DATASHEET
NỀN TẢNG DỮ LIỆU THÁM BÁO AN NINH MẠNG
VNPT CTIP – VNPT CYBER THREAT INTELLIGENCE PLATFORM

1. Mục tiêu

VNPT Cyber Threat Intelligence Platform (VNPT CTIP) là nền tảng hoàn toàn do VNPT tự làm chủ và phát triển với tên gọi "Nền tảng dữ liệu thám báo An ninh mạng". Nền tảng cung cấp cho tổ chức và doanh nghiệp khả năng cập nhật tự động các mối nguy hại mới, các nhân tố có thể làm ảnh hưởng cũng như đe doạ tới tài sản, uy tín và an toàn của tổ chức đơn vị. Nền tảng gói gọn quá trình cập nhật, phân tích và xử lý các thông tin về nguy cơ ATTT bằng AI/ML, các chuyên gia an ninh mạng giàu kinh nghiệm đến khách hàng một cách nhanh và chính xác nhất.

⇨ Triển khai Nền tảng dữ liệu thám báo An ninh mạng -VNPT CTIP cung cấp khả năng cập nhật tự động các mối nguy hại mới, cũng như phương pháp phòng ngừa từ các tổ chức uy tín về bảo mật. Đồng thời mở ra khả năng kết hợp cùng các hệ thống xử lý tự động (Incident Response), với phương pháp lấy thông tin được chuẩn hoá từ hệ thống Threat để áp dụng nhanh chóng các biện pháp phòng ngừa, giảm thiểu rủi ro trước các mối nguy hại thường trực.

2. Chức năng

2.1. Tổng quan

Nền tảng dữ liệu thám báo An ninh mạng được triển khai theo mô hình cloud-base, thu thập dữ liệu từ nhiều nguồn (chia sẻ của các đối tác, cộng đồng mở, các hệ thống logging của Tập đoàn, đội ngũ an toàn thông tin của TTATTT…).

VNPT CTIP sẽ bao gồm các thông tin:

- Malware Database: Cơ sở dữ liệu về mã độc
- DNS Query Database: Cơ sở dữ liệu về các truy vấn bản ghi DNS từ khách hàng
- Botnet Database: Cơ sở dữ liệu về các botnet.
- C&C Server Database: Cơ sở dữ liệu về các máy chủ điều khiển mã độc.
- Vulnerability/exploit Database: Cơ sở dữ liệu về các lỗ hổng ATTT và các mã khai thác lỗ hổng ATTT.

2.2. Chức năng chính

1. Risk Collection & Feed: thu thập thông tin về nguy cơ an ninh mạng từ nhiều nguồn cả nội dung từ nguồn mở và nguồn đóng. Chúng tôi thu nhặt các nội dung, tin nhắn, hình ảnh và thông tin về các mối nguy ATTT nhằm phân tích và đưa ra cảnh báo đến khách hàng một cách chính xác và nhanh chóng nhất. Các thông tin được đẩy tự động đến các giải pháp ATBM bằng RestAPI và chuẩn STIX/TAXII theo thời gian thực.
2. Threat Card: Cung cấp thông tin tổng quan về các mối đe doạ đã đang và từng phát hiện bởi hệ thống rộng lớn như mục tiêu tấn công, nhóm tấn công, dấu hiệu đặc biệt, kỹ thuật, CVSS, phân loại mã độc/lỗ hổng,...
3. Attack Collection: Cung cấp các thông tin tấn công Phishing, DdoS và Deface trong khu vực Việt Nam. Giúp doanh nghiệp dễ dàng nắm bắt tình hình, xu hướng tấn công chung có thể ảnh hưởng đến khách hàng.
4. Risk Profile: Liệt kê, định nghĩa và cung cấp các thông tin về các nhóm tin tặc, chiến dịch tấn công, dòng mã độc và lỗ hổng trên thế giới nói chung và Việt Nam nói riêng.
5. Threat Category: Định danh các loại nguy cơ, cảnh báo theo mức độ ảnh hưởng, chia sẻ thông tin, phân loại riêng phù hợp với khách hàng giúp dễ dàng kiểm soát thông tin và cảnh báo.

6. Incident & Response TI: Cung cấp thông tin về mối đe doạ một các chi tiết và dễ hiểu nhất cũng như đánh giá mức độ nguy hiểm và đưa ra khuyến cáo người dùng phù hợp với từng mối đe doạ. Ngoài ra Threat Intelligence cung cấp - hỗ trợ API Feed, tích hợp toàn diện cho các giải pháp ATTT hiện tại của VCI một cách tự động (SIEM, SmartIR,...) cũng như hỗ trợ các giải pháp khác trong việc tăng khả năng phát hiện và xử lý các mối đe doạ với ATTT của tổ chức.
7. Cung cấp báo cáo: Hệ thống VNPT CTIP cung cấp báo cáo hàng ngày /tuần/ tháng/ quý/ năm, cảnh báo sớm với các thông tin được cập nhật liên tục về mã độc, chiến dịch tấn công, lỗ hổng hay tình hình ATTT nổi trội trong và ngoài nước.

3. Thông số sản phẩm

Part number	Model	Hãng	Xuất xứ	Năm sản xuất
CTIP-24-OP-10-20-30-40-00-00-00	VNPT CTIP	VNPT	Việt Nam	2024