BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1356 /QĐ-BTTTT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 07 tháng 7 năm 2022

QUYẾT ĐỊNH

Ban hành Tiêu chí đánh giá giải pháp, dịch vụ Trung tâm giám sát điều hành an toàn, an ninh mạng (SOC)

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

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 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Chỉ thị 14/CT-TTg ngày 07 tháng 6 năm 2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Căn cứ Thông tư 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 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 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

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

Căn cứ Quyết định số 2036/QĐ-BTTTT ngày 27 tháng 11 năm 2019 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục An toàn thông tin;

Căn cứ văn bản số 2973/BTTTT-CATTT ngày 04 tháng 9 năm 2019 của Bộ Thông tin và Truyền thông về việc hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước;

Căn cứ Chỉ thị số 01/CT-BTTTT ngày 18 tháng 01 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông về định hướng phát triển ngành Thông tin và Truyền thông năm 2022 và giai đoạn 2022-2024;

Căn cứ Quyết định số 277/QĐ-BTTTT ngày 17 tháng 02 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành Kế hoạch phát triển Nền tảng Trung tâm giám sát điều hành an toàn thông tin mạng năm 2022;

Theo đề nghị của Cục trưởng Cục An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Tiêu chí đánh giá giải pháp, dịch vụ Trung tâm giám sát điều hành an toàn, an ninh mạng (SOC).

Điều 2. Tiêu chí nêu tại Điều 1 là cơ sở để thực hiện đánh giá các sản phẩm, dịch vụ SOC.

Điều 3. Cục An toàn thông tin phối hợp các cơ quan, tổ chức, đơn vị liên quan để hướng dẫn, triển khai thực hiện Quyết định này.

Điều 4. Quyết định này có hiệu lực kể từ ngày ký ban hành.

Điều 5. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin và Thủ trưởng các đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 5;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng;
- Các doanh nghiệp an toàn thông tin mạng;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

TIÊU CHÍ ĐÁNH GIÁ
Giải pháp, dịch vụ Trung tâm giám sát điều hành an toàn, an ninh mạng (SOC)

(Ban hành kèm theo Quyết định số 1356 /QĐ-BTTTT ngày 07 / 7 /2022 của Bộ Thông tin và Truyền thông)

1. Tiêu chí về công nghệ

TT	Tiêu chí/Nội dung đánh giá	Yêu cầu đáp ứng
1	**Tiêu chí yêu cầu với từng thành phần**	
1.1	***Yêu cầu về thành phần cơ bản*** Các thành phần cơ bản của giải pháp bao gồm: SIEM, NIPS, Anti-Virus, EDR.	Toàn bộ các thành phần cơ bản trong hệ thống SOC phải được đánh giá theo Yêu cầu kỹ thuật cơ bản do Bộ Thông tin và Truyền thông ban hành, bao gồm: - SIEM: 1127/QĐ-BTTTT ngày 30/07/2021 Yêu cầu kỹ thuật cơ bản đối với sản phẩm Quản lý và phân tích sự kiện an toàn thông tin; - NIPS: 1591/QĐ-BTTTT ngày 13/10/2021 Yêu cầu kỹ thuật cơ bản đối với sản phẩm Phòng, chống xâm nhập lớp mạng; - Anti-Virus: 176/QĐ-BTTTT ngày 09/02/2022 Yêu cầu kỹ thuật cơ bản đối với sản phẩm Phòng, chống mã độc; - EDR: 764/QĐ-BTTTT ngày 25/4/2022 Yêu cầu kỹ thuật cơ bản đối với sản phẩm Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối.
1.2	***Yêu cầu về thành phần nâng cao*** Các thành phần nâng cao của giải pháp bao gồm: WAF, SOAR, Threat Intelligence Platform.	Các thành phần nâng cao yếu tố nổi trội hơn của các giải pháp SOC. Thành phần nâng cao trong hệ thống SOC phải được đánh giá theo Yêu

		cầu kỹ thuật cơ bản do Bộ Thông tin và Truyền thông ban hành, bao gồm: - WAF: 1126/QĐ-BTTTT ngày 30/07/2021 Yêu cầu kỹ thuật cơ bản đối với sản phẩm Tường lửa ứng dụng web; - SOAR: 1907/QĐ-BTTTT ngày 02/12/2021 Yêu cầu kỹ thuật cơ bản đối với sản phẩm Điều phối, tự động hóa và phản ứng an toàn thông tin; - Threat Intelligence Platform: 1517/QĐ-BTTTT ngày 06/10/2021 Yêu cầu kỹ thuật cơ bản đối với sản phẩm Nền tảng tri thức mối đe dọa an toàn thông tin.
2	**Tiêu chí đánh giá hiệu quả của hệ thống hoàn chỉnh**	
2.1	***Giải pháp***	
2.1.1	***Hiệu quả của các thành phần trong hệ thống***	
2.1.1.1	Thu thập, xử lý, phân tích log.	Có khả năng tiếp nhận log của 04 nguồn log thiết yếu (thiết bị mạng (Router, Switch), thiết bị bảo mật (Firewall, NIDS, Endpoint server), hệ điều hành (Linux, Windows) , ứng dụng (Web, Mail, DNS, DHCP).
2.1.1.2	Phân tích phát hiện tấn công dựa vào phân tích lưu lượng mạng.	- Có khả năng phát hiện tấn công cơ bản lớp mạng; - Khả năng phát hiện kết nối đến máy chủ điều khiển của mã độc.
2.1.1.3	Phân tích phát hiện tấn công Endpoints, Server.	Có khả năng phát hiện các hành vi bất thường như: - Tập tin bị thay đổi, thêm mới trên đường dẫn cụ thể; - Chạy các lệnh nguy hiểm; - Có các hành vi như: thay đổi Registry, tự động khởi chạy; - Ngăn chặn từ trung tâm khi cần thiết.
2.1.1.4	Phát hiện, ngăn chặn tấn công lớp ứng dụng.	Tối thiểu có giải pháp bảo vệ Web hoặc tích hợp được với giải pháp có sẵn.

2.1.1.5	Quản lý, phân tích, cảnh báo.	Có hệ thống phần mềm hỗ trợ khách hàng đảm bảo có các thông tin: chi tiết về sự cố, tương quan giữa các sự kiện, mức độ, tình trạng xử lý.
2.1.2	***Chức năng cơ bản SOC***	
2.1.2.1	Tùy chỉnh giao diện giám sát	Giải pháp có thể tùy chỉnh giao diện giám sát.
2.1.2.2	Gửi cảnh báo đến thành phần thứ 3 (MAIL, SMS, APP…)	Gửi được cảnh báo đến tối thiểu 01 thành phần.
2.1.2.3	Truy xuất dữ liệu phục vụ phân tích tấn công.	Có thể truy xuất log network, security của Endpoint.
2.1.2.4	Ngăn chặn tấn công	Tối thiểu có khả năng chặn tấn công theo IP.
2.1.2.5	Tích hợp với các giải pháp/hệ thống cung cấp, chia sẻ thông tin tấn công mạng	Hệ thống có khả năng tích hợp với hệ thống Threat Intelligence hoặc dễ dàng tuỳ biến.
2.1.3	***Chức năng nâng cao SOC***	
2.1.3.1	Threat Intelligence	Có hệ thống Threat Intelligence tự phát triển hoặc mua của hãng thứ 3.
2.1.3.2	Vul Scan	Cung cấp hệ thống, hoặc tích hợp hệ thống của khách hàng vào hệ thống quản lý tập trung.
2.1.3.3	SOAR	Hệ thống có playbook (hướng dẫn xử lý các tình huống điển hình) để xử lý các trường hợp: phát hiện mã độc, hành vi dò quét.
2.2	***Khả năng làm chủ giải pháp***	
2.2.1	Mức độ làm chủ giải pháp - Mức độ làm chủ các giải pháp thương mại (nếu có); - Mức độ làm chủ các giải pháp tự phát triển, mã nguồn mở (nếu có).	Tự làm chủ giải pháp, hoặc có khả năng tuỳ biến theo yêu cầu của khách hàng.
2.2.2	Khả năng tùy chỉnh hệ thống đáp ứng yêu cầu đặc thù khách hàng.	Chứng minh được khả năng tuỳ biến qua một số yêu cầu cụ thể.
2.3	***Tuân thủ các quy định, hướng dẫn về an toàn thông tin***	
2.3.1	Kết nối, chia sẻ thông tin với Trung tâm Giám sát an toàn không	Kết nối và gửi dữ liệu thường xuyên về hệ thống của Trung tâm Giám sát an toàn không gian mạng quốc gia.

	gian mạng quốc gia theo yêu cầu, quy định hiện hành. - Khả năng kết nối chia sẻ dữ liệu; - Chất lượng dữ liệu chia sẻ.	
2.3.2	Tuân thủ các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ tại các văn bản quy định hiện hành.	Hồ sơ đề xuất cấp độ được phê duyệt - tối thiểu cấp độ 3.

2. Tiêu chí về chất lượng dịch vụ

TT	Tiêu chí/Nội dung đánh giá	Yêu cầu đáp ứng
1	**Đánh giá quy trình**	
1.1	Quy chế quản lý SOC (quy định chung bao gồm quyền hạn, trách nhiệm của cá nhân, tổ chức liên quan).	Cung cấp đủ hồ sơ, quyết định liên quan.
1.2	Quy trình, tài liệu liên quan đến vận hành SOC (thiết kế, thiết lập, vận hành, nâng cấp …).	Quy trình đảm bảo có đủ các mục: mô hình, vận hành, giám sát, phối hợp xử lý, quy trình xử lý sự cố, báo cáo định kỳ.
1.3	Đánh giá một số tình huống cụ thể trong việc xử lý các sự cố an toàn thông tin theo quy trình đã ban hành.	Tối thiểu 03 tình huống phù hợp với quy trình ở mục 1.2.
2	**Đánh giá con người**	
2.1	Đảm bảo số lượng nhân sự vận hành SOC: - Nhân sự trực 24/7; - Nhân sự hỗ trợ khách hàng xử lý các vấn đề phát sinh.	Đảm bảo đủ số lượng nhân sự Tổng nhân sự cho SOC: ít nhất 12 người trong đó: - Tier 1: có tối thiểu 06 người trong đó 02 người/ca; - Tier 2: tối thiểu 03 người; - Tier 3: tối thiểu 02 người; - SOC Manager: 01 người.
2.2	Chất lượng nhân sự: - Nhân sự chuyên môn có chứng chỉ hoặc hồ sơ năng lực đáp ứng yêu cầu (nếu có).	Nhân sự có hồ sơ năng lực đảm bảo yêu cầu cụ thể sau: **- Tier 1:** Tốt nghiệp ĐH chuyên ngành CNTT/ATTT hoặc chuyên ngành gần với CNTT theo quy định; Có kinh

		nghiệm ít nhất 1 năm trở lên; Có 1 trong các chứng chỉ CEH, S+, CSA, CND hoặc tương đương; - **Tier 2:** Tốt nghiệp ĐH chuyên ngành CNTT/ATTT hoặc chuyên ngành gần với CNTT theo quy định; Có kinh nghiệm ít nhất 3 năm trở lên; Có 1 trong các chứng chỉ: ECIH, CHFI, OCSP hoặc tương đương; - **Tier 3:** Có kinh nghiệm ít nhất 5 năm trở lên; Có 1 trong các chứng chỉ: CHFI, CTIA, OCSP, CHFI, OSCE, GSEC hoặc tương đương. - **SOC Manager:** Có kinh nghiệm ít nhất 5 năm trở lên; Có 1 trong các chứng chỉ: CISA, CISSP, CISM, CCISO hoặc tương đương.