, hành vi thao tác dữ liệu (INSERT/UPDATE/DELETE)	Giám sát thay đổi quyền truy cập, tạo tài khoản mới, hoặc cấp quyền DBA	Theo dõi hiệu năng DB: CPU, I/O, deadlock, kết nối bất thường	Giám sát backup/restore, lịch trình và trạng thái sao lưu
1	Giấy in A4	Gram	0,015	0	0	0,015
2	Mực in laser	Hộp	0,003	0	0	0,003

III. Phân tích và tương quan

1. Định mức lao động

1.1. Nội dung công việc

a) Tương quan các hành vi bất thường: DROP table + đăng nhập ngoài giờ + truy cập từ IP lạ.

b) Phát hiện truy vấn khối lượng lớn hoặc quét dữ liệu nhạy cảm (data exfiltration).

c) Đối chiếu nhật ký DB với log ứng dụng và hệ điều hành để xác minh hành vi.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng cơ sở dữ liệu và nguồn log cần tương quan	40	≤5: 10	6–20: 25	>20: 40
2	Mức độ phức tạp của mô hình hành vi và quy tắc tương quan	25	Quy tắc tĩnh, mẫu cố định: 5	Có kết hợp 2–3 điều kiện: 15	Nhiều điều kiện động, AI/ML hỗ trợ: 25
3	Tích hợp và đồng bộ dữ liệu log từ nhiều hệ thống (DB, OS, App)	20	Đã tích hợp sẵn SIEM: 5	Log forwarding riêng lẻ: 10	Chưa có, phải thiết lập tương quan mới: 20
4	Mức độ yêu cầu xác minh và đối chiếu thủ công	15	Có công cụ hỗ trợ phân tích tự động: 5	Bán tự động: 10	Thủ công hoàn toàn: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

STT	Danh mục công việc	KS3	KS4	Nhóm
1	Tương quan các hành vi bất thường: DROP table + đăng nhập ngoài giờ + truy cập từ IP lạ	2	1	3
2	Phát hiện truy vấn khối lượng lớn hoặc quét dữ liệu nhạy cảm (data exfiltration)	1	1	2
3	Đối chiếu nhật ký DB với log ứng dụng và hệ điều hành để xác minh hành vi	2		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Tương quan các hành vi bất thường: DROP table + đăng nhập ngoài giờ + truy cập từ IP lạ	CSDL	1,8	2,6	3,6
2	Phát hiện truy vấn khối lượng lớn hoặc quét dữ liệu nhạy cảm (data exfiltration)	CSDL	1,6	2,3	3,2
3	Đối chiếu nhật ký DB với log ứng dụng và hệ điều hành để xác minh hành vi	CSDL	1,9	2,7	3,8

2. Định mức thiết bị

Ca/01 CSDL

STT	Thiết bị	ĐVT	Công suất (Kw)	Tương quan các hành vi bất thường: DROP table + đăng nhập ngoài giờ + truy cập từ IP lạ	Phát hiện truy vấn khối lượng lớn hoặc quét dữ liệu nhạy cảm (data exfiltration)	Đối chiếu nhật ký DB với log ứng dụng và hệ điều hành để xác minh hành vi
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,6
2	Máy in laser	Cái	0,6	0	0,053	0,053
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,101
4	Điện năng	Kw		1,3	6,2	4,2

3. Định mức dụng cụ

Ca/01 CSDL

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Tương quan các hành vi bất thường: DROP table + đăng nhập ngoài giờ + truy cập từ IP lạ	Phát hiện truy vấn khối lượng lớn hoặc quét dữ liệu nhạy cảm (data exfiltration)	Đối chiếu nhật ký DB với log ứng dụng và hệ điều hành để xác minh hành vi
1	Ghế	Cái	96	0,2	1,2	0,6
2	Bàn làm việc	Cái	96	0,2	1,2	0,6
3	Quạt trần	Cái	96	0,035	0,21	0,105
4	Đèn neon	Bộ	24	0,1	0,6	0,3
5	Điện năng	kW		0,06	0,38	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Tương quan các hành vi bất thường: DROP table + đăng nhập ngoài giờ + truy cập từ IP lạ	Phát hiện truy vấn khối lượng lớn hoặc quét dữ liệu nhạy cảm (data exfiltration)	Đối chiếu nhật ký DB với log ứng dụng và hệ điều hành để xác minh hành vi
1	Giấy in A4	Gram		0,015	0,003
2	Mực in laser	Hộp		0,015	0,003

IV. Ứng cứu ban đầu

1. Định mức lao động

1.1. Nội dung công việc

a) Cô lập tài khoản nghi ngờ, thu hồi quyền truy cập, khóa session đang hoạt động.

b) Khôi phục dữ liệu từ bản sao lưu, ghi nhận log phục vụ điều tra.

c) Vá lỗi hoặc điều chỉnh cấu hình bảo mật (role, GRANT/REVOKE).

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng cơ sở dữ liệu cần xử lý hoặc khôi phục	40	≤3: 10	4–10: 25	>10: 40
2	Mức độ ảnh hưởng và phạm vi sự cố	25	Sự cố cục bộ (1 DB): 5	Ảnh hưởng nhóm DB hoặc máy chủ: 15	Ảnh hưởng hệ thống diện rộng: 25
3	Mức độ sẵn sàng của bản sao lưu và tài nguyên khôi phục	20	Sao lưu định kỳ, sẵn sàng: 5	Sao lưu không đầy đủ: 10	Thiếu bản sao lưu, cần phục hồi phức tạp: 20
4	Mức độ phức tạp của biện pháp khắc phục (vá lỗi, cấu hình bảo mật)	15	Thực hiện qua công cụ/GUI: 5	Kết hợp thủ công và script: 10	Toàn bộ thủ công, yêu cầu phân tích sâu: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS3	KS4	Nhóm
1	Cô lập tài khoản nghi ngờ, thu hồi quyền truy cập, khóa session đang hoạt động	2	1	3
2	Khôi phục dữ liệu từ bản sao lưu, ghi nhận log phục vụ điều tra	1	1	2
3	Vá lỗi hoặc điều chỉnh cấu hình bảo mật (role, GRANT/REVOKE)	2		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Cô lập tài khoản nghi ngờ, thu hồi quyền truy cập, khóa session đang hoạt động	CSDL	1,7	2,4	3,3
2	Khôi phục dữ liệu từ bản sao lưu, ghi nhận log phục vụ điều tra	CSDL	1,9	2,7	3,8
3	Vá lỗi hoặc điều chỉnh cấu hình bảo mật (role, GRANT/REVOKE)	CSDL	1,6	2,3	3,2

2. Định mức thiết bị

Ca/01 CSDL

STT	Thiết bị	ĐVT	Công suất (Kw)	Cô lập tài khoản nghi ngờ, thu hồi quyền truy cập, khóa session đang hoạt động	Khôi phục dữ liệu từ bản sao lưu, ghi nhận log phục vụ điều tra	Vá lỗi hoặc điều chỉnh cấu hình bảo mật (role, GRANT/ REVOKE)
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,6
2	Máy in laser	Cái	0,6	0	0,053	0,053
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,101
4	Điện năng	Kw		1,3	6,2	4,2

3. Định mức dụng cụ

Ca/01 CSDL

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Cô lập tài khoản nghi ngờ, thu hồi quyền truy cập, khóa session đang hoạt động	Khôi phục dữ liệu từ bản sao lưu, ghi nhận log phục vụ điều tra	Vá lỗi hoặc điều chỉnh cấu hình bảo mật (role, GRANT/REVOKE)
1	Ghế	Cái	96	0,2	1,2	0,6
2	Bàn làm việc	Cái	96	0,2	1,2	0,6
3	Quạt trần	Cái	96	0,035	0,21	0,105
4	Đèn neon	Bộ	24	0,1	0,6	0,3
5	Điện năng	kW		0,06	0,38	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Cô lập tài khoản nghi ngờ, thu hồi quyền truy cập, khóa session đang hoạt động	Khôi phục dữ liệu từ bản sao lưu, ghi nhận log phục vụ điều tra	Vá lỗi hoặc điều chỉnh cấu hình bảo mật (role, GRANT/REVOKE)
1	Giấy in A4	Gram		0,015	0,003
2	Mực in laser	Hộp		0,015	0,003

V. Bảo mật dữ liệu và log

1. Định mức lao động

1.1. Nội dung công việc

a) Mã hóa dữ liệu nhạy cảm (at rest, in transit), ẩn danh dữ liệu khi test.

b) Mã hóa log, kiểm soát quyền truy cập, lưu trữ an toàn và tuân thủ chính sách retention.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng cơ sở dữ liệu giám sát	40	≤5: 10	6–20: 25	>20: 40
2	Mức độ phân tán hệ thống CSDL	20	Tập trung 1 cụm: 5	2–3 cụm vùng mạng: 10	Nhiều vùng/DMZ/cloud: 20
3	Mức độ áp dụng cơ chế mã hóa và ẩn danh	25	Sử dụng sẵn tính năng DBMS: 5	Có điều chỉnh, script bổ trợ: 15	Tùy biến nhiều mức, có lớp trung gian: 25
4	Mức độ tích hợp và kiểm soát log tập trung	15	Có sẵn hệ thống log tập trung: 5	Có log riêng rẽ từng DB: 10	Phải triển khai mới hoặc hợp nhất log: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Mã hóa dữ liệu nhạy cảm (at rest, in transit), ẩn danh dữ liệu khi test	1	1		2
2	Mã hóa log, kiểm soát quyền truy cập, lưu trữ an toàn và tuân thủ chính sách retention		2	1	3

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Mã hóa dữ liệu nhạy cảm (at rest, in transit), ẩn danh dữ liệu khi test	CSDL	1,8	2,4	3,4
2	Mã hóa log, kiểm soát quyền truy cập, lưu trữ an toàn và tuân thủ chính sách retention	CSDL	1,6	2,2	3,0

2. Định mức thiết bị

Ca/01 CSDL

STT	Thiết bị	ĐVT	Công suất (Kw)	Mã hóa dữ liệu nhạy cảm (at rest, in transit), ẩn danh dữ liệu khi test	Mã hóa log, kiểm soát quyền truy cập, lưu trữ an toàn và tuân thủ chính sách retention
1	Máy tính để bàn	Cái	0,4	0,2	1,2
2	Máy in laser	Cái	0,6	0	0,053
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101
4	Điện năng	Kw		1,3	6,2

3. Định mức dụng cụ

Ca/01 CSDL

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Mã hóa dữ liệu nhạy cảm (at rest, in transit), ẩn danh dữ liệu khi test	Mã hóa log, kiểm soát quyền truy cập, lưu trữ an toàn và tuân thủ chính sách retention
1	Ghế	Cái	96	0,2	1,2
2	Bàn làm việc	Cái	96	0,2	1,2

3	Quạt trần	Cái	96	0,035	0,21
4	Đèn neon	Bộ	24	0,1	0,6
5	Điện năng	kW		0,06	0,38

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Mã hóa dữ liệu nhạy cảm (at rest, in transit), ẩn danh dữ liệu khi test	Mã hóa log, kiểm soát quyền truy cập, lưu trữ an toàn và tuân thủ chính sách retention
1	Giấy in A4	Gram		0,015
2	Mực in laser	Hộp		0,015

VI. Đánh giá và cải tiến

1. Định mức lao động

1.1. Nội dung công việc

a) Rà soát quyền tài khoản, kiểm tra chính sách backup và mã hóa định kỳ.

b) Kiểm thử xâm nhập database, cập nhật baseline bảo mật.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng cơ sở dữ liệu cần đánh giá định kỳ	40	≤5: 10	6–20: 25	>20: 40
2	Mức độ phân tán hệ thống cơ sở dữ liệu	20	Cùng mạng nội bộ: 5	2–3 mạng con: 10	Nhiều vùng/DMZ/cloud: 20
3	Mức độ phức tạp của quyền truy cập và chính sách backup	25	Quyền đơn giản, backup tập trung: 5	Có phân quyền chi tiết, backup theo nhóm: 15	Nhiều tầng quyền, backup độc lập: 25
4	Mức độ tích hợp và tự động hóa kiểm thử/baseline	15	Có công cụ tự động định kỳ: 5	Kiểm thử bán tự động: 10	Kiểm thử thủ công, cập nhật baseline thủ công: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Rà soát quyền tài khoản, kiểm tra chính sách backup và mã hóa định kỳ	1	1		2
2	Kiểm thử xâm nhập database, cập nhật baseline bảo mật		2	1	3

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Rà soát quyền tài khoản, kiểm tra chính sách backup và mã hóa định kỳ	CSDL	1,6	2,2	3,0
2	Kiểm thử xâm nhập database, cập nhật baseline bảo mật	CSDL	1,8	2,6	3,6

2. Định mức thiết bị

Ca/01 CSDL

STT	Thiết bị	ĐVT	Công suất (Kw)	Rà soát quyền tài khoản, kiểm tra chính sách backup và mã hóa định kỳ	Kiểm thử xâm nhập database, cập nhật baseline bảo mật
1	Máy tính để bàn	Cái	0,4	0,2	1,2
2	Máy in laser	Cái	0,6	0	0,053
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101
4	Điện năng	Kw		1,3	6,2

3. Định mức dụng cụ

Ca/01 CSDL

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Rà soát quyền tài khoản, kiểm tra chính sách backup và mã hóa định kỳ	Kiểm thử xâm nhập database, cập nhật baseline bảo mật
1	Ghế	Cái	96	0,2	1,2
2	Bàn làm việc	Cái	96	0,2	1,2
3	Quạt trần	Cái	96	0,035	0,21
4	Đèn neon	Bộ	24	0,1	0,6
5	Điện năng	kW		0,06	0,38

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Rà soát quyền tài khoản, kiểm tra chính sách backup và mã hóa định kỳ	Kiểm thử xâm nhập database, cập nhật baseline bảo mật
1	Giấy in A4	Gram		0,015
2	Mực in laser	Hộp		0,015

CHƯƠNG VI
ĐỊNH MỨC GIÁM SÁT ĐẢM BẢO AN TOÀN THÔNG TIN CHO NGƯỜI DÙNG

I. Chuẩn bị và thiết lập

1. Định mức lao động

1.1. Nội dung công việc

a) Kiểm kê danh sách tài khoản người dùng, vai trò, nhóm, và các đặc quyền.

b) Thiết lập hệ thống quản lý danh tính và truy cập (IAM) và bật audit log cho các sự kiện xác thực (Active Directory/SSO).

c) Cấu hình giám sát truy cập từ xa (VPN, VDI) và các dịch vụ chia sẻ tài nguyên.

d) Áp dụng chính sách mật khẩu và xác thực đa yếu tố (MFA).

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng tài khoản người dùng trong hệ thống	40	≤200: 10	201–1000: 25	>1000: 40
2	Mức độ phân tán hệ thống xác thực (AD, LDAP, SSO, Cloud IAM)	20	1 hệ thống tập trung: 5	2–3 hệ thống: 10	>3 hệ thống hoặc đa môi trường (cloud + on-prem): 20
3	Mức độ tích hợp và tự động hóa IAM/audit	25	Có sẵn IAM và log tập trung: 5	Có công cụ quản lý rời rạc: 15	Chưa có hệ thống, cần triển khai mới: 25
4	Mức độ phức tạp của cơ chế xác thực (MFA, VPN, VDI, chia sẻ tài nguyên)	15	Xác thực 1 lớp: 5	Có MFA và VPN: 10	Nhiều lớp (MFA, VPN, VDI, federated login): 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Kiểm kê danh sách tài khoản người dùng, vai trò, nhóm, và các đặc quyền	1	1		2
2	Thiết lập hệ thống quản lý danh tính và truy cập (IAM) và bật audit log cho các sự kiện xác thực (Active Directory/SSO)		2	1	3
3	Cấu hình giám sát truy cập từ xa (VPN, VDI) và các dịch vụ chia sẻ tài nguyên		2		2
4	Áp dụng chính sách mật khẩu và xác thực đa yếu tố (MFA)	1	1		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Kiểm kê danh sách tài khoản người dùng, vai trò, nhóm, và các đặc quyền	100 tài khoản	1,2	1,6	2,2
2	Thiết lập hệ thống quản lý danh tính và truy cập (IAM) và bật audit log cho các sự kiện xác thực (Active Directory/SSO)	Hệ thống	1,8	2,6	3,6
3	Cấu hình giám sát truy cập từ xa (VPN, VDI) và các dịch vụ chia sẻ tài nguyên	Hệ thống	1,6	2,2	3,0
4	Áp dụng chính sách mật khẩu và xác thực đa yếu tố (MFA)	Chính sách	1,4	2,0	2,8

2. Định mức thiết bị

Ca/01 hệ thống

STT	Thiết bị	ĐVT	Công suất (Kw)	Kiểm kê danh sách tài khoản người dùng, vai trò, nhóm, và các đặc quyền	Thiết lập hệ thống quản lý danh tính và truy cập (IAM) và bật audit log cho các sự kiện xác thực (Active Directory/SSO)	Cấu hình giám sát truy cập từ xa (VPN, VDI) và các dịch vụ chia sẻ tài nguyên	Áp dụng chính sách mật khẩu và xác thực đa yếu tố (MFA)
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,1	0,05
2	Máy in laser	Cái	0,6	0,018	0	0	0,004
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,017	0,008
4	Điện năng	Kw		1,409	5,889	0,646	0,352

3. Định mức dụng cụ

Ca/01 hệ thống

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Kiểm kê danh sách tài khoản người dùng, vai trò, nhóm, và các đặc quyền	Thiết lập hệ thống quản lý danh tính và truy cập (IAM) và bật audit log cho các sự kiện xác thực (Active Directory/SSO)	Cấu hình giám sát truy cập từ xa (VPN, VDI) và các dịch vụ chia sẻ tài nguyên	Áp dụng chính sách mật khẩu và xác thực đa yếu tố (MFA)
1	Ghế	Cái	96	0,2	1,2	0,1	0,05
2	Bàn làm việc	Cái	96	0,2	1,2	0,1	0,05
3	Quạt trần	Cái	96	0,035	0,21	0,02	0,018
4	Đèn neon	Bộ	24	0,1	0,6	0,05	0,025
5	Điện năng	kW		0,063	0,378	0,032	0,016

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Kiểm kê danh sách tài khoản người dùng, vai trò, nhóm, và các đặc quyền	Thiết lập hệ thống quản lý danh tính và truy cập (IAM) và bật audit log cho các sự kiện xác thực (Active Directory/SSO)	Cấu hình giám sát truy cập từ xa (VPN, VDI) và các dịch vụ chia sẻ tài nguyên	Áp dụng chính sách mật khẩu và xác thực đa yếu tố (MFA)
1	Giấy in A4	Gram	0,015	0	0	0,015
2	Mực in laser	Hộp	0,003	0	0	0,003

II. Thu thập và giám sát

1. Định mức lao động

1.1. Nội dung công việc

a) Thu thập log đăng nhập/đăng xuất thành công/thất bại, thay đổi mật khẩu, thay đổi vai trò.

b) Giám sát đăng nhập bất thường (từ IP lạ, ngoài giờ hành chính, tốc độ di chuyển không thể lý giải).

c) Giám sát hành vi người dùng đặc quyền (Admin, Root, DBA) trong

việc truy cập tài nguyên.

d) Thu thập log truy cập vào dữ liệu nhạy cảm (qua DLP, file share audit).

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng người dùng cần giám sát	40	≤200: 10	201–1000: 25	>1000: 40
2	Mức độ đa dạng nguồn log (AD, VPN, DLP, ứng dụng nội bộ, SSO, file server)	20	1–2 nguồn: 5	3–4 nguồn: 10	≥5 nguồn hoặc tích hợp SIEM phức tạp: 20
3	Mức độ tự động hóa phân tích hành vi và cảnh báo	25	Có sẵn công cụ SIEM/Audit log tự động: 5	Bán tự động, có script kiểm tra định kỳ: 15	Thủ công, cần tổng hợp và phân tích log riêng lẻ: 25
4	Mức độ phức tạp của quyền truy cập và dữ liệu nhạy cảm	15	Dữ liệu phân cấp rõ ràng, ít nhóm đặc quyền: 5	Có nhiều nhóm và quyền tùy chỉnh: 10	Nhiều lớp quyền, chồng chéo, cần phân tích chi tiết: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Thu thập log đăng nhập/đăng xuất thành công/thất bại, thay đổi mật khẩu, thay đổi vai trò	1	1		2
2	Giám sát đăng nhập bất thường (từ IP lạ, ngoài giờ hành chính, tốc độ di chuyển không thể lý giải)		2		2

3	Giám sát hành vi người dùng đặc quyền (Admin, Root, DBA) trong việc truy cập tài nguyên		2	1	3
4	Thu thập log truy cập vào dữ liệu nhạy cảm (qua DLP, file share audit)	1	1		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Thu thập log đăng nhập/đăng xuất thành công/thất bại, thay đổi mật khẩu, thay đổi vai trò	100 tài khoản	1,4	1,8	2,6
2	Giám sát đăng nhập bất thường (từ IP lạ, ngoài giờ hành chính, tốc độ di chuyển không thể lý giải)	100 tài khoản	1,6	2,2	3,0
3	Giám sát hành vi người dùng đặc quyền (Admin, Root, DBA) trong việc truy cập tài nguyên	Người dùng đặc quyền	1,8	2,6	3,6
4	Thu thập log truy cập vào dữ liệu nhạy cảm (qua DLP, file share audit)	Hệ thống	1,6	2,4	3,4

2. Định mức thiết bị

Ca/01 hệ thống

STT	Thiết bị	ĐVT	Công suất (Kw)	Thu thập log đăng nhập/đăng xuất thành công/thất bại, thay đổi mật khẩu, thay đổi vai trò	Giám sát đăng nhập bất thường (từ IP lạ, ngoài giờ hành chính, tốc độ di chuyển không thể lý giải)	Giám sát hành vi người dùng đặc quyền (Admin, Root, DBA) trong việc truy cập tài nguyên	Thu thập log truy cập vào dữ liệu nhạy cảm (qua DLP, file share audit)
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,1	0,05
2	Máy in laser	Cái	0,6	0,018	0	0	0,004
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,017	0,008
4	Điện năng	Kw		1,409	5,889	0,646	0,352

3. Định mức dụng cụ

Ca/01 hệ thống

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Thu thập log đăng nhập/đăng xuất thành công/thất bại, thay đổi mật khẩu, thay đổi vai trò	Giám sát đăng nhập bất thường (từ IP lạ, ngoài giờ hành chính, tốc độ di chuyển không thể lý giải)	Giám sát hành vi người dùng đặc quyền (Admin, Root, DBA) trong việc truy cập tài nguyên	Thu thập log truy cập vào dữ liệu nhạy cảm (qua DLP, file share audit)
1	Ghế	Cái	96	0,2	1,2	0,1	0,05
2	Bàn làm việc	Cái	96	0,2	1,2	0,1	0,05
3	Quạt trần	Cái	96	0,035	0,21	0,02	0,018
4	Đèn neon	Bộ	24	0,1	0,6	0,05	0,025
5	Điện năng	kW		0,063	0,378	0,032	0,016

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Thu thập log đăng nhập/đăng xuất thành công/thất bại, thay đổi mật khẩu, thay đổi vai trò	Giám sát đăng nhập bất thường (từ IP lạ, ngoài giờ hành chính, tốc độ di chuyển không thể lý giải)	Giám sát hành vi người dùng đặc quyền (Admin, Root, DBA) trong việc truy cập tài nguyên	Thu thập log truy cập vào dữ liệu nhạy cảm (qua DLP, file share audit)
1	Giấy in A4	Gram	0,015	0	0	0,015
2	Mực in laser	Hộp	0,003	0	0	0,003

III. Phân tích và tương quan

1. Định mức lao động

1.1. Nội dung công việc

a) Xây dựng baseline hành vi cho từng nhóm người dùng (giờ làm việc, tài nguyên truy cập, khối lượng download/upload).

b) Tương quan đăng nhập thành công bất thường + truy cập tệp nhạy cảm + download khối lượng lớn → rò rỉ dữ liệu nội bộ.

c) Phân tích chuỗi sự kiện để phát hiện tấn công chiếm quyền tài khoản (account takeover).

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng người dùng và nhóm người dùng cần phân tích hành vi	40	≤200: 10	201–1000: 25	>1000: 40
2	Số lượng nguồn log và mức độ tương quan dữ liệu (SIEM, DLP, AD, VPN, File Server)	20	1–2 nguồn: 5	3–4 nguồn: 10	≥5 nguồn: 20
3	Mức độ tự động hóa phân tích và xây dựng baseline hành vi	25	Có công cụ phân tích sẵn (UEBA, SIEM): 5	Bán tự động, cần cấu hình thủ công: 15	Phân tích thủ công, không có công cụ: 25
4	Mức độ phức tạp trong mô hình tương quan sự kiện và phát hiện tấn công	15	Các mẫu tương quan đơn giản (2 điều kiện): 5	Trung bình (3–4 điều kiện, kết hợp log): 10	Nâng cao (đa chuỗi sự kiện, thời gian, IP, hành vi): 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

Bảng số 01:

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Xây dựng baseline hành vi cho từng nhóm người dùng (giờ làm việc, tài nguyên truy cập, khối lượng download/upload)	1	1		2
2	Tương quan đăng nhập thành công bất thường + truy cập tệp nhạy cảm + download khối lượng lớn → rò rỉ dữ liệu nội bộ		2	1	3
3	Phân tích chuỗi sự kiện để phát hiện tấn công chiếm quyền tài khoản (account takeover)		2	1	3

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Xây dựng baseline hành vi cho từng nhóm người dùng (giờ làm việc, tài nguyên truy cập, khối lượng download/upload)	Nhóm người dùng	1,6	2,2	3,2
2	Tương quan đăng nhập thành công bất thường + truy cập tệp nhạy cảm + download khối lượng lớn → rò rỉ dữ liệu nội bộ	Mô hình tương quan	1,8	2,6	3,6
3	Phân tích chuỗi sự kiện để phát hiện tấn công chiếm quyền tài khoản (account takeover)	Chuỗi sự kiện	2,0	2,8	3,8

2. Định mức thiết bị

Ca/01 Chuỗi sự kiện

STT	Thiết bị	ĐVT	Công suất (Kw)	Xây dựng baseline hành vi cho từng nhóm người dùng (giờ làm việc, tài nguyên truy cập, khối lượng download/upload)	Tương quan đăng nhập thành công bất thường + truy cập tệp nhạy cảm + download khối lượng lớn → rò rỉ dữ liệu nội bộ	Phân tích chuỗi sự kiện để phát hiện tấn công chiếm quyền tài khoản (account takeover)
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,6
2	Máy in laser	Cái	0,6	0	0,053	0,053
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,101
4	Điện năng	Kw		1,3	6,2	4,2

3. Định mức dụng cụ

Ca/01 Chuỗi sự kiện

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Xây dựng baseline hành vi cho từng nhóm người dùng (giờ làm việc, tài nguyên truy cập, khối lượng download/upload)	Tương quan đăng nhập thành công bất thường + truy cập tệp nhạy cảm + download khối lượng lớn → rò rỉ dữ liệu nội bộ	Phân tích chuỗi sự kiện để phát hiện tấn công chiếm quyền tài khoản (account takeover)
1	Ghế	Cái	96	0,2	1,2	0,6
2	Bàn làm việc	Cái	96	0,2	1,2	0,6
3	Quạt trần	Cái	96	0,035	0,21	0,105
4	Đèn neon	Bộ	24	0,1	0,6	0,3
5	Điện năng	kW		0,06	0,38	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Xây dựng baseline hành vi cho từng nhóm người dùng (giờ làm việc, tài nguyên truy cập, khối lượng download/upload)	Tương quan đăng nhập thành công bất thường + truy cập tệp nhạy cảm + download khối lượng lớn → rò rỉ dữ liệu nội bộ	Phân tích chuỗi sự kiện để phát hiện tấn công chiếm quyền tài khoản (account takeover)
1	Giấy in A4	Gram		0,015	0,003
2	Mực in laser	Hộp		0,015	0,003

IV. Ứng cứu ban đầu

1. Định mức lao động

1.1. Nội dung công việc

a) Vô hiệu hóa hoặc tạm khóa tài khoản bị chiếm quyền.

b) Buộc đăng xuất (force logoff) và reset mật khẩu cho người dùng.

c) Cô lập thiết bị đầu cuối của người dùng có hành vi bất thường.

d) Thông báo và phối hợp với phòng ban nhân sự/quản lý để xác minh.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng tài khoản và thiết bị cần ứng cứu	40	≤50: 10	51–200: 25	>200: 40
2	Mức độ phân tán người dùng và thiết bị (văn phòng, remote, VDI)	20	1–2 site: 5	3–5 site: 10	>5 site hoặc nhiều môi trường cloud: 20
3	Mức độ phức tạp trong quy trình phối hợp với các phòng ban	25	Phối hợp đơn giản, ít bước: 5	Trung bình, nhiều phòng ban: 15	Phức tạp, nhiều phòng ban và approval: 25
4	Mức độ nguy cơ và khối lượng dữ liệu/tài nguyên liên quan	15	Tài nguyên ít nhạy cảm: 5	Một số dữ liệu quan trọng: 10	Dữ liệu nhạy cảm hoặc nhiều hệ thống: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Vô hiệu hóa hoặc tạm khóa tài khoản bị chiếm quyền	1	1		2
2	Buộc đăng xuất (force logoff) và reset mật khẩu cho người dùng	1	1		2
3	Cô lập thiết bị đầu cuối của người dùng có hành vi bất thường		2	1	3
4	Thông báo và phối hợp với phòng ban nhân sự/quản lý để xác minh	1	1		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Vô hiệu hóa hoặc tạm khóa tài khoản bị chiếm quyền	Tài khoản	1,2	1,6	2,2
2	Buộc đăng xuất (force logoff) và reset mật khẩu cho người dùng	Tài khoản	1,4	2,0	2,8

3	Cô lập thiết bị đầu cuối của người dùng có hành vi bất thường	Thiết bị	1,6	2,4	3,2
4	Thông báo và phối hợp với phòng ban nhân sự/quản lý để xác minh	Trường hợp	1,0	1,6	2,2

2. Định mức thiết bị

Ca/01 thiết bị

STT	Thiết bị	ĐVT	Công suất (Kw)	Vô hiệu hóa hoặc tạm khóa tài khoản bị chiếm quyền	Buộc đăng xuất (force logoff) và reset mật khẩu cho người dùng	Cô lập thiết bị đầu cuối của người dùng có hành vi bất thường	Thông báo và phối hợp với phòng ban nhân sự/quản lý để xác minh
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,1	0,05
2	Máy in laser	Cái	0,6	0,018	0	0	0,004
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,017	0,008
4	Điện năng	Kw		1,409	5,889	0,646	0,352

3. Định mức dụng cụ

Ca/01 thiết bị

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Vô hiệu hóa hoặc tạm khóa tài khoản bị chiếm quyền	Buộc đăng xuất (force logoff) và reset mật khẩu cho người dùng	Cô lập thiết bị đầu cuối của người dùng có hành vi bất thường	Thông báo và phối hợp với phòng ban nhân sự/quản lý để xác minh
1	Ghế	Cái	96	0,2	1,2	0,1	0,05
2	Bàn làm việc	Cái	96	0,2	1,2	0,1	0,05
3	Quạt trần	Cái	96	0,035	0,21	0,02	0,018
4	Đèn neon	Bộ	24	0,1	0,6	0,05	0,025
5	Điện năng	kW		0,063	0,378	0,032	0,016

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Vô hiệu hóa hoặc tạm khóa tài khoản bị chiếm quyền	Buộc đăng xuất (force logoff) và reset mật khẩu cho người dùng	Cô lập thiết bị đầu cuối của người dùng có hành vi bất thường	Thông báo và phối hợp với phòng ban nhân sự/quản lý để xác minh
1	Giấy in A4	Gram	0,015	0	0	0,015
2	Mực in laser	Hộp	0,003	0	0	0,003

V. Bảo mật dữ liệu và log

1. Định mức lao động

1.1. Nội dung công việc

a) Đảm bảo log xác thực được mã hóa và lưu trữ an toàn, tách biệt khỏi log hệ thống.

b) Tuân thủ chính sách lưu giữ log theo quy định pháp luật.

c) Thực hiện ẩn danh (anonymization) hoặc che giấu (masking) thông tin nhận dạng cá nhân (PII) trong log.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	**Các yếu tố ảnh hưởng**	**Điểm tối đa**	**Mức thấp**	**Mức trung bình**	**Mức cao**
1	Số lượng log và hệ thống lưu trữ log cần quản lý	40	≤50 log nguồn: 10	51–200 log nguồn: 25	>200 log nguồn: 40
2	Mức độ phân tán và tách biệt log (cục bộ, tập trung, cloud)	20	1 site hoặc tập trung: 5	2–3 site/môi trường: 10	>3 site/môi trường hoặc phức tạp: 20
3	Mức độ áp dụng cơ chế bảo mật và anonymization	25	Sử dụng tính năng sẵn có: 5	Có điều chỉnh/thiết lập thêm: 15	Tùy biến cao, nhiều lớp masking/anonymization: 25
4	Tuân thủ chính sách lưu giữ log và quy định pháp luật	15	Quy định đơn giản, ít loại log: 5	Trung bình, nhiều loại log: 10	Nhiều quy định, nhiều loại log nhạy cảm: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Đảm bảo log xác thực được mã hóa và lưu trữ an toàn, tách biệt khỏi log hệ thống	1	1		2
2	Tuân thủ chính sách lưu giữ log theo quy định pháp luật		2		2
3	Thực hiện ẩn danh (anonymization) hoặc che giấu (masking) thông tin nhận dạng cá nhân (PII) trong log	1	1		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Đảm bảo log xác thực được mã hóa và lưu trữ an toàn, tách biệt khỏi log hệ thống	Hệ thống	1,6	2,2	3,0
2	Tuân thủ chính sách lưu giữ log theo quy định pháp luật	Loại log	1,4	2,0	2,8
3	Thực hiện ẩn danh (anonymization) hoặc che giấu (masking) thông tin nhận dạng cá nhân (PII) trong log	Hệ thống	1,8	2,6	3,4

2. Định mức thiết bị

Ca/01 hệ thống

STT	Thiết bị	ĐVT	Công suất (Kw)	Đảm bảo log xác thực được mã hóa và lưu trữ an toàn, tách biệt khỏi log hệ thống	Tuân thủ chính sách lưu giữ log theo quy định pháp luật	Thực hiện ẩn danh (anonymization) hoặc che giấu (masking) thông tin nhận dạng cá nhân (PII) trong log
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,6
2	Máy in laser	Cái	0,6	0	0,053	0,053
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,101
4	Điện năng	Kw		1,3	6,2	4,2

3. Định mức dụng cụ

Ca/01 hệ thống

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Đảm bảo log xác thực được mã hóa và lưu trữ an toàn, tách biệt khỏi log hệ thống	Tuân thủ chính sách lưu giữ log theo quy định pháp luật	Thực hiện ẩn danh (anonymization) hoặc che giấu (masking) thông tin nhận dạng cá nhân (PII) trong log
1	Ghế	Cái	96	0,2	1,2	0,6
2	Bàn làm việc	Cái	96	0,2	1,2	0,6
3	Quạt trần	Cái	96	0,035	0,21	0,105
4	Đèn neon	Bộ	24	0,1	0,6	0,3
5	Điện năng	kW		0,06	0,38	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Đảm bảo log xác thực được mã hóa và lưu trữ an toàn, tách biệt khỏi log hệ thống	Tuân thủ chính sách lưu giữ log theo quy định pháp luật	Thực hiện ẩn danh (anonymization) hoặc che giấu (masking) thông tin nhận dạng cá nhân (PII) trong log
1	Giấy in A4	Gram		0,015	0,003
2	Mực in laser	Hộp		0,015	0,003

VI. Đánh giá và cải tiến

1. Định mức lao động

1.1. Nội dung công việc

a) Rà soát định kỳ các tài khoản không hoạt động (idle accounts) và đặc quyền.

b) Thực hiện các chiến dịch kiểm tra phishing và đào tạo nhận thức bảo mật cho người dùng.

c) Cập nhật baseline hành vi UEBA dựa trên các sự cố đã xảy ra.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng tài khoản và người dùng cần rà soát/đào tạo	40	≤200: 10	201–1000: 25	>1000: 40
2	Mức độ phân tán hệ thống và người dùng (cơ sở, remote, VDI)	20	1–2 site: 5	3–5 site: 10	>5 site hoặc nhiều môi trường cloud: 20
3	Mức độ phức tạp của chương trình kiểm tra phishing/UEBA	25	Chiến dịch đơn giản, mẫu có sẵn: 5	Có điều chỉnh/tùy biến: 15	Phức tạp, nhiều tình huống, nhiều nhóm người dùng: 25
4	Mức độ cập nhật và cải tiến dựa trên sự cố thực tế	15	Cập nhật đơn giản: 5	Cập nhật theo nhóm/sự kiện: 10	Cập nhật toàn hệ thống, nhiều nguồn log: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Rà soát định kỳ các tài khoản không hoạt động (idle accounts) và đặc quyền	1	1		2
2	Thực hiện các chiến dịch kiểm tra phishing và đào tạo nhận thức bảo mật cho người dùng		2	1	3
3	Cập nhật baseline hành vi UEBA dựa trên các sự cố đã xảy ra	1	1		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Rà soát định kỳ các tài khoản không hoạt động (idle accounts) và đặc quyền	Tài khoản	1,4	2,0	2,8

2	Thực hiện các chiến dịch kiểm tra phishing và đào tạo nhận thức bảo mật cho người dùng	Chiến dịch	1,6	2,4	3,2
3	Cập nhật baseline hành vi UEBA dựa trên các sự cố đã xảy ra	Hệ thống	1,8	2,6	3,6

2. Định mức thiết bị

Ca/01 hệ thống

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Rà soát định kỳ các tài khoản không hoạt động (idle accounts) và đặc quyền	Thực hiện các chiến dịch kiểm tra phishing và đào tạo nhận thức bảo mật cho người dùng	Cập nhật baseline hành vi UEBA dựa trên các sự cố đã xảy ra
1	Máy tính để bàn	Bộ	60	4,027	24,160	24,160
2	Máy in laser	Cái	60	-		
3	Điều hoà nhiệt độ	Cái	96	0,705	4,228	4,228
4	Máy photocopy	Cái	96	-	-	-
5	Điện năng (kw)	kW		15,644	93,862	93,862

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 hệ thống

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Rà soát định kỳ các tài khoản không hoạt động (idle accounts) và đặc quyền	Thực hiện các chiến dịch kiểm tra phishing và đào tạo nhận thức bảo mật cho người dùng	Cập nhật baseline hành vi UEBA dựa trên các sự cố đã xảy ra
1	Ghế	Cái	96	5,033	5,033	30,200
2	Bàn làm việc	Cái	96	5,033	5,033	30,200

3	Quạt trần 0,1 kW	Cái	60	0,881	0,881	5,285
4	Đèn neon 0,04 kW	Bộ	36	2,517	2,517	15,100
5	Điện năng (kw)	kW		1,586	1,586	9,513

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Rà soát định kỳ các tài khoản không hoạt động (idle accounts) và đặc quyền	Thực hiện các chiến dịch kiểm tra phishing và đào tạo nhận thức bảo mật cho người dùng	Cập nhật baseline hành vi UEBA dựa trên các sự cố đã xảy ra
1	Giấy in A4	Gram	-	-	-
2	Mực in laser	Hộp	-	-	-
3	Mực máy photocopy	Hộp	-	-	-
4	Cặp để tài liệu	Cái	-	-	-

CHƯƠNG VII
ĐỊNH MỨC GIÁM SÁT ĐẢM BẢO AN TOÀN THÔNG TIN CHO TOÀN BỘ HỆ THỐNG (SOC - TRUNG TÂM ĐIỀU HÀNH AN NINH MẠNG)

I. Chuẩn bị và thiết lập

1. Định mức lao động

1.1. Nội dung công việc

a) Triển khai và cấu hình hệ thống SIEM/SOAR, tích hợp log từ các nguồn: mạng, máy chủ, ứng dụng, cơ sở dữ liệu, endpoint, cloud.

b) Xây dựng thư viện tình huống (use-case library) theo mô hình MITRE ATT&CK.

c) Xác định ngưỡng cảnh báo, mức độ ưu tiên (severity), quy trình phân quyền xử lý.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng nguồn log cần tích hợp (mạng, server, ứng dụng, DB, endpoint, cloud)	40	≤5 nguồn: 10	6–10 nguồn: 25	>10 nguồn: 40
2	Mức độ phức tạp của hệ thống SIEM/SOAR và workflow xử lý	20	Hệ thống cơ bản, ít playbook: 5	Hệ thống có vài playbook: 10	Hệ thống phức tạp, nhiều playbook & tự động hóa: 20
3	Mức độ phát triển thư viện tình huống (use-case library) MITRE ATT&CK	25	Sử dụng tình huống mẫu sẵn: 5	Chỉnh sửa và bổ sung tình huống: 15	Xây dựng toàn bộ thư viện theo tổ chức/phòng ban: 25
4	Mức độ thiết lập ngưỡng cảnh báo, severity và phân quyền xử lý	15	Ngưỡng đơn giản, ít rule: 5	Ngưỡng trung bình, rule đa lớp: 10	Ngưỡng phức tạp, nhiều rule, nhiều nhóm xử lý: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Triển khai và cấu hình hệ thống SIEM/SOAR, tích hợp log từ các nguồn: mạng, máy chủ, ứng dụng, cơ sở dữ liệu, endpoint, cloud		2	1	3
2	Xây dựng thư viện tình huống (use-case library) theo mô hình MITRE ATT&CK		2	1	3
3	Xác định ngưỡng cảnh báo, mức độ ưu tiên (severity), quy trình phân quyền xử lý	1	1		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Triển khai và cấu hình hệ thống SIEM/SOAR, tích hợp log từ các nguồn: mạng, máy chủ, ứng dụng, cơ sở dữ liệu, endpoint, cloud	Hệ thống	2,2	3,2	4,5
2	Xây dựng thư viện tình huống (use-case library) theo mô hình MITRE ATT&CK	Use-case	1,8	2,6	3,6
3	Xác định ngưỡng cảnh báo, mức độ ưu tiên (severity), quy trình phân quyền xử lý	Rule/Playbook	1,6	2,4	3,2

2. Định mức thiết bị

Ca/01 hệ thống

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Triển khai và cấu hình hệ thống SIEM/SOAR, tích hợp log từ các nguồn: mạng, máy chủ, ứng dụng, cơ sở dữ liệu, endpoint, cloud	Xây dựng thư viện tình huống (use-case library) theo mô hình MITRE ATT&CK	Xác định ngưỡng cảnh báo, mức độ ưu tiên (severity), quy trình phân quyền xử lý
1	Máy tính để bàn	Bộ	60	4,027	24,160	24,160
2	Máy in laser	Cái	60	-		
3	Điều hoà nhiệt độ	Cái	96	0,705	4,228	4,228
4	Máy photocopy	Cái	96	-	-	-
5	Điện năng (kw)	kW		15,644	93,862	93,862

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 hệ thống

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Triển khai và cấu hình hệ thống SIEM/SOAR, tích hợp log từ các nguồn: mạng, máy chủ, ứng dụng, cơ sở dữ liệu, endpoint, cloud	Xây dựng thư viện tình huống (use-case library) theo mô hình MITRE ATT&CK	Xác định ngưỡng cảnh báo, mức độ ưu tiên (severity), quy trình phân quyền xử lý
1	Ghế	Cái	96	5,033	5,033	30,200
2	Bàn làm việc	Cái	96	5,033	5,033	30,200
3	Quạt trần 0,1 kW	Cái	60	0,881	0,881	5,285
4	Đèn neon 0,04 kW	Bộ	36	2,517	2,517	15,100
5	Điện năng (kw)	kW		1,586	1,586	9,513

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Triển khai và cấu hình hệ thống SIEM/SOAR, tích hợp log từ các nguồn: mạng, máy chủ, ứng dụng, cơ sở dữ liệu, endpoint, cloud	Xây dựng thư viện tình huống (use-case library) theo mô hình MITRE ATT&CK	Xác định ngưỡng cảnh báo, mức độ ưu tiên (severity), quy trình phân quyền xử lý
1	Giấy in A4	Gram	-	-	-
2	Mực in laser	Hộp	-	-	-
3	Mực máy photocopy	Hộp	-	-	-
4	Cặp để tài liệu	Cái	-	-	-

II. Giám sát và phân tích

1. Định mức lao động

1.1. Nội dung công việc

a) Giám sát liên tục 24/7 các sự kiện an ninh trên toàn hệ thống.

b) Thực hiện phân loại (triage), làm giàu dữ liệu (enrichment), tương quan cảnh báo (correlation).

c) Phát hiện hành vi tấn công (brute force, phishing, privilege escalation, lateral movement).

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng sự kiện và cảnh báo cần giám sát	40	≤1000 sự kiện/ngày: 10	1001–5000 sự kiện/ngày: 25	>5000 sự kiện/ngày: 40
2	Mức độ phức tạp trong phân loại, làm giàu và tương quan dữ liệu	20	Triage đơn giản, ít nguồn: 5	Trung bình, nhiều nguồn: 10	Phức tạp, nhiều nguồn & enrichment tự động: 20
3	Mức độ phát hiện hành vi tấn công	25	Chỉ một số hành vi phổ biến: 5	Nhiều loại hành vi, kết hợp cảnh báo: 15	Phát hiện nâng cao, nhiều kịch bản MITRE ATT&CK: 25
4	Mức độ tự động hóa giám sát và cảnh báo	15	Giám sát thủ công, ít rule: 5	Một phần tự động, có playbook: 10	Giám sát tự động 24/7, nhiều playbook và cảnh báo: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS3	KS4	Nhóm
1	Giám sát liên tục 24/7 các sự kiện an ninh trên toàn hệ thống	2	1	3
2	Thực hiện phân loại (triage), làm giàu dữ liệu (enrichment), tương quan cảnh báo (correlation)	2	1	3
3	Phát hiện hành vi tấn công (brute force, phishing, privilege escalation, lateral movement)	2	1	3

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Giám sát liên tục 24/7 các sự kiện an ninh trên toàn hệ thống	Hệ thống	2,5	3,5	5,0
2	Thực hiện phân loại (triage), làm giàu dữ liệu (enrichment), tương quan cảnh báo (correlation)	Cảnh báo	2,2	3,2	4,5
3	Phát hiện hành vi tấn công (brute force, phishing, privilege escalation, lateral movement)	Hành vi tấn công	2,0	3,0	4,0

2. Định mức thiết bị

Ca/01 hệ thống

STT	Thiết bị	ĐVT	Thời hạn (tháng)	Giám sát liên tục 24/7 các sự kiện an ninh trên toàn hệ thống	Thực hiện phân loại (triage), làm giàu dữ liệu (enrichment), tương quan cảnh báo (correlation)	Phát hiện hành vi tấn công (brute force, phishing, privilege escalation, lateral movement)
1	Máy tính để bàn	Bộ	60	4,027	24,160	24,160
2	Máy in laser	Cái	60	-		
3	Điều hoà nhiệt độ	Cái	96	0,705	4,228	4,228
4	Máy photocopy	Cái	96	-	-	-
5	Điện năng (kw)	kW		15,644	93,862	93,862

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

3. Định mức dụng cụ

Ca/01 hệ thống

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Giám sát liên tục 24/7 các sự kiện an ninh trên toàn hệ thống	Thực hiện phân loại (triage), làm giàu dữ liệu (enrichment), tương quan cảnh báo (correlation)	Phát hiện hành vi tấn công (brute force, phishing, privilege escalation, lateral movement)
1	Ghế	Cái	96	5,033	5,033	30,200
2	Bàn làm việc	Cái	96	5,033	5,033	30,200
3	Quạt trần 0,1 kW	Cái	60	0,881	0,881	5,285
4	Đèn neon 0,04 kW	Bộ	36	2,517	2,517	15,100
5	Điện năng (kw)	kW		1,586	1,586	9,513

Ghi chú: Mức thiết bị trên tính cho loại KK2, mức cho các loại khó khăn khác tính như sau:

KK1 = 0,8 x KK2.

KK3 = 1,3 x KK2.

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Giám sát liên tục 24/7 các sự kiện an ninh trên toàn hệ thống	Thực hiện phân loại (triage), làm giàu dữ liệu (enrichment), tương quan cảnh báo (correlation)	Phát hiện hành vi tấn công (brute force, phishing, privilege escalation, lateral movement)
1	Giấy in A4	Gram	-	-	-
2	Mực in laser	Hộp	-	-	-
3	Mực máy photocopy	Hộp	-	-	-
4	Cặp để tài liệu	Cái	-	-	-

III. Ứng cứu và xử lý sự cố

1. Định mức lao động

1.1. Nội dung công việc

a) Thực hiện playbook phản ứng: DDoS, ransomware, khai thác lỗ hổng, lạm dụng đặc quyền.

b) Kích hoạt quy trình escalation đến đội chuyên trách, cô lập hệ thống hoặc tài khoản nghi ngờ.

c) Ghi nhận và lưu trữ toàn bộ chuỗi sự kiện phục vụ điều tra.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng sự cố cần ứng cứu và mức độ ảnh hưởng	40	≤5 sự cố/ngày: 10	6–20 sự cố/ngày: 25	>20 sự cố/ngày: 40
2	Mức độ phức tạp của playbook và loại tấn công	20	Playbook cơ bản, tấn công phổ biến: 5	Playbook trung bình, nhiều loại tấn công: 10	Playbook phức tạp, nhiều loại tấn công & scenario: 20
3	Mức độ phối hợp với đội chuyên trách và cô lập hệ thống	25	Quy trình đơn giản, ít nhóm liên quan: 5	Trung bình, vài nhóm: 15	Phức tạp, nhiều nhóm, nhiều phê duyệt: 25
4	Mức độ ghi nhận và lưu trữ chuỗi sự kiện phục vụ điều tra	15	Ghi nhận cơ bản: 5	Ghi nhận chi tiết, một số hệ thống: 10	Ghi nhận đầy đủ, nhiều hệ thống & chuẩn pháp lý: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Thực hiện playbook phản ứng: DDoS, ransomware, khai thác lỗ hổng, lạm dụng đặc quyền		2	1	3
2	Kích hoạt quy trình escalation đến đội chuyên trách, cô lập hệ thống hoặc tài khoản nghi ngờ	1	1		2
3	Ghi nhận và lưu trữ toàn bộ chuỗi sự kiện phục vụ điều tra	1	1		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Thực hiện playbook phản ứng: DDoS, ransomware, khai thác lỗ hổng, lạm dụng đặc quyền	Sự cố	2,0	3,0	4,0
2	Kích hoạt quy trình escalation đến đội chuyên trách, cô lập hệ thống hoặc tài khoản nghi ngờ	Sự cố	1,6	2,4	3,2
3	Ghi nhận và lưu trữ toàn bộ chuỗi sự kiện phục vụ điều tra	Sự cố	1,8	2,6	3,4

2. Định mức thiết bị

Ca/01 sự cố

STT	Thiết bị	ĐVT	Công suất (Kw)	Thực hiện playbook phản ứng: DDoS, ransomware, khai thác lỗ hổng, lạm dụng đặc quyền	Kích hoạt quy trình escalation đến đội chuyên trách, cô lập hệ thống hoặc tài khoản nghi ngờ	Ghi nhận và lưu trữ toàn bộ chuỗi sự kiện phục vụ điều tra
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,6
2	Máy in laser	Cái	0,6	0	0,053	0,053
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,101
4	Điện năng	Kw		1,3	6,2	4,2

3. Định mức dụng cụ

Ca/01 sự cố

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Thực hiện playbook phản ứng: DDoS, ransomware, khai thác lỗ hổng, lạm dụng đặc quyền	Kích hoạt quy trình escalation đến đội chuyên trách, cô lập hệ thống hoặc tài khoản nghi ngờ	Ghi nhận và lưu trữ toàn bộ chuỗi sự kiện phục vụ điều tra
1	Ghế	Cái	96	0,2	1,2	0,6
2	Bàn làm việc	Cái	96	0,2	1,2	0,6
3	Quạt trần	Cái	96	0,035	0,21	0,105

4	Đèn neon	Bộ	24	0,1	0,6	0,3
5	Điện năng	kW		0,06	0,38	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Thực hiện playbook phản ứng: DDoS, ransomware, khai thác lỗ hổng, lạm dụng đặc quyền	Kích hoạt quy trình escalation đến đội chuyên trách, cô lập hệ thống hoặc tài khoản nghi ngờ	Ghi nhận và lưu trữ toàn bộ chuỗi sự kiện phục vụ điều tra
1	Giấy in A4	Gram		0,015	0,003
2	Mực in laser	Hộp		0,015	0,003

IV. Săn tìm mối đe dọa

1. Định mức lao động

1.1. Nội dung công việc

a) Phân tích hành vi ẩn, IOC, log lịch sử để phát hiện tấn công chưa được cảnh báo.

b) Sử dụng nguồn threat intelligence nội bộ và bên thứ ba (MISP, VirusTotal, AlienVault OTX).

c) Cập nhật danh sách IOC, YARA rule, pattern nhận diện tấn công mới.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng log và IOC cần phân tích	40	≤500 IOC/log/ngày : 10	501–2000 IOC/log/ngày : 25	>2000 IOC/log/ngày: 40
2	Mức độ phức tạp của threat intelligence và nguồn dữ liệu	20	Dữ liệu sẵn có, ít nguồn: 5	Một số nguồn, nội bộ + bên ngoài: 10	Nhiều nguồn, kết hợp nội bộ và bên thứ ba: 20
3	Mức độ cập nhật IOC, YARA rule, pattern nhận diện	25	Cập nhật cơ bản, ít rule: 5	Cập nhật trung bình, một số nhóm rule: 15	Cập nhật toàn hệ thống, nhiều nhóm rule & pattern: 25
4	Mức độ tự động hóa và tích hợp vào SOC	15	Thủ công, ít tích hợp: 5	Một phần tự động, tích hợp một số playbook: 10	Hoàn toàn tự động, tích hợp nhiều playbook: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	K ≤ 50
2	KK2	50 < K < 80
3	KK3	K ≥ 80

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Phân tích hành vi ẩn, IOC, log lịch sử để phát hiện tấn công chưa được cảnh báo		2	1	3
2	Sử dụng nguồn threat intelligence nội bộ và bên thứ ba (MISP, VirusTotal, AlienVault OTX)		2	1	3
3	Cập nhật danh sách IOC, YARA rule, pattern nhận diện tấn công mới	1	1		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Phân tích hành vi ẩn, IOC, log lịch sử để phát hiện tấn công chưa được cảnh báo	IOC/log	2,0	3,0	4,0
2	Sử dụng nguồn threat intelligence nội bộ và bên thứ ba (MISP, VirusTotal, AlienVault OTX)	Nguồn	1,8	2,6	3,6
3	Cập nhật danh sách IOC, YARA rule, pattern nhận diện tấn công mới	Rule/ pattern	1,6	2,4	3,2

2. Định mức thiết bị

Ca/ IOC/log

STT	Thiết bị	ĐVT	Công suất (Kw)	Phân tích hành vi ẩn, IOC, log lịch sử để phát hiện tấn công chưa được cảnh báo	Sử dụng nguồn threat intelligence nội bộ và bên thứ ba (MISP, VirusTotal, AlienVault OTX)	Cập nhật danh sách IOC, YARA rule, pattern nhận diện tấn công mới
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,6
2	Máy in laser	Cái	0,6	0	0,053	0,053

3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,101
4	Điện năng	Kw		1,3	6,2	4,2

3. Định mức dụng cụ

Ca/ IOC/log

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Phân tích hành vi ẩn, IOC, log lịch sử để phát hiện tấn công chưa được cảnh báo	Sử dụng nguồn threat intelligence nội bộ và bên thứ ba (MISP, VirusTotal, AlienVault OTX)	Cập nhật danh sách IOC, YARA rule, pattern nhận diện tấn công mới
1	Ghế	Cái	96	0,2	1,2	0,6
2	Bàn làm việc	Cái	96	0,2	1,2	0,6
3	Quạt trần	Cái	96	0,035	0,21	0,105
4	Đèn neon	Bộ	24	0,1	0,6	0,3
5	Điện năng	kW		0,06	0,38	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Phân tích hành vi ẩn, IOC, log lịch sử để phát hiện tấn công chưa được cảnh báo	Sử dụng nguồn threat intelligence nội bộ và bên thứ ba (MISP, VirusTotal, AlienVault OTX)	Cập nhật danh sách IOC, YARA rule, pattern nhận diện tấn công mới
1	Giấy in A4	Gram		0,015	0,003
2	Mực in laser	Hộp		0,015	0,003

V. Rà soát và cải tiến

1. Định mức lao động

1.1. Nội dung công việc

a) Thực hiện đánh giá sau sự cố (post-incident review), cập nhật quy tắc SIEM và playbook.

b) Đánh giá năng lực phản ứng của đội SOC, đề xuất đào tạo và nâng cấp công cụ.

c) Báo cáo định kỳ kết quả vận hành và cải thiện khả năng phát hiện.

1.2. Phân loại khó khăn

Các yếu tố ảnh hưởng

STT	Các yếu tố ảnh hưởng	Điểm tối đa	Mức thấp	Mức trung bình	Mức cao
1	Số lượng sự cố cần đánh giá và quy tắc SIEM/playbook cập nhật	40	≤5 sự cố: 10	6–20 sự cố: 25	>20 sự cố: 40
2	Mức độ phức tạp của playbook và quy trình đánh giá	20	Quy trình cơ bản, ít playbook: 5	Trung bình, một số playbook: 10	Phức tạp, nhiều playbook & scenario: 20
3	Mức độ đánh giá năng lực và đề xuất cải tiến	25	Đơn giản, nhóm nhỏ: 5	Trung bình, một số nhóm SOC: 15	Phức tạp, toàn SOC, nhiều kỹ năng và công cụ: 25
4	Mức độ lập báo cáo định kỳ và cải thiện khả năng phát hiện	15	Báo cáo đơn giản: 5	Trung bình, báo cáo chi tiết 1–2 lần/tháng: 10	Chi tiết, toàn hệ thống, báo cáo nhiều lần/tháng: 15

Phân loại khó khăn

STT	Mức độ khó khăn	Khoảng điểm (K)
1	KK1	$K \leq 50$
2	KK2	$50 < K < 80$
3	KK3	$K \geq 80$

1.3. Định biên

STT	Danh mục công việc	KS2	KS3	KS4	Nhóm
1	Thực hiện đánh giá sau sự cố (post-incident review), cập nhật quy tắc SIEM và playbook		2	1	3
2	Đánh giá năng lực phản ứng của đội SOC, đề xuất đào tạo và nâng cấp công cụ	1	1		2
3	Báo cáo định kỳ kết quả vận hành và cải thiện khả năng phát hiện	1	1		2

1.4. Định mức

STT	Danh mục công việc	ĐVT	KK1	KK2	KK3
1	Thực hiện đánh giá sau sự cố (post-incident review), cập nhật quy tắc SIEM và playbook	Sự cố	2,0	3,0	4,0
2	Đánh giá năng lực phản ứng của đội SOC, đề xuất đào tạo và nâng cấp công cụ	Lần đánh giá	1,6	2,4	3,2
3	Báo cáo định kỳ kết quả vận hành và cải thiện khả năng phát hiện	Báo cáo	1,8	2,6	3,4

2. Định mức thiết bị

Ca/ Báo cáo

STT	Thiết bị	ĐVT	Công suất (Kw)	Thực hiện đánh giá sau sự cố (post-incident review), cập nhật quy tắc SIEM và playbook	Đánh giá năng lực phản ứng của đội SOC, đề xuất đào tạo và nâng cấp công cụ	Báo cáo định kỳ kết quả vận hành và cải thiện khả năng phát hiện
1	Máy tính để bàn	Cái	0,4	0,2	1,2	0,6
2	Máy in laser	Cái	0,6	0	0,053	0,053
3	Điều hoà nhiệt độ	Cái	2,2	0,034	0,101	0,101
4	Điện năng	Kw		1,3	6,2	4,2

3. Định mức dụng cụ

Ca/ Báo cáo

STT	Dụng cụ	ĐVT	Thời hạn (tháng)	Báo cáo định kỳ kết quả vận hành và cải thiện khả năng phát hiện	Báo cáo định kỳ kết quả vận hành và cải thiện khả năng phát hiện	Báo cáo định kỳ kết quả vận hành và cải thiện khả năng phát hiện
1	Ghế	Cái	96	0,2	1,2	0,6
2	Bàn làm việc	Cái	96	0,2	1,2	0,6
3	Quạt trần	Cái	96	0,035	0,21	0,105
4	Đèn neon	Bộ	24	0,1	0,6	0,3
5	Điện năng	kW		0,06	0,38	0,19

4. Định mức vật liệu

STT	Vật liệu	ĐVT	Báo cáo định kỳ kết quả vận hành và cải thiện khả năng phát hiện	Báo cáo định kỳ kết quả vận hành và cải thiện khả năng phát hiện	Báo cáo định kỳ kết quả vận hành và cải thiện khả năng phát hiện
1	Giấy in A4	Gram		0,015	0,003
2	Mực in laser	Hộp		0,015	0,003

PHỤ LỤC 1: GIÁM SÁT AN TOÀN THÔNG TIN CHO THIẾT BỊ MẠNG

TT	Tên sản phẩm	Tên mẫu biểu	Dạng lưu trữ	Mẫu
1.	Báo cáo hàng ngày: số lượng cảnh báo, sự kiện quan trọng, thiết bị ngừng hoạt động	TBM.01	Số	TBM.01.docx
2.	Báo cáo hàng tuần: mức sử dụng băng thông, tình trạng backup cấu hình	TBM.02	Số	TBM.02.docx
3.	Báo cáo sự cố (theo ISO/IEC 27035): chuỗi thời gian, nguyên nhân gốc, biện pháp xử lý	TBM.03	Số + giấy	TBM.03.docx
4.	Báo cáo hàng tháng: xu hướng tấn công, IOC, baseline lưu lượng	TBM.04	Số + giấy	TBM.04.docx
5.	Báo cáo tuân thủ cấu hình, audit log	TBM.05	Số	TBM.05.docx
6.	Chỉ số đo lường (KPI): thời gian phát hiện (MTTD), thời gian xử lý (MTTR), tỷ lệ cảnh báo sai (false positives), tỷ lệ thiết bị gửi log	TBM.06	Số	TBM.06.docx

PHỤ LỤC 2: GIÁM SÁT AN TOÀN THÔNG TIN CHO HẠ TẦNG ẢO HÓA (CLOUD, VIRTUALIZATION)

TT	Tên sản phẩm	Tên mẫu biểu	Dạng lưu trữ	Mẫu
1.	Báo cáo hàng ngày: sự kiện truy cập IAM, thay đổi cấu hình cloud, cảnh báo bảo mật container/VM	AH.01	Số	AH.01.docx
2.	Báo cáo hàng tuần: trạng thái tài nguyên cloud (CPU, storage, network), nhật ký audit API, tình trạng backup snapshot	AH.02	Số	AH.02.docx
3.	3. Báo cáo sự cố: chi tiết sự kiện vi phạm quyền truy cập, rò rỉ dữ liệu, hành vi bất thường trên VM/container, biện pháp khắc phục	AH.03	Số + giấy	AH.03.docx
4.	4. Báo cáo hàng tháng: xu hướng tấn công trên hạ tầng ảo hóa, phân tích sử dụng IAM key, thống kê thay đổi cấu hình và baseline bảo mật	AH.04	Số + giấy	AH.04.docx
5.	5. Báo cáo tuân thủ: đánh giá chính sách bảo mật cloud (CIS Benchmark, ISO/IEC 27017), kiểm tra lưu giữ log và mã hóa dữ liệu	AH.05	Số	AH.05.docx
6.	6. Chỉ số đo lường (KPI): Thời gian phát hiện và xử lý sự cố (MTTD, MTTR); Tỷ lệ sự kiện bất thường được phân tích tự động (automation rate); Số lượng tài nguyên tuân thủ baseline bảo mật (% compliant);	AH.06	Số	AH.06.docx

PHỤ LỤC 3: GIÁM SÁT AN TOÀN THÔNG TIN CHO MÁY CHỦ (HỆ ĐIỀU HÀNH WINDOWS, LINUX)

TT	Tên sản phẩm	Tên mẫu biểu	Dạng lưu trữ	Mẫu
1.	Báo cáo hàng ngày: đăng nhập bất thường, lỗi hệ thống, dịch vụ dừng đột ngột, thay đổi quyền hoặc nhóm người dùng	HĐH.01	Số	HĐH.01.docx
2.	Báo cáo hàng tuần: tình trạng CPU/RAM/I/O, số lượng kết nối, trạng thái bản vá và dịch vụ quan trọng	HĐH.02	Số	HĐH.02.docx
3.	Báo cáo sự cố: chi tiết sự kiện xâm nhập, lỗi bảo mật, kết quả forensic (log, memory dump, snapshot), biện pháp khắc phục	HĐH.03	Số + giấy	HĐH.03.docx
4.	Báo cáo hàng tháng: thống kê xu hướng sự cố, mức độ tuân thủ hardening, tỷ lệ máy chủ đã vá đầy đủ, thay đổi cấu hình bảo mật	HĐH.04	Số + giấy	HĐH.04.docx
5.	Báo cáo tuân thủ: đối chiếu chuẩn CIS, NIST, ISO/IEC 27001; kiểm tra chính sách quản lý tài khoản, lưu trữ và mã hóa log	HĐH.05	Số	HĐH.05.docx
6.	Chỉ số đo lường (KPI): Thời gian phát hiện và xử lý sự cố (MTTD, MTTR); Tỷ lệ máy chủ cập nhật bản vá đúng hạn; Số lượng cảnh báo sai (false positives); Tỷ lệ máy chủ gửi log và tuân thủ baseline bảo mật	HĐH.06	Số	HĐH.06.docx

PHỤ LỤC 4: GIÁM SÁT AN TOÀN THÔNG TIN CHO ỨNG DỤNG (WEB, ERP, CRM, API, EMAIL)

TT	Tên sản phẩm	Tên mẫu biểu	Dạng lưu trữ	Mẫu
1.	Báo cáo hàng ngày: số lượng truy cập, lỗi ứng dụng, cảnh báo WAF/API, đăng nhập bất thường	UD.01	Số	UD.01.docx
2.	Báo cáo hàng tuần: trạng thái hoạt động ứng dụng, hiệu suất API, tỷ lệ lỗi và phản hồi chậm	UD.02	Số	UD.02.docx
3.	Báo cáo sự cố: chi tiết khai thác lỗ hổng, tấn công brute force, phishing, rò rỉ dữ liệu; biện pháp xử lý	UD.03	Số + giấy	UD.03.docx
4.	Báo cáo hàng tháng: thống kê xu hướng tấn công, hiệu quả quy tắc WAF, tỷ lệ giao dịch nghi ngờ, đánh giá bảo mật API	UD.04	Số + giấy	UD.04.docx
5.	Báo cáo tuân thủ: đối chiếu OWASP Top 10, ISO/IEC 27034, GDPR (nếu có), kiểm tra chính sách PII và mã hóa log	UD.05	Số	UD.05.docx
6.	Chỉ số đo lường (KPI): MTTD/MTTR (thời gian phát hiện và khắc phục); Số lượng lỗ hổng được vá đúng hạn; Tỷ lệ cảnh báo đúng (true positives); Tỷ lệ log ứng dụng được thu thập và phân tích đầy đủ	UD.06	Số	UD.06.docx

PHỤ LỤC 5: GIÁM SÁT AN TOÀN THÔNG TIN CHO CƠ SỞ DỮ LIỆU

TT	Tên sản phẩm	Tên mẫu biểu	Dạng lưu trữ	Mẫu
1.	Báo cáo hàng ngày: đăng nhập bất thường, truy vấn lỗi, thay đổi cấu trúc hoặc quyền truy cập	CSDL.01	Số	CSDL.01.docx
2.	Báo cáo hàng tuần: tình trạng hiệu năng DB, lịch backup/restore, log audit	CSDL.02	Số	CSDL.02.docx
3.	Báo cáo sự cố: chi tiết truy vấn phá hoại (DROP/DELETE), rò rỉ dữ liệu, biện pháp khôi phục	CSDL.03	Số + giấy	CSDL.03.docx
4.	Báo cáo hàng tháng: xu hướng truy cập, thay đổi quyền, thống kê hiệu năng, kiểm tra tuân thủ chính sách lưu trữ	CSDL.04	Số + giấy	CSDL.04.docx
5.	Báo cáo tuân thủ: đối chiếu chuẩn bảo mật cơ sở dữ liệu (CIS Benchmark, ISO/IEC 27001, PCI DSS), đánh giá trạng thái mã hóa và quản lý quyền	CSDL.05	Số	CSDL.05.docx
6.	Chỉ số đo lường (KPI): Thời gian phát hiện và xử lý sự cố (MTTD, MTTR); Tỷ lệ backup thành công và khôi phục thử nghiệm; Tỷ lệ phát hiện truy vấn bất thường; Tỷ lệ cơ sở dữ liệu tuân thủ baseline bảo mật và mã hóa	CSDL.06	Số	CSDL.06.docx

PHỤ LỤC 6: GIÁM SÁT AN TOÀN THÔNG TIN CHO NGƯỜI DÙNG

TT	Tên sản phẩm	Tên mẫu biểu	Dạng lưu trữ	Mẫu
1.	Báo cáo hàng ngày: Đăng nhập bất thường (khác vị trí, ngoài giờ), thất bại đăng nhập/MFA liên tục, thay đổi mật khẩu/đặc quyền người dùng	USER.01	Số	USER.01.docx
2.	Báo cáo hàng tuần: Thống kê hành vi người dùng đặc quyền, tổng hợp truy cập dữ liệu nhạy cảm, trạng thái xác thực MFA/SSO, tài khoản không hoạt động	USER.02	Số	USER.02.docx
3.	Báo cáo sự cố: Chi tiết sự kiện chiếm quyền tài khoản, vi phạm chính sách truy cập, rò rỉ dữ liệu nội bộ do người dùng; biện pháp khắc phục	USER.03	Số + giấy	USER.03.docx
4.	Báo cáo hàng tháng: Xu hướng hành vi bất thường (UEBA), đánh giá tài khoản đặc quyền, thống kê kết quả kiểm tra phishing, rà soát tài khoản không hoạt động	USER.04	Số + giấy	USER.04.docx
5.	Báo cáo tuân thủ: Đối chiếu chính sách IAM với ISO/IEC 27001 (A.9, A.11), NIST CSF; kiểm tra việc áp dụng MFA, và chính sách quản lý mật khẩu	USER.05	Số	USER.05.docx
6.	Chỉ số đo lường (KPI): Thời gian phát hiện và xử lý sự cố (MTTD, MTTR); Tỷ lệ tài khoản có MFA; Tỷ lệ người dùng vi phạm chính sách mật khẩu; Tỷ lệ hành vi bất thường được UEBA phát hiện chính xác	USER.06	Số	USER.06.docx

PHỤ LỤC 7: GIÁM SÁT AN TOÀN THÔNG TIN CHO TOÀN BỘ HỆ THỐNG (SOC - TRUNG TÂM ĐIỀU HÀNH AN NINH MẠNG)

TT	Tên sản phẩm	Tên mẫu biểu	Dạng lưu trữ	Mẫu
1.	Báo cáo hàng ngày: số lượng cảnh báo, sự kiện nghi ngờ, tình trạng thiết bị/nguồn log, hành vi đáng chú ý	SOC.01	Số	 SOC.01.docx
2.	Báo cáo hàng tuần: thống kê mức độ cảnh báo, top 10 mối đe dọa, hiệu quả quy tắc phát hiện, tình trạng phản ứng sự cố	SOC.02	Số	 SOC.02.docx
3.	Báo cáo sự cố: chi tiết chuỗi sự kiện, phân tích nguyên nhân gốc (root cause), tác động và biện pháp khắc phục theo ISO/IEC 27035	SOC.03	Số + giấy	 SOC.03.docx
4.	Báo cáo hàng tháng: xu hướng tấn công, thống kê IOC, hiệu quả threat hunting, tỷ lệ cảnh báo chính xác	SOC.04	Số + giấy	 SOC.04.docx
5.	Báo cáo tuân thủ: đối chiếu tiêu chuẩn vận hành SOC (ISO/IEC 27035, NIST 800-61, MITRE ATT&CK), kiểm tra đầy đủ nguồn log	SOC.05	Số	 SOC.05.docx
6.	Chỉ số đo lường (KPI): MTTD, MTTR (thời gian phát hiện và xử lý); Tỷ lệ cảnh báo chính xác (true positive rate); Số lượng sự cố được phát hiện chủ động qua threat hunting; Tỷ lệ hệ thống/thiết bị gửi log đầy đủ về SIEM	SOC.06	Số	 SOC.06.docx