



VERAMINE CYBER DEFENSE SYSTEM (VCDSP) PREMIUM

Version 1.8



Thu thập hiệu quả và toàn diện dữ liệu về hoạt động trên điểm cuối

Phát hiện tự động các mối đe dọa không biết trước

Điều tra các dấu hiệu bị tấn công dễ dàng

Tăng tốc xử lý sự cố đa dạng

NOVEMBER 18, 2019

Mục lục

a. Lợi ích chính dành cho khách hàng	2
b. Thuật ngữ.....	3
1. Tổng quan Sản phẩm	4
2. Thu thập thông tin từ các đầu cuối hiệu quả toàn diện	5
3. Phát hiện tự động các mối đe dọa	8
4. Điều tra tìm kiếm dễ dàng các thông tin tấn công.....	10
5. Đẩy nhanh quá trình phản hồi	12
6. Hệ thống Bẫy đa năng.....	15
7. Những đặc tính khác	17

a. Lợi ích chính dành cho khách hàng

1. 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.
2. 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 có chủ đích APT trong thời gian thực.
3. 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).
4. Lưu trữ thông tin thu thập để cho phép xử lý tập trung, phân tích, điều tra, trích xuất và tìm kiếm dễ dàng trong tương lai.
5. Cung cấp giao diện khép kín để điều tra các cuộc tấn công: Detection – Investigation – Response.
6. 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
7. Chỉ cần một lần nhấp chuột để truy cập vào bộ nhớ của từng tiến trình hoặc của toàn bộ máy.
8. 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.
9. 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.
10. 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.
11. Dùng rất ít tài nguyên của hệ thống (< 1% CPU và < 64 MB RAM) để thu thập và xử lý các cuộc tấn công, mã độc thông thường và tinh vi

b. 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.

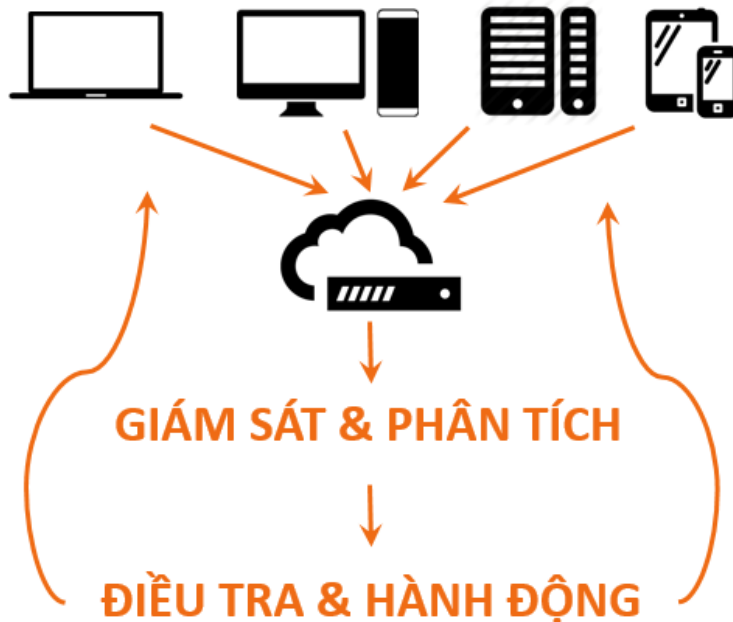
LE (Large Enterprises) là Doanh nghiệp Lớn.

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.

1. 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 các thuật toán nâng cao 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. Các thông số chức năng như sau.

Hệ thống phần mềm quản lý và tùy biến báo cáo

- Lưu trữ các loại dữ liệu về hoạt động của hệ thống: file chạy, trạng thái bộ nhớ, đăng nhập người dùng... cho công tác phân tích và điều tra.
- Phân tích để phát hiện tấn công, xâm nhập và các dấu hiệu bất thường.
- Điều tra và hiển thị toàn bộ phạm vi và diễn biến của những sự kiện.
- Đưa ra các mệnh lệnh để ngăn chặn và loại bỏ các mã độc các loại tấn công từ một màn hình quản trị duy nhất
- Tạo các loại bẫy đa dạng để đánh lừa phát hiện và ngăn cản các mã độc và tấn công mạng
- Sử dụng hệ thống học máy để phân tích bất thường

- Cung cấp báo cáo liên tục trên hệ thống báo cáo trung tâm

Hệ thống phần mềm trên các End-point

- Hỗ trợ nhiều số lượng end point khác nhau, như 100, 1000 hay 10 000 endpoint.
- Thu thập tất cả những hành vi trong các máy tính và máy chủ Windows của người dùng, trong thời gian thực, triết xuất, thu thập và hiển thị dữ liệu chi tiết về những hành vi này, cho các máy (machines), chương trình (applications), tiến trình (processes), người dùng (users), kết nối mạng (network connections), chia sẻ dữ liệu (SMB data sharing), tệp tin chạy (binaries)...
- Thực hiện các mệnh lệnh để loại bỏ và ngăn chặn mã độc và các cuộc tấn công mạng.

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

The screenshot shows the Vera Hosts View interface. On the left, a sidebar contains navigation icons. The main content area is divided into two sections. The top section, 'Online Hosts', displays a large number '21' indicating the count of online hosts out of 24 monitored. Below this, there are status indicators for 'Offline' (2), 'Troubled' (0), and 'Inactive' (1). The bottom section, 'Monitored Hosts', displays a table of hosts currently on the network. The table has columns for 'St' (Status), 'Host...', 'IP Address...', and 'Last Contact'. The table lists 12 hosts, each with a status icon (a blue square with a white 'A'), a host name, an IP address, and the time since the last contact.

St	Host...	IP Address...	Last Contact
A	PADC01...	172.16.40.21	7 seconds ago
A	680DC01...	172.16.1.21, ...	2 minutes ago
A	NJSYNC0...	172.16.1.133...	5 seconds ago
A	pajcav01...	172.16.1.139...	3 seconds ago
A	PAJCES0...	172.16.1.86, ...	7 seconds ago
A	pajcsf01...	10.10.50.122...	4 seconds ago
A	PAJCXA0...	172.16.1.78, ...	7 seconds ago
A	NJARG01...	172.16.1.41, ...	6 seconds ago
A	PAJCDB0...	172.16.1.100...	15 seconds ago
A	NYDC01...	172.16.20.21	2 minutes ago
A	NY-1023...	172.16.21.67	2 minutes ago

Figure 1 – Hosts View

Điểm mạnh của sản phẩm bảo mật 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 kỹ 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 thiết lập bảo mật của hệ thống
- Các thông tin về registry
- Kết nối mạng
- Tạo, xóa, thay đổi dịch vụ
- Phiên SMB và các giao thức liên quan
- Việc vi phạm chính sách
- Các thông tin về máy

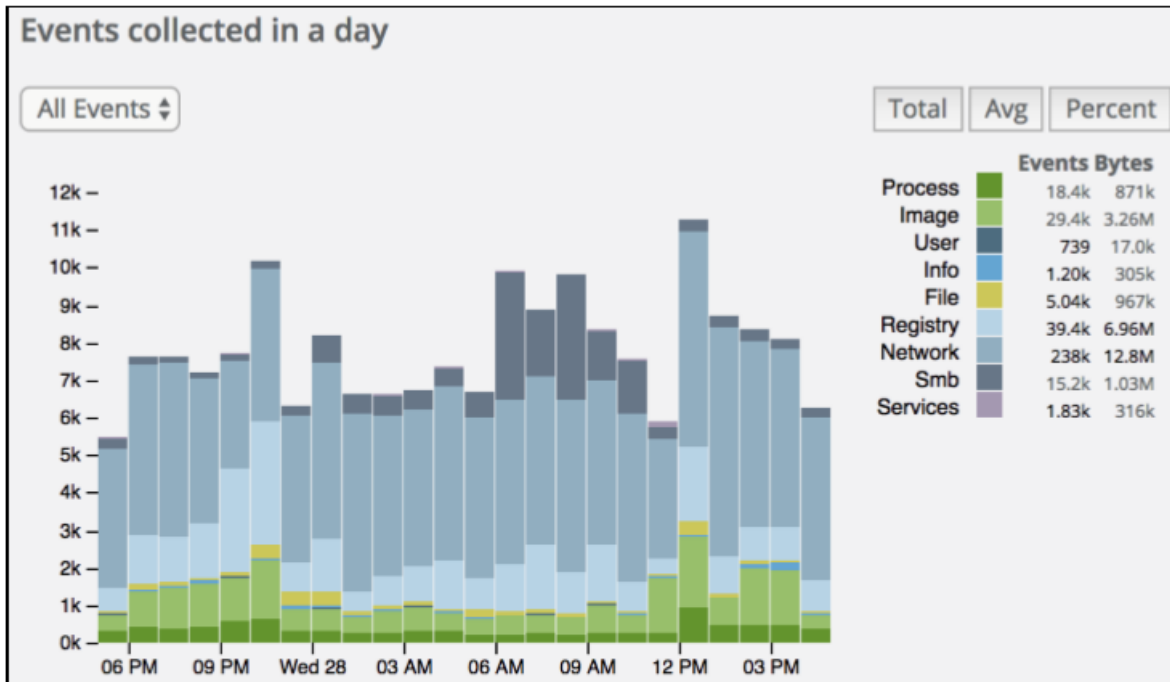


Figure 2 – Example event volume by type of event

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 điểm cuối 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.

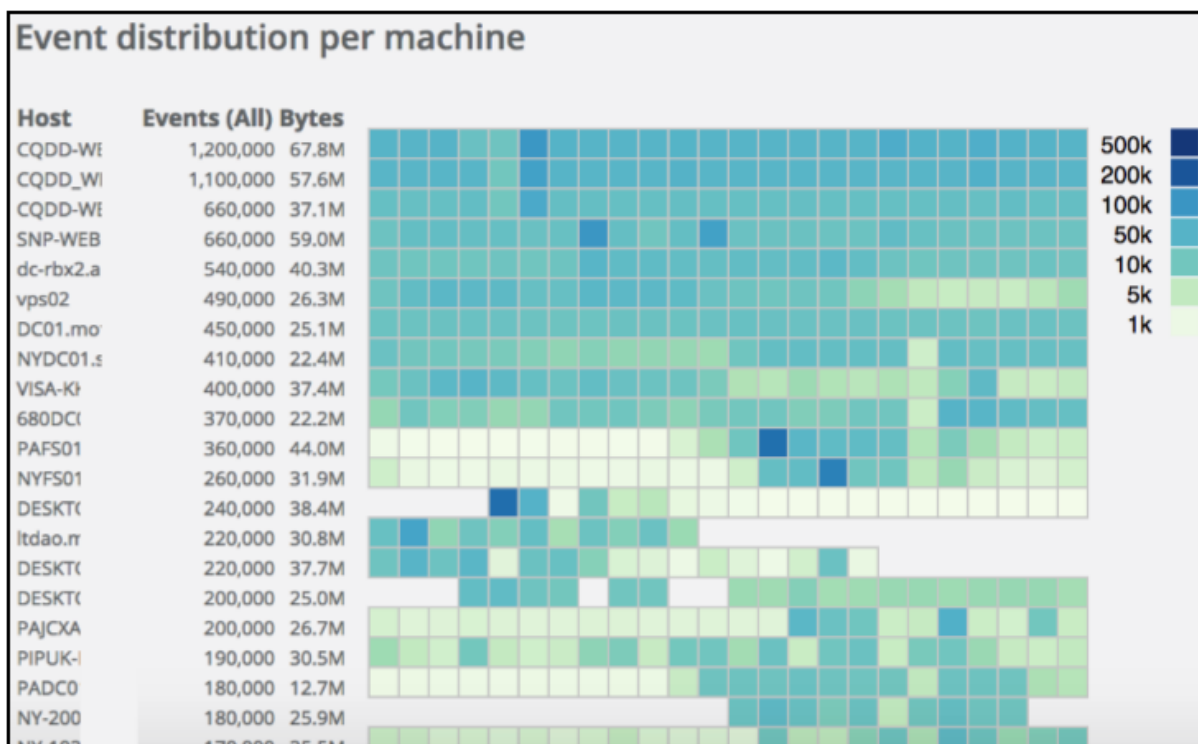


Figure 3 – Example event volume by host

3. 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 để xác định hành vi bất thường hoặc khả nghi. Khả năng quan sát và hiển thị toàn diện vào hành 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.

Các mối đe dọa có thể được phát hiện dựa trên quy tắc (rule), phân tích hành vi (behavioral analytics): cho phép khám phá các hành vi tấn công và xác định các dấu hiệu xâm phạm dựa trên việc sử dụng các quy tắc được định nghĩa trước. Một hành vi hoặc một chuỗi các hành vi dẫn đến việc vi phạm các quy tắc được định nghĩa sẽ được coi là dấu hiệu tấn công, xâm phạm. Việc phát hiện có thể được tăng cường bởi việc kết hợp với thông tin từ các nguồn thông tin tình báo mạng.

Các mối đe dọa cũng có thể được phát hiện dựa trên các thuật toán máy học (machine learning): sử dụng công nghệ dữ liệu lớn kết hợp với các thuật toán máy học để đánh giá các thông tin thu thập được từ các điểm cuối để xác định các bất thường về một hay nhiều khía cạnh so với baseline đã được hồ sơ hóa trong quá trình học. Việc sử dụng các thuật toán máy học cho phép phát hiện ra các mẫu của các mối đe dọa chưa được biết đến đồng thời giảm thiểu tối đa các cảnh báo sai.

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.

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 ...

Persistence	Privilege Escalation	Defense Evasion
Accessibility Features ✓	Accessibility Features ✓	Binary Padding ✓
Applnit DLLs ✓	Applnit 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>

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.	\\DC01	...

Figure 5 –Veramine detection example

4. 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 chất lọc, kết nối và bổ sung. Giao diện web này cho phép người dùng thực hiện các tìm kiếm đặc biệt về các hoạt động của hệ thống và người dùng, 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".

Các dữ liệu tại một thời điểm bất kỳ (tối thiểu trong vòng 6 tháng) trên bất kỳ điểm cuối nào đã được cài đặt cảm biến đều có thể được trích xuất, để hỗ trợ việc điều tra giám định, kể cả trong trường hợp điểm cuối đã offline hoặc không còn tồn tại tại thời điểm thực hiện việc điều tra.

Việc chủ động săn tìm các mối đe dọa (threat hunting) cần được hỗ trợ thông qua tính năng tìm kiếm trên bộ nhớ của host hoặc tiến trình sử dụng công cụ tìm kiếm dựa trên YARA, và hỗ trợ dump memory. Việc tìm kiếm có thể được thực hiện trên một điểm cuối hoặc đồng thời trên nhiều điểm cuối.

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.

Child Processes				Loaded Modules	Network Activity
Status: Any ▾				Cmd Bin Dir	
Process Tree		User	Started	Command Line / Process Binar...	
smss.exe (6836)	>	Local Syst...	5/9/17 1:37:32am	\SystemRoot\System32\smss.exe 00000000 00000040	
winlogon.exe (4172)	>	Local Syst...	5/9/17 1:37:32am	winlogon.exe	
userinit.exe (7748)	>	S	5/9/17 1:37:37am	C:\Windows\system32\userinit.exe	
explorer.exe (4348)	>	S	5/9/17 1:37:37am	C:\Windows\Explorer.EXE	
powershell.exe (7748)	>	SI	5/9/17 1:41:59am	"C:\WINDOWS\system32\Windows PowerShell\1.0\powershell.exe"	
mmc.exe (8352)	>	S	5/9/17 1:42:25am	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\dsa.msc"	
All ▾		Showing all 6 entries		<< Prev Next >>	

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.

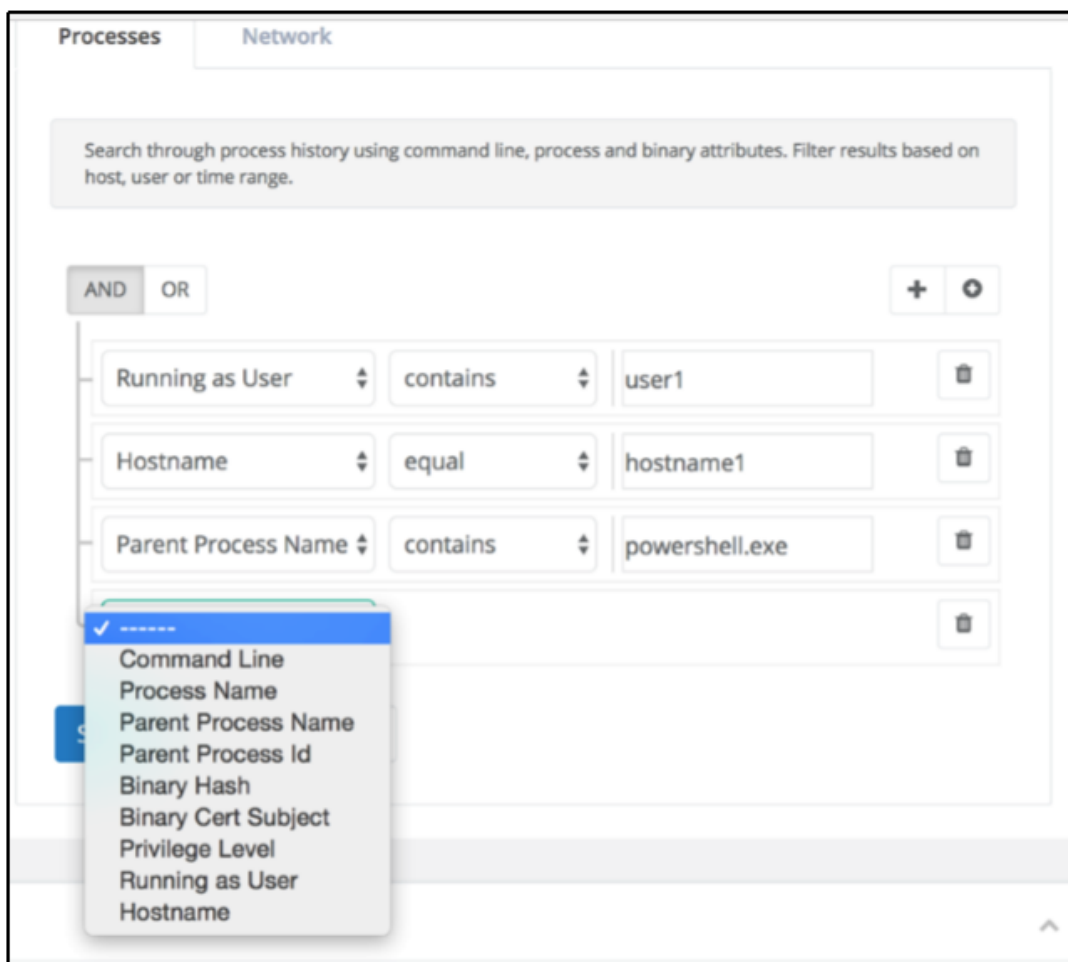


Figure 7 – Process Search Interface

5. 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

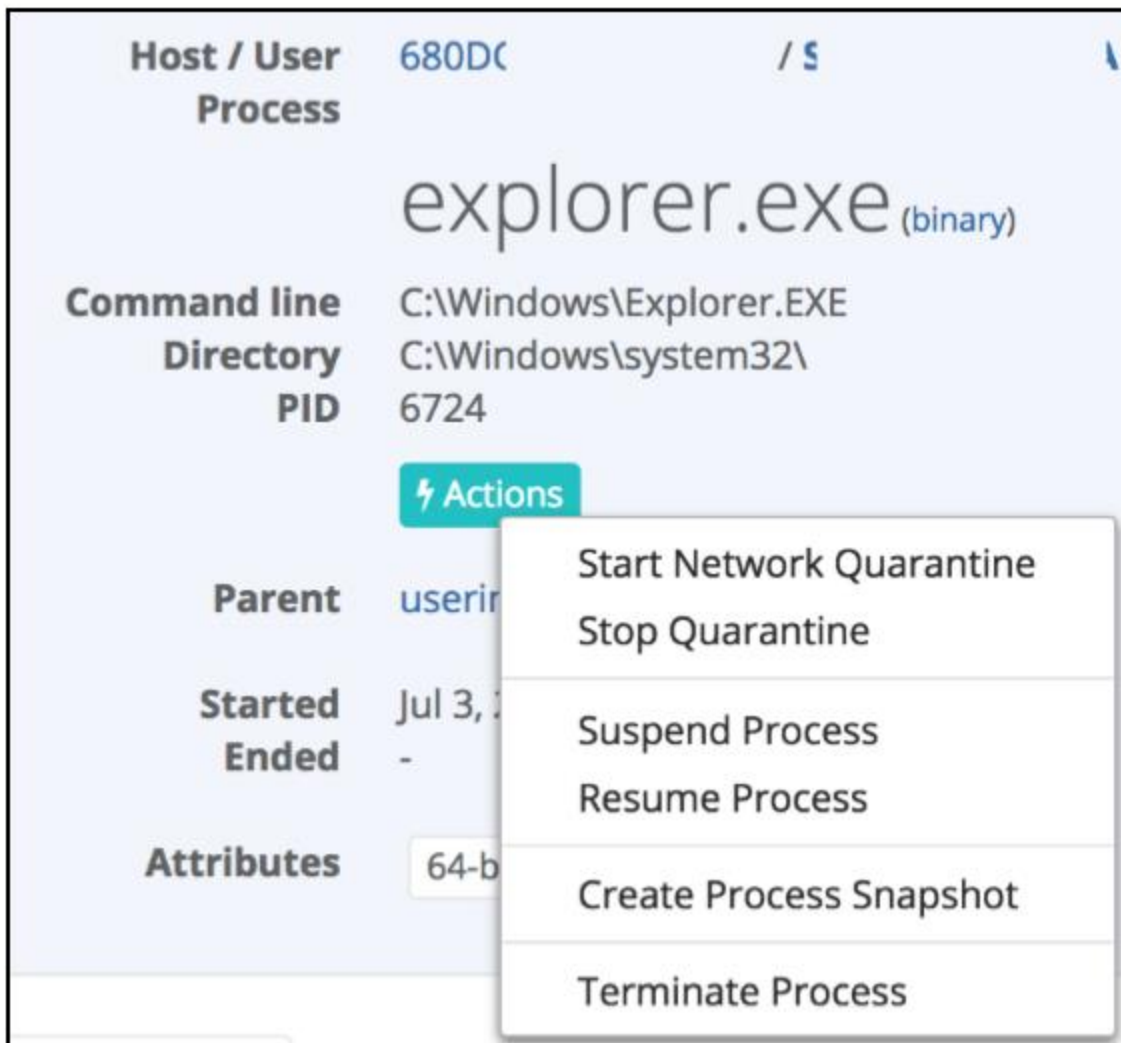


Figure 8 – Running Process Sensor Actions

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 chủ 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.

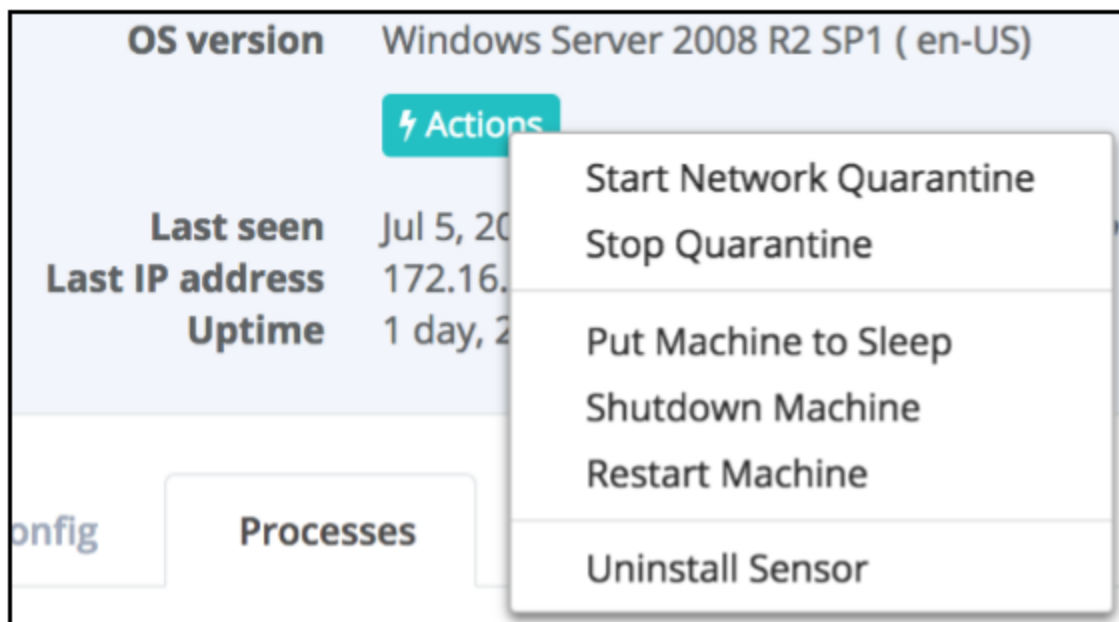


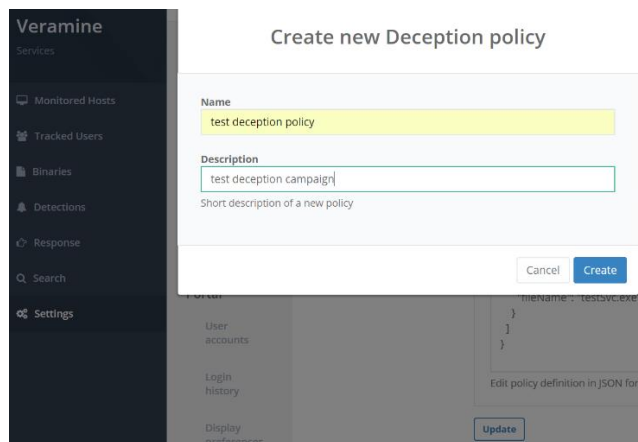
Figure 10 – Host Sensor Actions

6. Hệ thống Bẫy đa năng

Hệ thống Bẫy được duy nhất Veramine phát triển có thể được triển khai tới bất kỳ tập hợp máy tính nào trong hệ thống IT, là phương pháp hiện đại phòng thủ chủ động để chống tấn công mạng. Phần lớn các phương pháp bảo mật hiện nay là phòng thủ bị động. Hệ thống bẫy của Veramine có thể biến bất kỳ máy tính nào thành honeypot, đặt dọ theo kill chain để đánh lừa, phát hiện và ngăn chặn xâm nhập mạng. Trong phương thức triển khai bẫy, các chiến thuật được liệt kê và cập nhật dùng json qua portal (Settings, Policies, Deception).

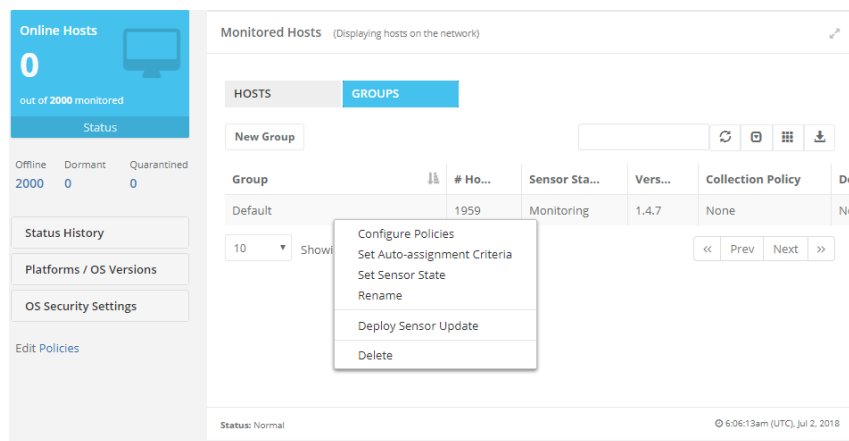
Cài đặt Chính sách Bẫy

Những chiến thuật bẫy đã được làm sẵn và triển khai ngay. Tạo 1 chiến thuật bẫy mới bằng nhấn chuột vào “New Policy”, điền thông tin yêu cầu và chọn “Create”.



Chính sách Bẫy

Chính sách được cập nhật bằng thay đổi JSON và nhấn vào “Update”.



Chọn chính sách triển khai tới 1 nhóm

Để triển khai 1 chiến thuật, chọn “Groups” tab, nhấn chuột phải vào group và chọn “Configure Policies”.

Sau đó chọn chính sách bẫy từ danh sách và nhấn vào “Update.”

Gỡ cài đặt 1 chính sách bằng chọn “None” và nhấn “Update”.

Bẫy dịch vụ

Đây là JSON mô tả 2 bẫy dịch vụ,

```
{
  "services": [
    {
      "name": "testSvc",
      "displayName": "test display name",
```

```

    "fileName": "testSvc.exe"
  },
  {
    "name": "testSvc2",
    "displayName": "test2 display name",
    "fileName": "testSvc2.exe"
  }
]
}

```

Risk	Rece... ↓↑	Description	Dt	Hosts
Medium	8/31/17 4:17:54pm	A user terminated a deception process on host pc06	▼ ...	pc06.verami...
Medium	8/31/17 4:17:53pm	A user tampered with a deception service on host pc06.	▼ ...	pc06.verami...
Time ↓↑	Description			
8/31/17 4:17:53pm	Deception Service SecMonSvc on host pc06 was modified, possibly by an attacker. The configuration changed from (85) to (69)			

Bắt tiến trình

Chọn 1 tiến trình bắt với tên bất kỳ và triển khai, ví dụ.

```

{
  "processes": [
    {
      "fileName": "process.exe",
      "baseDirectory": "ProgramFiles"
    }
  ]
}

```

Base directories hợp lệ là: ProgramFiles, ProgramFilesX86, Windows, System32, Drivers, Deception.

Risk	Rec... ↓↑	Description	Dt	Hosts
Medium	8/31/17 4:07:02...	A user terminated a deception process on host pc06	^ ...	pc06.verami...
Time ↓↑	Description			
8/31/17 4:07:02pm	Deception Process secmonitor.exe was unexpectedly terminated with exitcode 4294967295, possibly by an attacker.			

7. Những đặc tính khác

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. Máy chủ cũng sử dụng những công nghệ big data để tính toán và lưu trữ thông tin.

Triển khai (Deployment)

Giải pháp 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.