
Cyber Security

APT Malware

Deception

SOC EDR

DLP

IR

# Mục lục

## LỢI ÍCH CHÍNH DÀNH CHO KHÁCH HÀNG

- Thu thập và hiển thị toàn bộ thông tin cần thiết cho bảo mật của tất cả các thiết bị đầu cuối, bất kể có đang trực tuyến hay ngoại tuyến trên mạng.
- Liên tục giám sát các điểm cuối giúp đưa ra cảnh báo cùng mức độ nguy hiểm với tất cả các hành vi bất thường hoặc tấn công trong thời gian thực.
- Duy trì tất cả các dữ liệu thu thập được tại cơ sở dữ liệu trên máy chủ của khách hàng (On-premise) hoặc máy chủ của Veramine (trên Cloud).
- Lưu trữ thông tin thu thập dài hạn (thậm chí lưu trữ vĩnh viễn không bị xoá) để cho phép điều tra, trích xuất và tìm kiếm dễ dàng trong tương lai
- Tích trữ một bản sao của mọi chương trình đã từng được tải tại bất kì máy nào cũng như trong bất cứ tiến trình nào
- Tìm kiếm trên toàn bộ nhớ của mọi tiến trình đang chạy hoặc các tệp (file), sử dụng Yara, rất hữu ích và chỉ Veramine có.
- Chỉ cần một lần nhấp chuột để truy cập vào bộ nhớ của từng tiến trình hoặc của toàn bộ máy.
- Ứng phó đa dạng chống lại các cuộc tấn công, chẳng hạn bằng cách cô lập một tiến trình đơn lẻ hoặc một máy khỏi toàn bộ hệ thống mạng, chấm dứt kết nối của một người dùng, hoặc ngăn chặn một tệp được thực thi.
- Giảm chi phí xử lý sự cố và điều tra chứng cứ số bằng cách thu thập tất cả các thông tin liên quan đến bảo mật.
- Cài đặt nhanh trên máy Windows bất kì nhờ thực thi đơn giản chương trình cài đặt, không cần thiết tạo cấu hình trên mỗi máy trạm, cho phép triển khai dễ dàng lên hàng ngàn máy.
- Dùng rất ít tài nguyên của hệ thống (< 1% CPU và < 64 MB RAM)

# THUẬT NGỮ

DF (Digital Forensics) là Điều tra Chứng cứ số của Sự cố Bảo mật.

IR (Incident Response) là Ứng phó với Sự cố Bảo mật.

LE (Large Enterprises) là Doanh nghiệp Lớn.

MSSP (Managed Security Service Provider) là Dịch vụ Quản lý An toàn Thông tin.

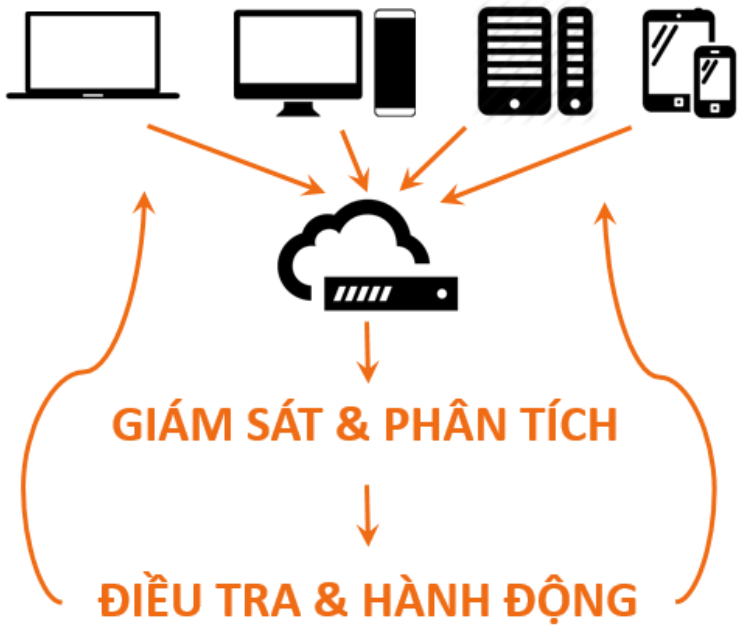
SMB (Small Medium Businesses) là Doanh nghiệp Vừa và Nhỏ.

SOC (Security Operation Center) là Trung tâm Giám sát An ninh mạng.

VEDR (Veramine Endpoint Detection and Reponse) là Giải pháp Cảnh báo và Ứng phó của Veramine.

VSTP (Veramine Security Training Program) là Chương trình Đào tạo An toàn Thông tin của Veramine.

# Tổng quan Sản phẩm




Veramine Platform thu thập hiệu quả tất cả sự kiện liên quan đến bảo mật thông qua cảm biến (sensor) thông minh, và gửi những sự kiện đó tới máy chủ dùng điện toán đám mây của Veramine hoặc đến máy chủ riêng của khách hàng. Máy chủ sử dụng quá trình tự học nâng cao và thuật toán máy học để phát hiện các tấn công như thu thập mật khẩu dùng Mimikatz, khai thác lỗi (kernel-mode exploits), leo thang đặc quyền địa phương (Local Elevation of Privilege - EOP), cấy mã độc vào tiến trình, xâm nhập lan tỏa trái phép và các hoạt động tấn công khác. Máy chủ hiển thị những sự kiện này bằng cả dạng thô và qua giao diện web trực quan cho phép khách hàng có thể tìm kiếm dễ dàng tất cả dữ liệu được thu thập giúp việc xử lý sự cố và chủ động điều tra được hiệu quả hơn. Một người phân tích bảo mật nhận thấy hành vi bất thường có thể dễ dàng chấm dứt hoặc tạm dừng một tiến trình riêng lẻ, cô lập một tiến trình hoặc một máy tính khỏi hệ thống mạng, chấm dứt kết nối hoặc vô hiệu hóa một tài khoản người dùng, hoặc ngăn chặn một chương trình thực thi không được tải. Cảm biến cũng hỗ trợ việc điều tra bộ nhớ bằng cách tải lên máy chủ nội dung bộ nhớ của một tiến trình cụ thể hoặc của toàn bộ một máy tính

# Thu thập thông tin từ các đầu cuối hiệu quả toàn diện

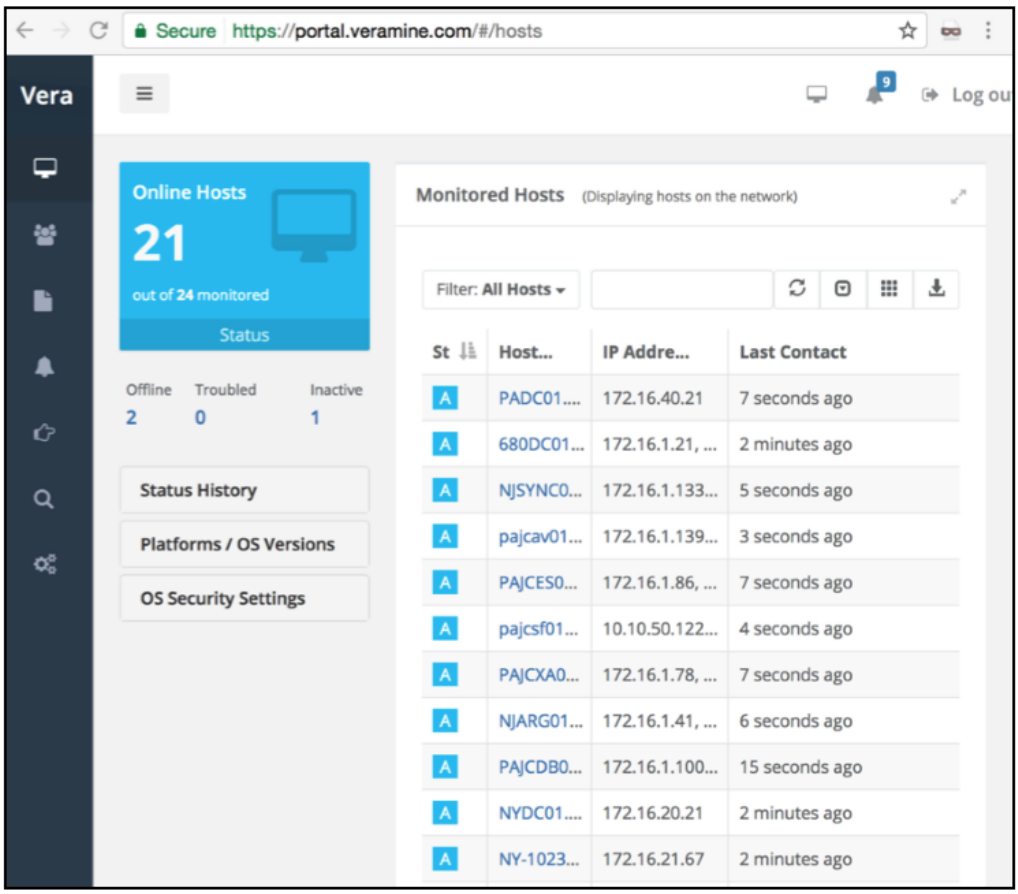



Figure 1 – Hosts View

Điểm mạnh của bất kì sản phẩm EDR phụ thuộc vào phạm vi và tính trung thực của khả năng quan sát và hiển thị những hành vi của các máy. Cảm biến Veramine sử dụng các thành phần ở cả mức người dùng và mức lõi hệ điều hành (kernel) để thu thập và xử lý các sự kiện hệ thống liên quan bảo mật một cách an toàn và đáng tin cậy. Veramine sử dụng nhiều kĩ thuật giảm thiểu tác động tiêu cực vào sự ổn định của hệ thống cũng như hạn chế việc các sản phẩm bảo mật khác nhận nhầm cảm biến của Veramine là một phần mềm độc hại. Cảm biến dùng cho Windows được xây dựng bởi các chuyên gia và kỹ sư lập trình ở mức lõi hệ điều hành đã từng làm việc tại Microsoft, những người đã dành hơn 20 năm điều chỉnh, phát triển và bảo đảm an toàn cho các chương trình chạy trong lõi Windows. Cảm biến được tối ưu hóa không ngừng nghỉ về hiệu suất và hiệu quả để giảm thiểu việc sử dụng tài nguyên tại điểm cuối. Sau lần chạy khởi đầu trong một giai đoạn ngắn gọn, bộ cảm biến tiêu thụ ít hơn 1% CPU. Việc chạy bộ cảm biến trên các máy ảo đám mây yếu nhất (Azure A0 hay AWS t2.nano) có ảnh hưởng không đáng kể đến hoạt động tổng thể của máy.

# PHẠM VI CÁC SỰ KIỆN ĐƯỢC THU THẬP TẠO NÊN SỰ KHÁC BIỆT LỚN GIỮA SẢN PHẨM CỦA VERAMINE VỚI CÁC ĐỐI THỦ CẠNH TRANH.

Sản phẩm Veramine thu thập những thông tin sau đây:

- Sự kiện khởi tạo và kết thúc của các tiến trình
- Sự kiện mở tiến trình, và tạo các luồng thực thi (thread)
- Các tiến trình được tải
- Sự kiện thay đổi cấu trúc quyền hạn (privilege token) của một tiến trình
- Phiên người dùng đăng nhập, đăng xuất, cũng như thay đổi
- Thay đổi thông tin metadata của một file
- Thay đổi các thiếp lập bảo mật của hệ thống
- Các thông tin về registry
- Kết nối mạng
- Tạo, xóa, thay đổi dịch vụ
- Các giao thức và phiên SMB, RDP, SSH, FTP, HTTP
- Việc vi phạm chính sách
- Các thông tin về máy (OS, version, network interface, hardware, dns, drivers)

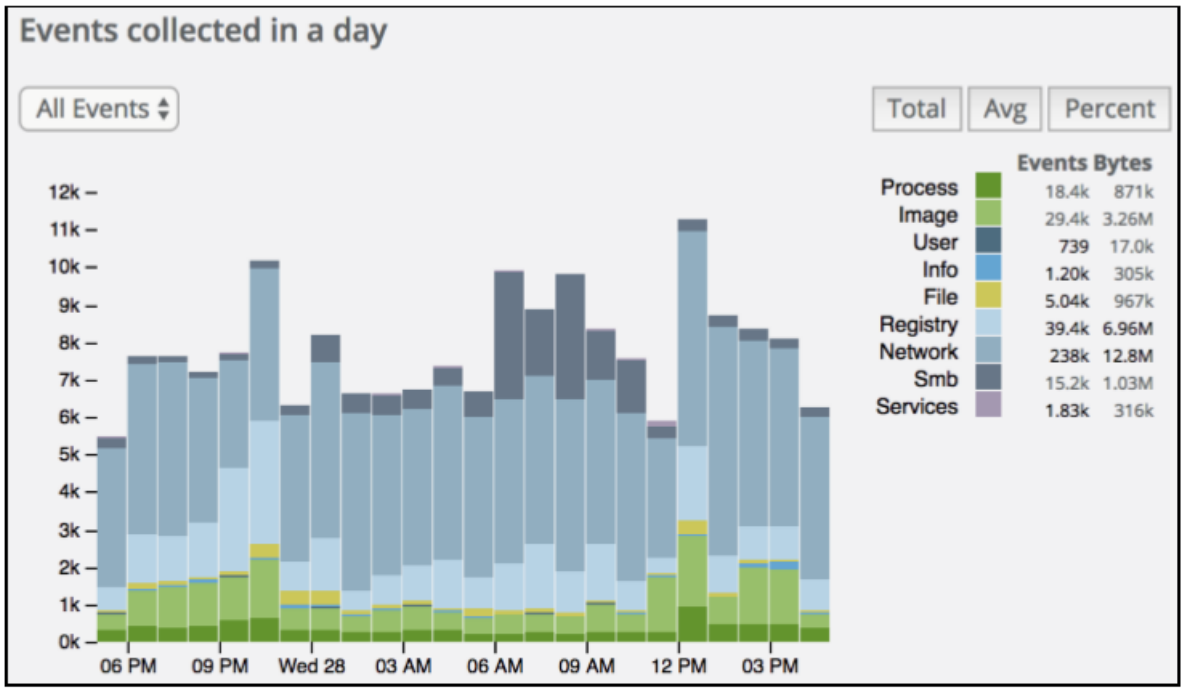



Figure 2 – Example event volume by type of event

Liên tục thu thập mở rộng một loạt các sự kiện hành vi đầu cuối như vậy, nếu làm 1 cách đơn sơ thiếu tinh vi, sẽ làm cạn kiệt tài nguyên cả ở máy trạm và máy chủ đối với một giải pháp EDR điển hình. Rất ít sản phẩm khác cung cấp khả năng thu thập một cách liên tục cùng với việc sử dụng ít tài nguyên của hệ thống đến như vậy. Nhóm Veramine đã đầu tư rất nhiều nỗ lực để phát triển khả năng thu thập có hiệu quả những sự kiện này và lựa chọn các thông tin cần thiết một cách thông minh để gửi từ cảm biến đến máy chủ. Tất cả các chi tiết liên quan hoặc cần thiết đều được các cảm biến gửi đầy đủ đến máy chủ. Cùng như hạn chế các thông tin không cần thiết nên cảm biến cần rất ít lưu lượng mạng. Máy trạm trong điều kiện bình thường có thể chỉ gửi vài trăm kilobyte sự kiện mỗi ngày trong khi các máy trạm có nhiều event cũng chỉ gửi khoảng 100mb mỗi ngày. Khi máy trạm mất kết nối lên máy chủ, sự kiện được lưu lại và đợi cho đến khi chúng có thể được gửi tới máy chủ.

Bộ cảm biến Veramine rất dễ dàng để triển khai và quản lý. Mỗi khách hàng của Veramine được cung cấp một bộ cài đặt đã được cấu hình trước. Với các thông tin tích hợp trong file cài đặt, khách hàng có thể đơn giản cài đặt cảm biến như một quản trị viên trên bất kỳ máy tính nào và nó sẽ bắt đầu gửi các sự kiện - không cần cấu hình! Cảm biến được xây dựng có khả năng ngăn chặn việc bị gỡ bỏ bởi hệ thống bằng mọi cách vô tình hoặc cố ý nào. Bộ cảm biến rất dễ dừng, khởi động, khởi động lại hoặc gỡ bỏ cài đặt từ giao diện web portal.

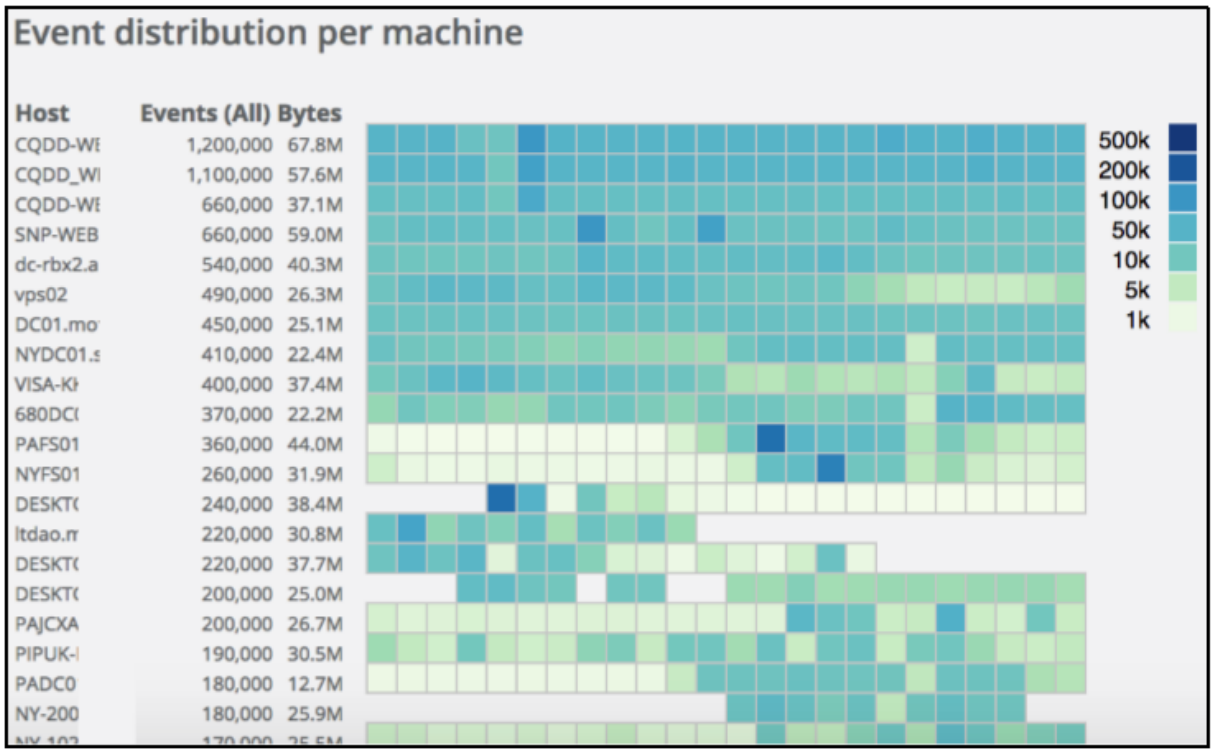



Figure 3 – Example event volume by host

# Phát hiện tự động các mối đe dọa

Các luồng dữ liệu từ cảm biến được phân tích liên tục bởi máy chủ Veramine bằng cách sử dụng nhiều thuật toán dựa trên quy tắc và máy học để xác định hành vi bất thường hoặc khả nghi. Khả năng quan sát và hiển thị toàn diện vào h ành vi đầu cuối có liên quan đến bảo mật cho phép công cụ phát hiện phía máy chủ tìm ra nhiều mối đe dọa an ninh mạng, bao gồm các cuộc tấn công phức tạp khó phát hiện, chẳng hạn như không sử dụng tệp mà chỉ trong các công cụ bộ nhớ.

Sức mạnh của các thuật toán liên tục được củng cố cập nhật. Veramine đặt mục tiêu có khả năng bao quát nhất trong việc phát hiện và cảnh báo những chiến lược chiến thuật và kỹ năng tấn công liệt kê trong ma trận Mitre. Khả năng bao quát ma trận này hiện nay của Veramine được hiển thị ở https://github.com/veramine/Detections/wiki. Hình 4 cho thấy một ảnh chụp màn hình từ wiki đó.

| Persistence | Privilege Escalation | Defense Evasion |
|---|---|---|
| Accessibility Features ✅ | Accessibility Features ✅ | Binary Padding ✅ |
| AppInit DLLs ✅ | AppInit DLLs ✅ | Bypass User Account Control ✅ |
| Authentication Package ✅ | Bypass User Account Control ✅ | Code Signing ✅ |
| Basic Input/Output System ❌ | DLL Injection ✅ | Component Firmware ❌ |
| Bootkit ❌ | DLL Search Order Hijacking ✅ | Component Object Model Hijacking ✅ |
| Change Default File Association ✅ | Exploitation of Vulnerability ✅ | DLL Injection ✅ |
| Component Firmware ❌ | File System Permissions Weakness ✅ | DLL Search Order Hijacking ✅ |
| Component Object Model Hijacking ✅ | Legitimate Credentials ❌ | DLL Side-Loading ✅ |
| DLL Search Order Hijacking ✅ | Local Port Monitor ✅ | Disabling Security Tools ✅ |
| External Remote Services ❌ | New Service ✅ | Exploitation of |

Figure 4 – Screenshot from https://github.com/veramine/Detections

Tính năng phát hiện xâm nhập cũng được hỗ trợ bởi nền tảng máy học của Veramine được thiết kế với khả năng mở rộng, nâng cấp và tương tác. Nó sử dụng công nghệ dữ liệu lớn để đánh giá dòng dữ liệu cảm biến và có thể tích hợp tất cả các kỹ thuật máy học được viết bằng các ngôn ngữ khác nhau để xử lý bất kỳ vấn đề dữ liệu nào, đồng thời cung cấp các giám sát học tập (learning) khác nhau. Ví dụ, 3 loại phát hiện sau được xây dựng dựa trên các chuỗi thuật toán máy học khác nhau:

- Hồ sơ hoạt động của tiến trình: theo dõi các chỉ tiêu lịch sử của mỗi tiến trình theo tên tiến trình và cảnh báo về sự phân kỳ từ các định mức đã được thiết lập.
- Lấy cắp dữ liệu ra ngoài: theo dõi lịch sử sử dụng mạng của từng tiến trình theo tên và cảnh báo về phân kỳ.
- Theo dõi người dùng: theo dõi các mẫu hành vi đăng nhập cho mỗi người dùng và cảnh báo về sự bất thường.

Hình 5 cho thấy một mẫu phát hiện của Veramine kết quả từ một kẻ tấn công lấy trộm các chứng chỉ bảo mật trên máy tính của khách hàng sử dụng công cụ Powershell Invoke - Mimikatz. Công cụ phát hiện Veramine quan sát tiến trình Powershell.exe đã mở bộ nhớ của tiến trình lsass.exe, một trong những cảnh báo chính xác cao nhất của hành vi trích xuất mật khẩu. Kết quả phát hiện bao gồm tất cả các thông tin cần thiết để điều tra tình huống này - tiến trình đáng ngờ (powershell.exe), tiến trình đang được mở (lsass.exe), máy tính trên đó các tiến trình đã được chạy, và người dùng thực hiện tiến trình đáng ngờ. Các trang chi tiết được liên kết để xử lý và hiển thị tất cả các mô đun đã tải, mọi kết nối mạng, tiến trình mẹ, và bất kỳ tiến trình con nào, v.v …

| Time | Description | Host | User |
|---|---|---|---|
| 5/9/17 2:10:00am | powershell.exe (PID 6768), a Microsoft-signed "Container" process, opened process memory of lsass.exe (PID 580). This process could be being used by attackers to dump credentials stored in memory. | \DC01 | |
| 5/9/17 1:47:23am | powershell.exe (PID 7748), a Microsoft-signed "Container" process, opened process memory of lsass.exe (PID 552). This process could be being used by attackers to dump credentials stored in memory. | 0DC01 | |

Figure 5 –Veramine detection example

# Điều tra tìm kiếm dễ dàng các thông tin tấn công

Luồng dữ liệu cảm biến chắc chắn hữu ích cho việc phát hiện. Tuy nhiên, thông tin thu thập được cũng được trình bày trên giao diện web của khách hàng cùng với các thông tin hữu ích được chắt lọc, kết nối và bổ sung. Giao diện web này cho phép người dùng thực hiện các tìm kiếm đặc biệt để tìm ra các câu trả

lời giúp tạo điều kiện và tăng sức mạnh cho các cuộc điều tra cũng như khả năng phản ứng với các cuộc xâm nhập và cũng cho phép tìm kiếm các mối đe dọa có hiệu quả. Một số khách hàng đã đề cập đến khả năng này là "giống như trình duyệt tiến trình SysInternals trên web đang chạy trên mọi máy tính".

Để điều tra việc phát hiện Powershell.exe độc hại ở trên, chúng ta bắt đầu với trang chi tiết tiến trình để xem toàn bộ cây tiến trình, bao gồm bất kỳ tiến trình con nào được kích hoạt bởi powershell.exe độc đó. Hình 6 cho thấy khung nhìn này.

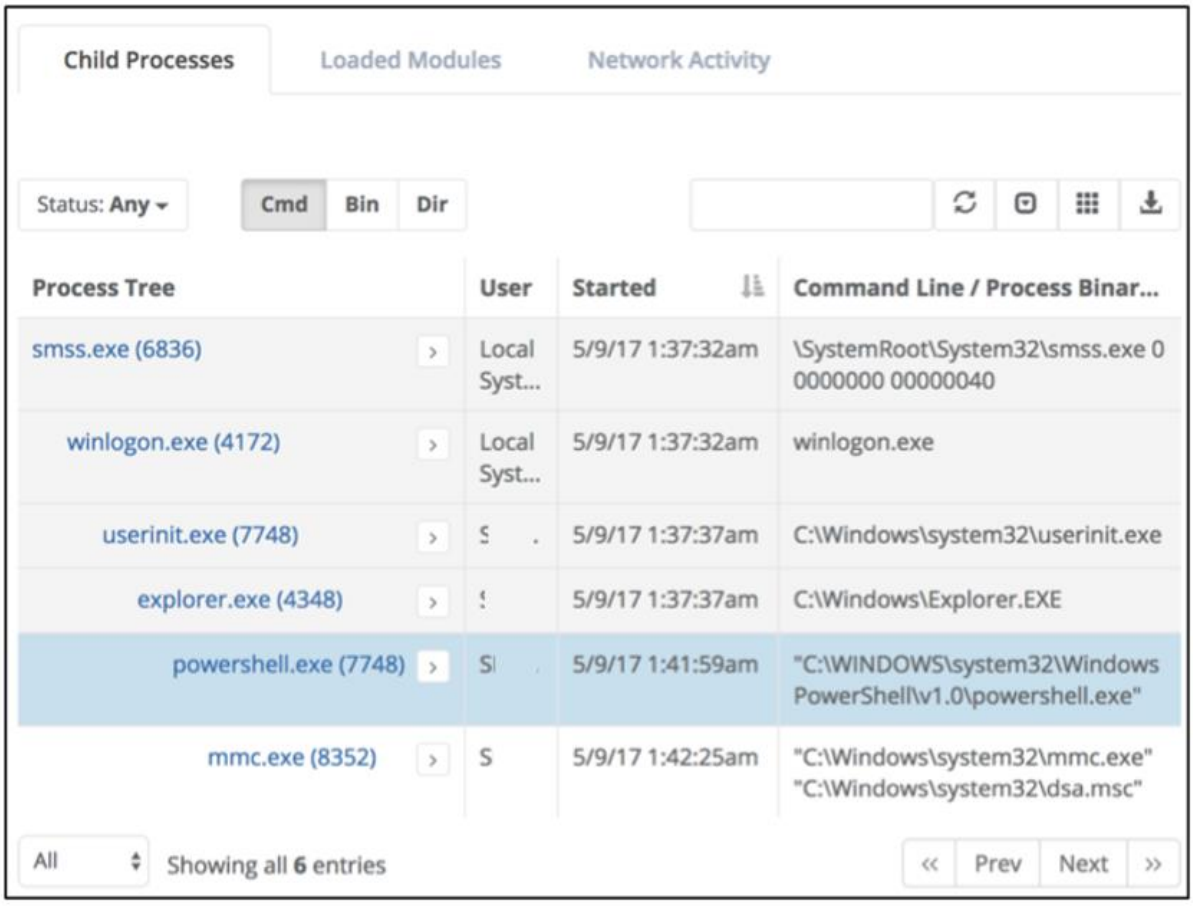



Figure 6 –Process Detail page "Child Processes" tab

Nhấp vào **liên kết** giám sát viên của tiến trình mẹ explorer.exe (PID 4348) sẽ hiển thị các tiến trình đồng đẳng khác cho tiến trình độc hại powershell.exe (PID 7748), các tiến trình được đưa ra bởi cùng một mẹ. Nó chỉ là một vài cú nhấp chuột trong giao diện Tìm kiếm tiến trình của Veramine để tìm các hoạt động liên quan đến tiến trình, chẳng hạn như sau:

- Tất cả các tiến trình được khởi chạy trong các máy trên hệ thống bằng cùng một tài khoản người dùng đã bị xâm nhập
- Tất cả các tiến trình được khởi chạy cùng thời gian trên cùng các máy tính như Powershell độc hại.
- Tất cả các tiến trình con của PowerShell.exe được khởi chạy trên các máy tính của cùng một người dùng bất cứ lúc nào.

Hình 7 cho thấy một ảnh chụp màn hình ví dụ của giao diện tìm kiếm. Khách hàng cụ thể này có thể sử dụng giao diện tìm kiếm của Veramine để xác định các tiến trình độc hại khác, người dùng bị xâm nhập và các hệ thống bị xâm nhập khác. Khả năng quan sát và hiển thị này cho phép họ xác định được mọi đặc điểm chính trong mỗi phiên người dùng của kẻ tấn công để dễ dàng theo dõi và quan sát mọi hành động của kẻ tấn công trên mạng này.

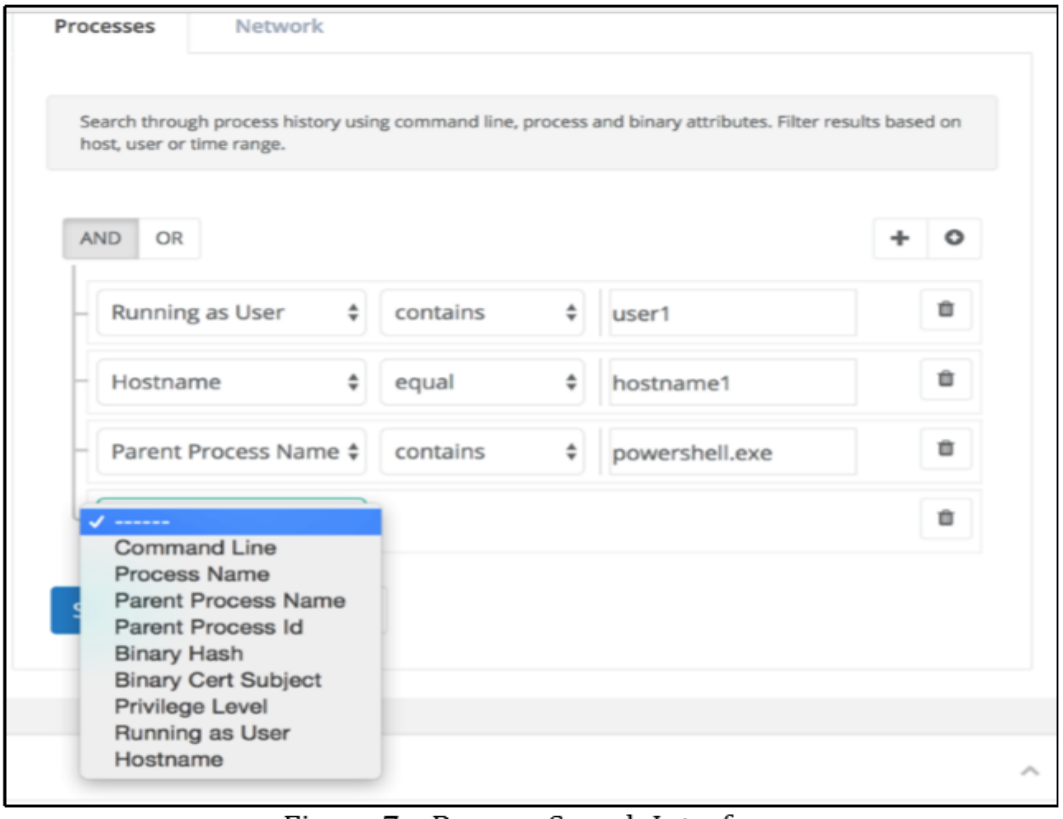



Figure 7 – Process Search Interface

# Đẩy nhanh quá trình phản hồi

Nền tảng Veramine cung cấp các tính năng điều khiển và phản hồi để cho phép phản hồi sự cố nhanh chóng và hiệu quả từ bảng điều khiển trung tâm. Những người giám sát và phân tích có thể gửi hành động phản ứng tới bộ cảm biến Veramine để tương tác với các tiến trình, tệp chạy, người dùng và máy tính.

Các hành động ứng phó liên quan đến tiến trình hiện đang có sẵn, như thể hiện trong hình 8:

- Tạm dừng hoặc chấm dứt bất kỳ tiến trình đang chạy.
- Tạo và tải nội dung bộ nhớ của tiến trình lên máy chủ Veramine.
- Ngăn chặn một tiến trình thực hiện bất kỳ kết nối mạng đi

Ngoài các lệnh xử lý riêng lẻ này, bộ cảm biến Veramine hỗ trợ khả năng tìm kiếm trên bộ nhớ thông qua các luật Yara.

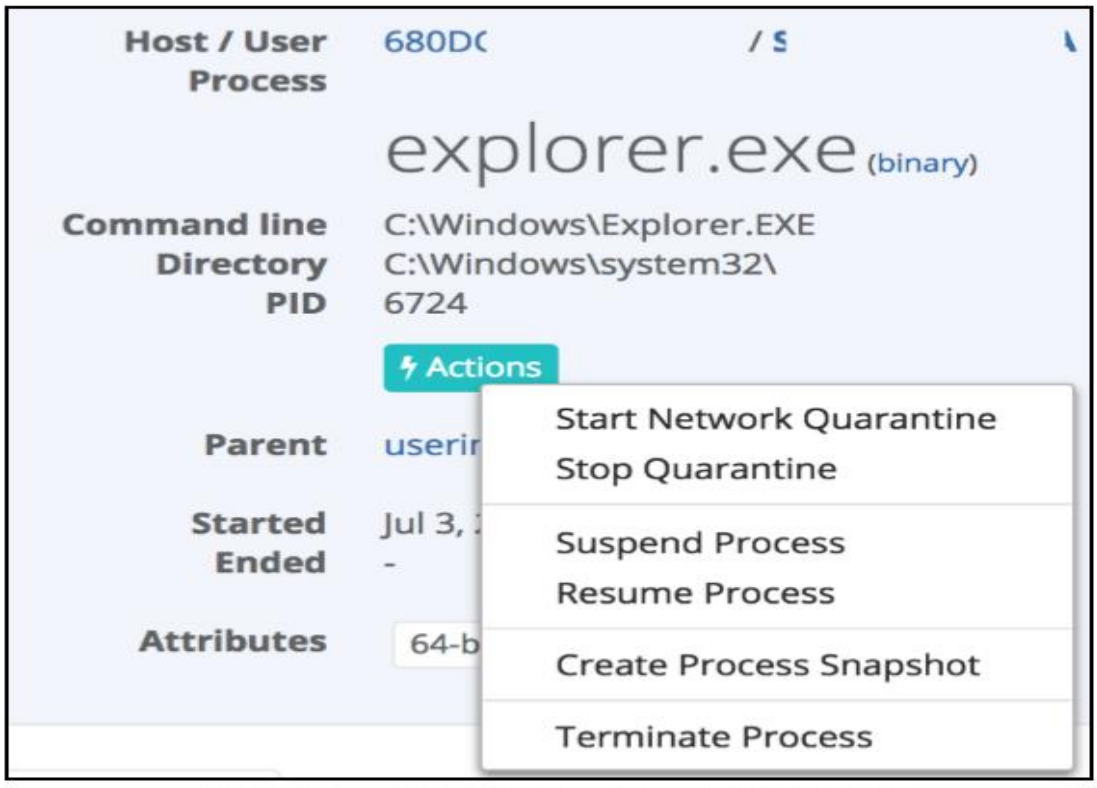



Figure 8 – Running Process Sensor Actions

Cảm biến Veramine cung cấp các hành động với tệp chạy, như thể hiện trong hình 9:

Ngăn chặn một tệp chạy không được tải nạp bởi bất kỳ tiến trình nào.

Sau khi tải một tệp chạy, ngăn tiến trình được tải đó kết nối mạng đi.

Nền tảng Veramine cũng giữ lại một bản sao của mỗi tệp chạy được tải bởi bất kỳ tiến trình nào và làm cho tệp đó có sẵn để tải xuống từ giao diện web của Veramine.

Cảm biến Veramine cũng cung cấp một số hành động liên quan đến người dùng. Nó có thể vô hiệu hóa hoặc kích hoạt một tài khoản người dùng cục bộ hoặc ngắt kết nối một phiên đăng nhập RDP của người dùng cụ thể.


Figure 9 – Binary Sensor Actions

## Cuối cùng, cảm biến Veramine cung cấp các hành động liên quan đến máy tính, như thể hiện trong hình 10:

- Tắt nguồn, Khởi động lại, hoặc cho máy ngủ.
- Ngăn không cho máy trạm thực hiện các kết nối mạng đi đến các điểm đến khác ngoài máy chủ.
- Gỡ cài đặt cảm biến.

Hành động Gỡ cài đặt bộ cảm biến được đề cập cụ thể bởi vì thông qua cổng thông tin web là cách duy nhất để gỡ cài đặt cảm biến sản phẩm. Phiên bản thử nghiệm của bộ cảm biến Veramine có thể được gỡ bỏ một cách dễ dàng bằng câu lệnh command.

Tuy nhiên, phiên bản sản phẩm của bộ cảm ứng chống lại những nỗ lực tấn công từ các phần mềm độc hại khác để ngăn chặn việc hoạt động của cảm biến. Các sản phẩm cạnh tranh có thể bị vô hiệu hóa trên máy tính đã bị xâm nhập nhưng nền tảng của Veramine có khả năng chống lại các cuộc tấn công trên máy tính nhằm vào cảm biến.

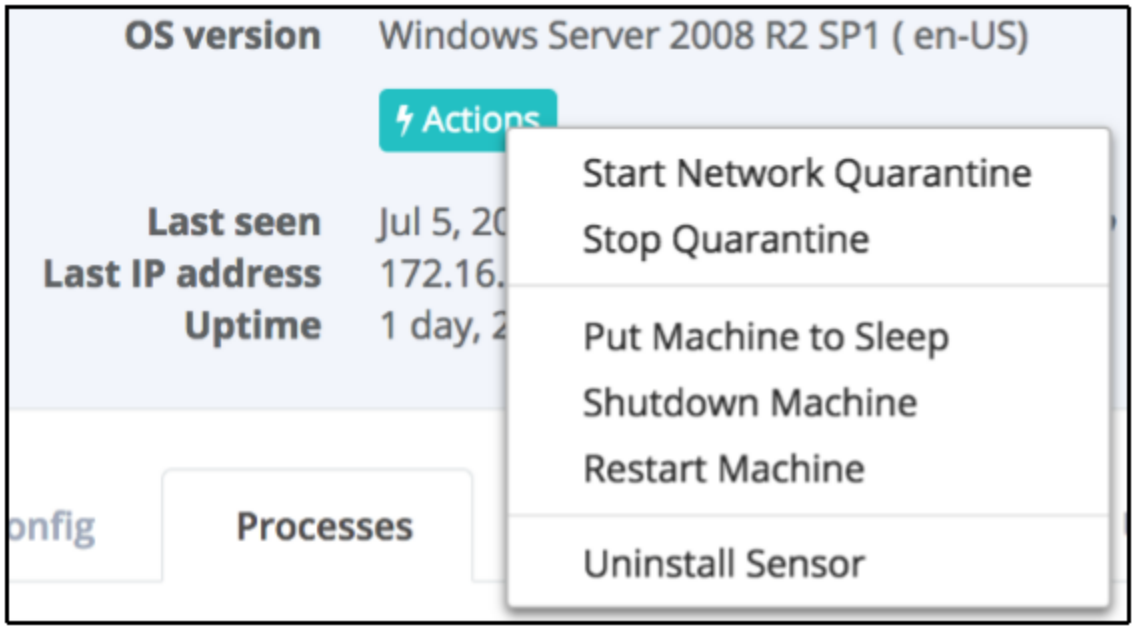



Figure 10 – Host Sensor Actions

# Những đặc tính khác

## 1 | Hiệu suất (Performance)

Veramine Sensor cho máy trạm thì rất gọn nhẹ (lightweight), có lẽ không thua kém bất kỳ sản phẩm nào trên thế giới, tiêu tốn rất ít, hầu như không tốn CPU (< 1%), và khoảng 5 - 64 MB RAM tùy theo lượng tiến trình và ứng dụng đang chạy ở máy trạm.

## 2 | Khả năng Mở rộng (Scalability)

Máy chủ cũng sử dụng những công nghệ big data để tính toán và lưu trữ thông tin, nên cho phép mở rộng theo chiều ngang (horizontal scalibity): có thể phục vụ nhiều máy trạm hơn bằng cách lắp đặt thêm nhiều máy chủ trong một hệ thống phân phối (distributed system). Đồng thời VEDR cũng có khả năng phân bố dữ liệu trên các máy chủ dựa trên vị trí địa lý của vùng miền khác nhau.

## 3 | Triển khai (Deployment)

VEDR có cả bản Đám mây (Cloud) và bản Nội bộ (On-Premise). Sensor gọn nhẹ có thể được cài đặt rất dễ dàng, với 1 dòng lệnh 'phantom -install', nên sensor có thể được triển khai rất nhanh chóng cho khách hàng với 1 hoặc 2 máy, hoặc hàng ngàn máy bằng cách dùng psexec, SCCM, AD group policy, startup script và các phương pháp khác.

Cho 1000 máy trạm trong 1 hệ thống thì có thể triển khai trong vòng 1 tuần, và có thể cần 2 hoặc 3 người sử dụng sản phẩm.

# Veramine Inc.

## Dùng thử hoàn toàn miễn phí ngay hôm nay

Gửi yêu cầu tới contact@veramine.com để bắt đầu dùng thử miễn phí ngay hôm nay. Chỉ mất vài phút để chúng tôi có thể cấu hình các thành phần phía máy chủ và gửi một liên kết để tải về một bộ cảm biến được tùy chỉnh chỉ dành cho bạn.

## Giới thiệu Công ty Veramine

Veramine được thành lập ở Seattle bởi những chuyên gia bảo mật chủ chốt của Microsoft trong nhiều năm. Đây là những người đã lãnh đạo công việc ứng phó, vá lỗi, và cập nhật về bảo mật cho tất cả sản phẩm của Microsoft. Hơn nữa, họ cũng chịu trách nhiệm việc kiểm tra an toàn (Penetration Testing) những sản phẩm quan trọng nhất của Microsoft như Windows, Office, Azure, Xbox... Họ là khách mời nói chuyện ở nhiều sự kiện bảo mật danh tiếng nhất như Black Hat, Chaos Computer Club (CCC), ReCon, NATO Cyber Defense, RSA, (https://www.youtube.com/watch?v=rOwMW6agpTI). Và họ cũng đã viết những cuốn sách chuyên sâu về bảo mật được đánh giá rất cao, chẳng hạn là cuốn sách đứng đầu trên Amazon.com về dịch ngược mã độc (https://www.amazon.com/s/ref=nb_sb_noss_2?url=search-alias%3Daps&field-keywords=reverse+engineering).

Veramine đã được hợp đồng xây dựng giải pháp Cybersecurity của Không quân Mỹ (U.S. Air Force) https://www.federaltimes.com/2016/07/28/air-force-awards-contract-for-deceptive-cyber-research/. Veramine cũng được hợp đồng xây dựng giải pháp Cybersecurity của Bộ An Toàn Nội Địa Mỹ (U.S. Department of Homeland Security - DHS), như được thông báo trên Wall Street Journal Pro https://www.linkedin.com/pulse/cyber-matters-dhs-aims-help-secure-critical-jonathan-ness, đồng thời được DHS lựa chọn và tiến cử (recommended) là nền tảng tin dùng cho các khách hàng trong ngành tài chính và ngân hàng của DHS. Tiếp theo, sản phẩm Veramine được hợp đồng bảo vệ hệ thống thông tin cho hội nghị APEC 2017 (Asia-Pacific Economic Cooperation Forum https://www.apec2017.vn) và hợp đồng với Bộ Quốc phòng Singapore.

Sản phẩm Veramine đã được sử dụng nhiều nơi ở Mỹ, châu Âu và Việt nam, và rất hiệu quả trong việc phát hiện, cảnh báo và ứng phó với những cuộc tấn công xâm nhập mạng APT tinh vi. Veramine đã có kinh nghiệm thực tế sử dụng sản phẩm để phát hiện, ứng phó và điều tra nhiều vụ tấn công xâm nhập, của nhiều tổ chức lớn và quan trọng trên thế giới. Đáng chú ý là các tổ chức này đều đã sử dụng các giải pháp cybersecurity của các hãng bảo mật danh tiếng nhất thế giới, nhưng không hề phát hiện ra những vụ xâm nhập này, thậm chí những giải pháp này còn bị lợi dụng để mã độc ngụy trang, hoặc truyền ra dữ liệu đánh cắp, hoặc phát tán lên cả hệ thống. Hiện nay nhu cầu bảo vệ an toàn Hệ thống Thông tin ở Việt Nam là rất cấp thiết và cần được đáp ứng tốt nhất. Theo những báo cáo như của Microsoft và CrowdStrike, Việt nam nằm trong những nước bị tấn công mạng và bị nhiễm mã độc nhiều nhất thế giới.