VERAMINE ADVANCED ENDPOINT DETECTION & RESPONSE (VAEDR) PLATFORM

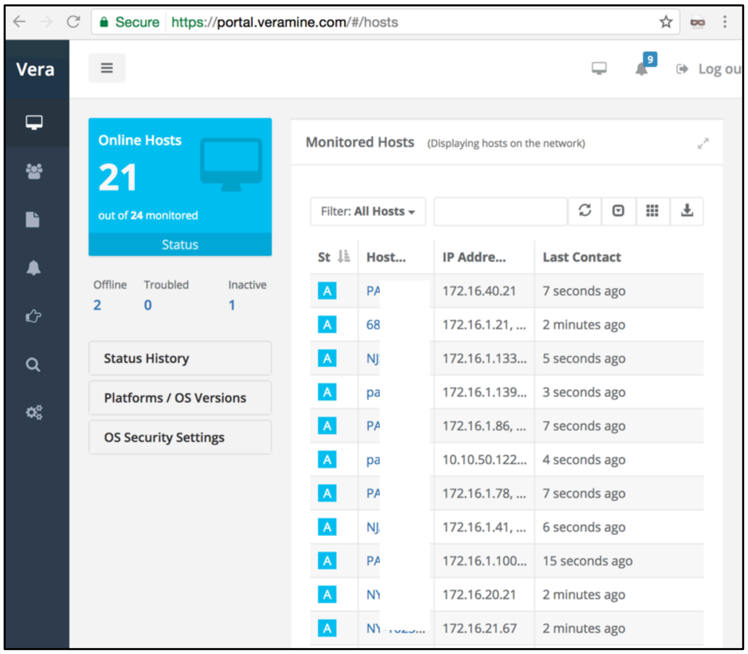
Efficiently Collect Endpoint Behavioral Information.
Automatically Detect Unknown Threats.
Easily Search for Indicators of Attack.
Accelerate Incident Response.

KEY CUSTOMER BENEFITS:

- Gain complete visibility into all of your endpoints, regardless of whether they are currently on or off your network.
- Continuously monitor endpoints and receive prioritized alerts of anomalous behavior and attacks in real-time.
- Quickly install on any Windows host by simply executing the install binary, no configuration necessary on each host.
- Maintain local control of all collected data in your own data center (on prem), or store in Veramine's Cloud (Azure).
- Efficiently store collected information long-term (effectively forever) to allow easy reference and replay in the future.
- Stores a copy of every binary ever loaded on any endpoint by any process.
- Search through memory of every running process using Yara expressions.
- One click access to individual process memory snapshot or full system dump.
- Respond to attacks by isolating an individual process or system from the network, disconnecting a user, or preventing a file from being loaded.
- Reduce cost of IR and forensics by collecting all security-relevant host information preemptively.

PRODUCT OVERVIEW

The Veramine platform efficiently collects all security-relevant events via an intelligent, lightweight (<1% CPU) Windows host-based sensor and sends those events to a cloud-based or customer-hosted server. The server uses advanced heuristics and machine learning algorithms to detect attacks such as Mimikatz-style password dumping, kernel-mode exploitation (local privilege escalation), process injection, unauthorized lateral movement, and other attacker activity. The server exposes those events in both raw form and via an intuitive web-based portal that allows customers to easily search all collected data for answers to reactive incident response questions or proactive threat hunting investigations. An analyst that finds anomalous behavior can easily terminate or suspend an individual process, quarantine a process or host from the network, disconnect or disable a user account, or prevent a particular binary from ever being loaded. The sensor also facilitates memory forensics by uploading to the server a snapshot of a particular process's memory or a full dump of a particular system's memory.



Online Hosts

21

out of 24 monitored

Status

Offline	Troubled	Inactive
2	0	1

Monitored Hosts (Displaying hosts on the network)

St	Host...	IP Addre...	Last Contact
A	PA[redacted]	172.16.40.21	7 seconds ago
A	68[redacted]	172.16.1.21, ...	2 minutes ago
A	NJ[redacted]	172.16.1.133...	5 seconds ago
A	pa[redacted]	172.16.1.139...	3 seconds ago
A	PA[redacted]	172.16.1.86, ...	7 seconds ago
A	pa[redacted]	10.10.50.122...	4 seconds ago
A	PA[redacted]	172.16.1.78, ...	7 seconds ago
A	NJ[redacted]	172.16.1.41, ...	6 seconds ago
A	PA[redacted]	172.16.1.100...	15 seconds ago
A	NY[redacted]	172.16.20.21	2 minutes ago
A	NY[redacted]...	172.16.21.67	2 minutes ago

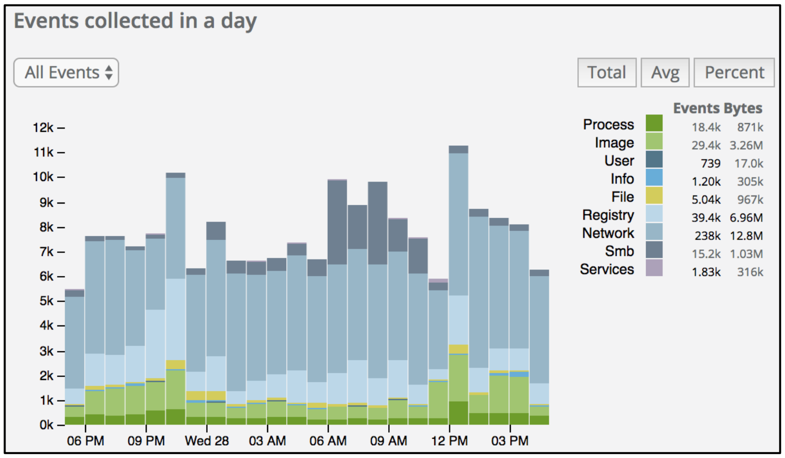
Figure 1 – Hosts View

EFFICIENT, INTELLIGENT ENDPOINT COLLECTION

The strength of any EDR product depends on the scope and integrity of its visibility into endpoint behavior. The Veramine sensor leverages user and kernel mode components to safely and reliably gather and pre-process security-relevant system events. It relies on techniques that minimize negative impact on system stability and limit the probability of other security products reporting false positives related to Veramine sensor. The Windows sensor was built by ex-Microsoft kernel-mode device driver experts, engineers who have each spent 20+ years tuning, developing, and securing Windows device drivers. The sensor is relentlessly optimized for performance and efficiency to minimize the resource load on the endpoint. After an initial, brief enumeration period, the sensor aims to consume less than 1% CPU. Running the sensor on even the least powerful cloud-based virtual machines (Azure A0, AWS t2.nano) has a negligible effect on overall performance of the system.

The scope of events collected distinguishes the Veramine product from its competition. It collects the following:

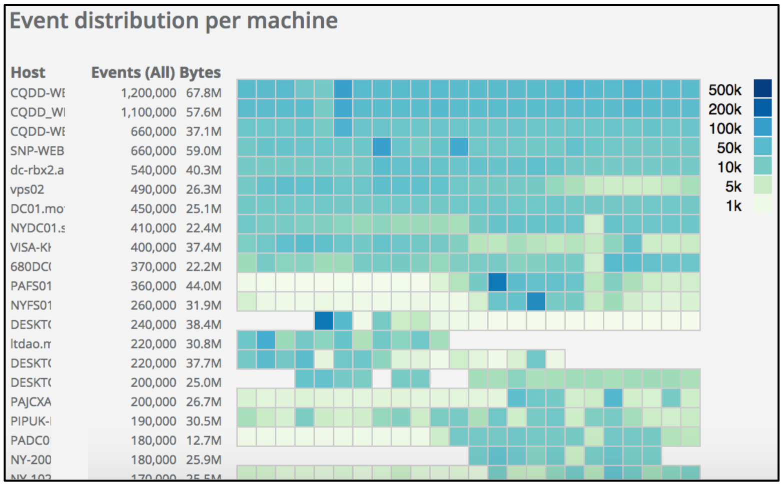
- Process Create, Terminate events
- Process Open, Thread Create events
- Process Image Load events
- Process Token Change events
- User Session Logon, Logoff, Change
- File metadata change events
- System security change events
- Registry Write events
- Network Connection events
- Service Create, Delete, Change events
- SMB session and protocol events
- Sensor policy violation events
- Host information events



		Events	Bytes
Process	🟩	18.4k	871k
Image	🟩	29.4k	3.26M
User	■	739	17.0k
Info	🟦	1.20k	305k
File	🟨	5.04k	967k
Registry	🟦	39.4k	6.96M
Network	🟦	238k	12.8M
Smb	■	15.2k	1.03M
Services	🟪	1.83k	316k

Figure 2 – Example event volume by type of event

Naively and continuously collecting such an expansive set of endpoint behavioral events might overwhelm both client-side and server-side components of a typical EDR solution. Few other products provide this granular level of continuous visibility due to the performance and storage considerations of doing so. The Veramine team has invested a tremendous amount of effort to efficiently collect these events and intelligently choose which to send from the sensor to the server. All relevant details are sent for security-relevant events while abridged events are sent when the sensor determines an event is unlikely to be relevant from a security perspective. The sensor's intelligence constrains the volume of bytes needed to be sent to the server. Idle workstations might send only a few hundred kilobytes of events per day while heavily used servers could send 100mb or more each day. When a host loses network connectivity, events are queued locally in a rolling buffer until they can be sent to the server.



Host	Events (All)	Bytes
CQDD-WE	1,200,000	67.8M
CQDD_WI	1,100,000	57.6M
CQDD-WE	660,000	37.1M
SNP-WEB	660,000	59.0M
dc-rbx2.a	540,000	40.3M
vps02	490,000	26.3M
DC01.mo	450,000	25.1M
NYDC01.s	410,000	22.4M
VISA-KI	400,000	37.4M
680DC(	370,000	22.2M
PAFS01	360,000	44.0M
NYFS01	260,000	31.9M
DESKT(	240,000	38.4M
ltdao.m	220,000	30.8M
DESKT(	220,000	37.7M
DESKT(	200,000	25.0M
PAJCXA	200,000	26.7M
PIPUK-I	190,000	30.5M
PADC0	180,000	12.7M
NY-200	180,000	25.9M
NY-102	170,000	25.5M

Figure 3 – Example event volume by host

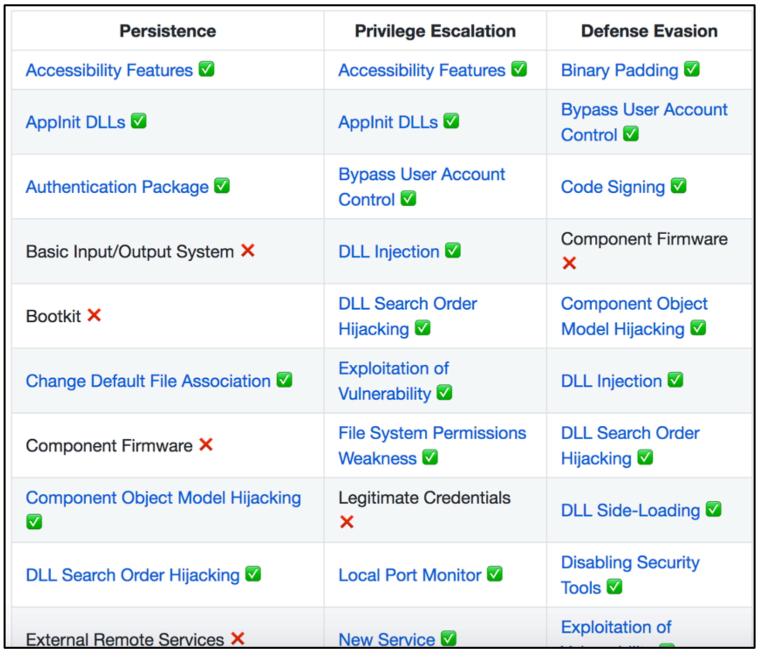
The Veramine sensor is easy to deploy and manage while being difficult to disrupt. Each Veramine customer is given a pre-configured installation binary. With appropriate metadata embedded in the binary, customers can simply execute the sensor as administrator on any host and it will begin sending events – no configuration needed! Each sensor is hardened against tampering to prevent the driver from being uninstalled or the service from being stopped by attackers on the host. The sensor is easy to stop, start, restart, or uninstall from the web portal.

AUTOMATIC DETECTION OF UNKNOWN THREATS

The sensor data streams are continuously analyzed by the Veramine server using a variety of rule-based and machine learning algorithms to identify anomalous behavior. This comprehensive visibility into security-relevant endpoint behavior allows the server-side detection engine to detect a wide variety of cybersecurity threats, including file-less attacks leveraging only built-in tools and sophisticated malware engineered to evade detection.

The strength of the rule-based detection algorithms is continually increasing. Veramine aims to have the industry's widest coverage of Mitre's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) matrix. You can see the current coverage of the ATT&CK matrix on the Veramine Detections wiki at https://github.com/veramine/Detections/wiki. Figure 4 shows a screenshot from that wiki.

Intrusion detection is also supported by Veramine's Machine Learning (ML) platform designed with extensibility, scalability and interactivity. It uses big data technologies to evaluate the sensor data stream and can integrate all ML techniques written in different languages to handle any data problems, while providing various learning supervisions. It currently has 3 detection types that were built based on different pipelines of ML algorithms:

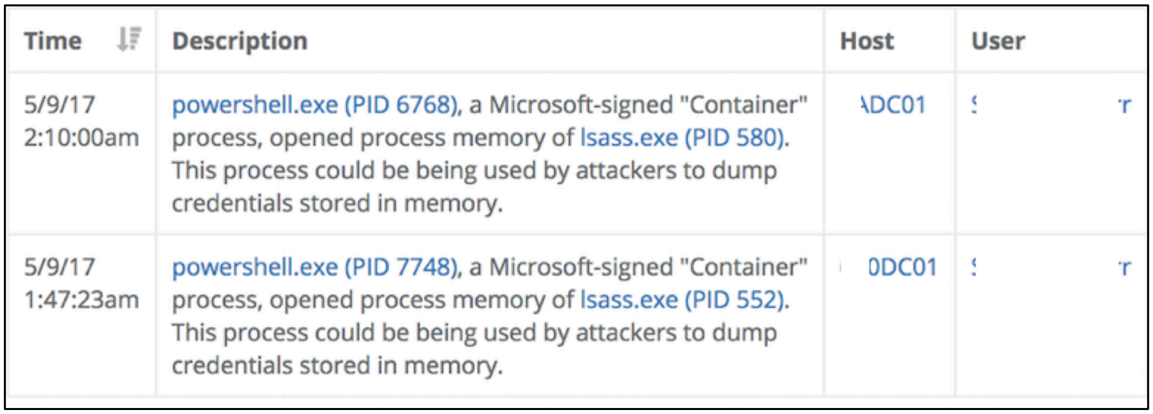


Persistence	Privilege Escalation	Defense Evasion
Accessibility Features ✅	Accessibility Features ✅	Binary Padding ✅
AppInit DLLs ✅	AppInit DLLs ✅	Bypass User Account Control ✅
Authentication Package ✅	Bypass User Account Control ✅	Code Signing ✅
Basic Input/Output System ✗	DLL Injection ✅	Component Firmware ✗
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

- Process Profiling observes historical norms of each process by process name and alerts on divergences from established norms.
- Data Exfiltration detection observes network utilization norms of each process by name and alerts on divergences.
- User Tracking detection observes login behavior patterns for each user and alerts on divergences.

Figure 5 shows a sample Veramine detection resulting from an attacker dumping cleartext credentials on a customer's domain controllers using the Powershell module Invoke-Mimikatz. The Veramine detection engine observed the Powershell.exe process opening process memory of the lsass.exe process, one of the highest fidelity indicators of password dumping behavior. The resulting detection includes all the information necessary to investigate this situation – the suspicious process (powershell.exe), the process being opened (lsass.exe), the host on which the processes were run, and the user executing the suspicious process. The linked-to process detail pages display all loaded modules, every network connection, the parent processes, any child processes, etc.



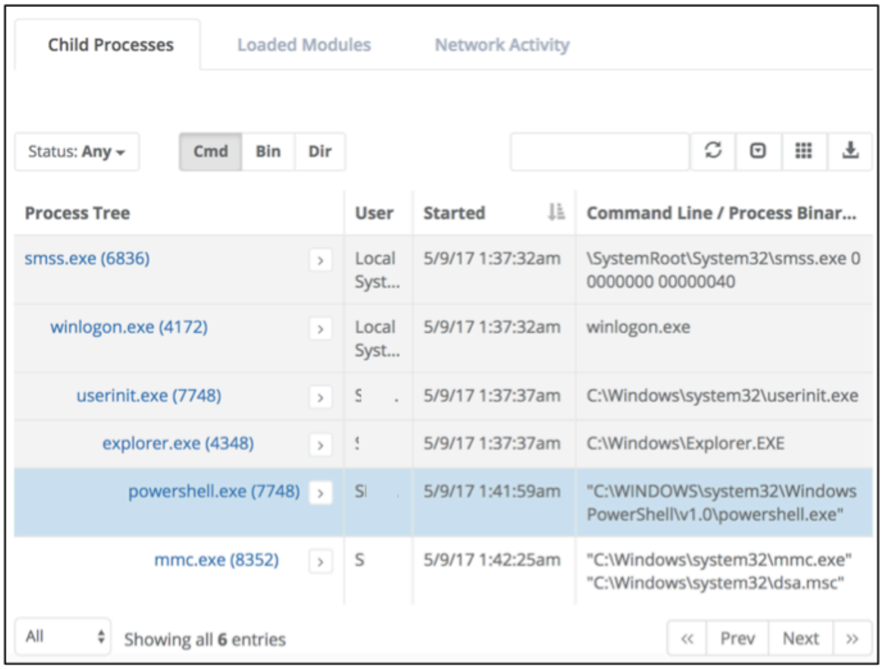
Time	Description	Host	User
5/9/17 2:10:00am	powershell.exe (PID 6768), a Microsoft-signed "Container" process, opened process memory of lsass.exe (PID 580). This process could be being used by attackers to dump credentials stored in memory.	ADC01	S r
5/9/17 1:47:23am	powershell.exe (PID 7748), a Microsoft-signed "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	S r

Figure 5 –Veramine detection example

EASILY SEARCH FOR INDICATORS OF ATTACK

The stream of sensor data is certainly useful for detection. However, the collected information is also presented via the customer portal after being correlated and augmented with additional context. The portal allows users to perform ad-hoc searches to discover answers that facilitate and empower reactive intrusion response investigations and also to enable effective proactive threat hunting. Some customers have referred to this capability as “like a web-based SysInternals Process Explorer running on every host”.

To investigate the malicious Powershell.exe detection above, we begin with the process detail page to see the full process tree, to include any child processes launched by the malicious powershell.exe. Figure 6 shows that view.



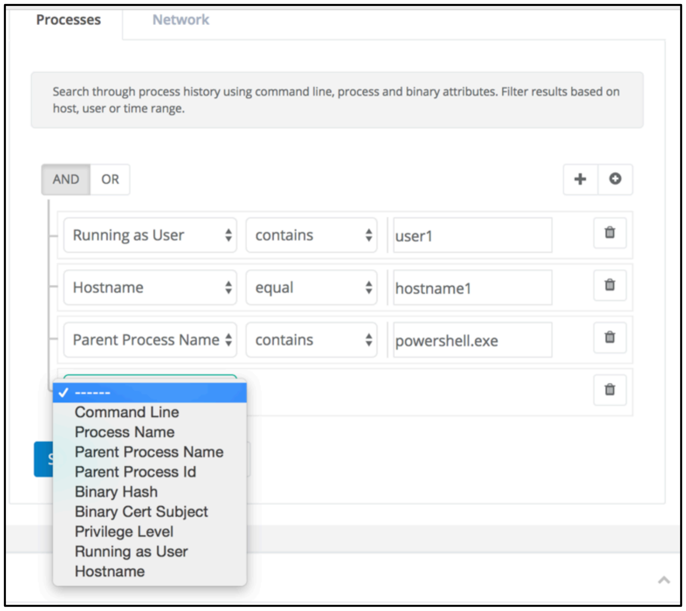
Process Tree	User	Started	Command Line / Process Binar...
smss.exe (6836)	Local Syst...	5/9/17 1:37:32am	\SystemRoot\System32\smss.exe 0 0000000 00000040
winlogon.exe (4172)	Local Syst...	5/9/17 1:37:32am	winlogon.exe
userinit.exe (7748)	S .	5/9/17 1:37:37am	C:\Windows\system32\userinit.exe
explorer.exe (4348)	S	5/9/17 1:37:37am	C:\Windows\Explorer.EXE
powershell.exe (7748)	Sl	5/9/17 1:41:59am	"C:\WINDOWS\system32\Windows PowerShell\v1.0\powershell.exe"
mmc.exe (8352)	S	5/9/17 1:42:25am	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\dsa.msc"

Figure 6 –Process Detail page “Child Processes” tab

Clicking on the explorer.exe parent process (PID 4348) hyperlink will show the other peer processes to the malicious powershell.exe process (PID 7748), processes launched by the same parent. It’s also just a few clicks in the Veramine Process Search interface to find related process activity, such as the following:

- All processes launched across the network by the same compromised user account
- All processes launched around the same time on the same hosts as the malicious powershell.
- All powershell.exe child processes launched on the same hosts by the same user at any time.

Figure 7 shows an example screenshot of the search interface. This particular customer was able to use the Veramine search interface to identify other malicious processes, other compromised users, and other compromised systems. This visibility enabled them to also identify a key characteristic present in every attacker user session to easily follow and observe the attacker’s every move on this network.



Search through process history using command line, process and binary attributes. Filter results based on host, user or time range.

Running as User	contains	user1
Hostname	equal	hostname1
Parent Process Name	contains	powershell.exe

Figure 7 – Process Search Interface

ACCELERATE INTRUSION RESPONSE

The Veramine platform provides control and response features to enable rapid, effective incident response from a central console. Analysts can send response actions to the Veramine sensor to interact with processes, binaries, users, and hosts.

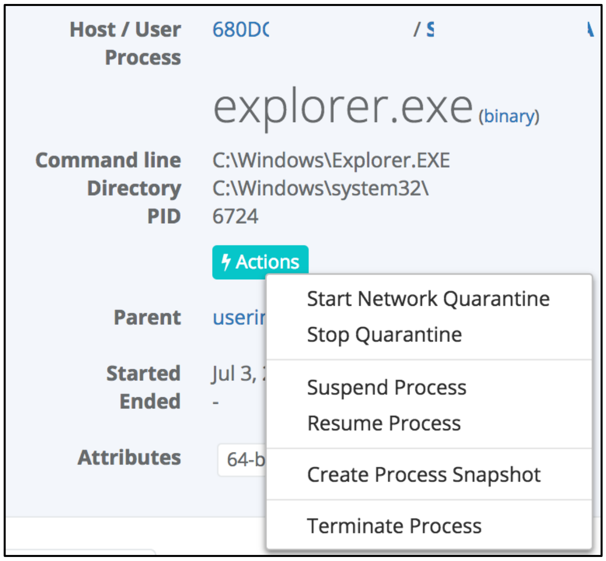

Host / User 680DC / S
Process explorer.exe (binary)
Command line C:\Windows\Explorer.EXE
Directory C:\Windows\system32\
PID 6724
Parent userir
Started Jul 3,
Ended -
Attributes 64-b

Figure 8 – Running Process Sensor Actions

The following process-related response actions are currently available, as shown in Figure 8:

- Suspend or terminate any running process.
- Create and upload a process memory snapshot to the Veramine server.
- Prevent an individual process from making any outbound network connections

In addition to these indivdiual process commands, the Veramine sensor can search across system memory for a Yara expression and report the processes with matches.

The Veramine sensor provides several binary-related actions as well, as shown in Figure 9:

- Prevent a binary from being loaded by any process.
- After a binary has been loaded, prevent the loading process from making outbound network connections.

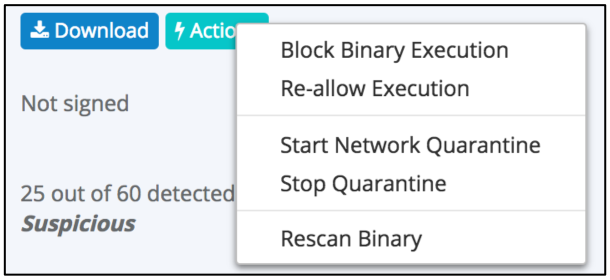

Not signed
25 out of 60 detected
Suspicious

Figure 9 – Binary Sensor Actions

The Veramine platform also retains a single copy of each binary loaded by any process and makes that binary available for download within the Veramine portal.

The Veramine sensor also provides several user-related actions. It can disable or enable a local user account or disconnect an individual RDP login session.

Finally, the Veramine sensor provides the following host-related actions, as shown in Figure 10:

- Shutdown, Restart, or Hibernate the machine.
- Prevent the host from making outbound network connections to destinations other than the server.
- Uninstall the sensor.

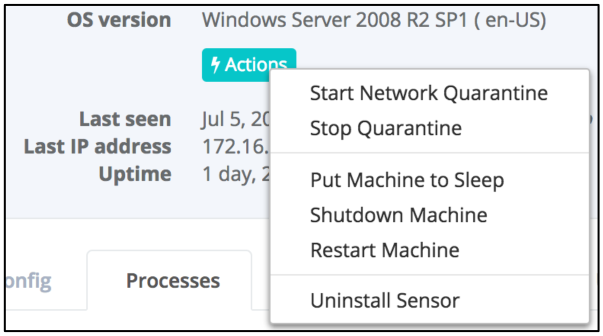

OS version Windows Server 2008 R2 SP1 (en-US)
Last seen Jul 5, 20
Last IP address 172.16.
Uptime 1 day, 2

Figure 10 – Host Sensor Actions

The Uninstall Sensor action merits particular mention because the web portal is the only way to uninstall the production sensor. The trial version of the Veramine sensor can be be easily uninstalled from the command line. However, the production version of the sensor resists attacker attempts to either stop the user mode service or uninstall the kernel-mode driver. Competing products can be easily disabled on a compromised host but the Veramine platform is resilient against tampering and against host-based attacks targeting the sensor.

START A FREE TRIAL TODAY!

Send a request to contact@veramine.com to start a free trial today. It takes only a few moments for us to configure the server-side components and send a link to download a sensor customized just for you.