

LogRhythm Threat Detection Cookbook

LogRhythm Labs Threat Intelligence
2014-09-24

Contents

Attack

SQL Injection.....	3
Exploit Scanner User-Agents.....	4
URL-Encoded Control Characters.....	5
Cross-Site Scripting.....	6
Excessive HTTP Errors.....	7
Repeat Signature Detection.....	8
Bad Bot User-Agents.....	9

Denial of Service

Web Server DDoS Attack.....	10
-----------------------------	----

Compromise

Internal Attack then Privilege Escalation.....	11
Lateral Movement then External Connection.....	12
Vulnerability Exploited Internally.....	13

Malware

Malware Not Cleaned.....	14
Outbreak.....	15
Spamming Zombie.....	16

Network Anomaly

Common Applications on Non-Standard Ports.....	17
Non-Standard Use of Common Ports.....	18
Threat List-TOR Server or TOR Exit Node.....	19
Connection with Non-Whitelisted Country.....	20
Host Compromised-Recon Followed By Attack.....	21
Attack Followed by Firewall Allow.....	22
Excessive Firewall Denies.....	23
Rogue Host Detection.....	24
Internationalized Domain Names.....	25
Suspicious Top Level Domains.....	26

Account Anomaly

Failed Non-Primary Exchange Account Authentication.....	27
Recently Disabled Account Access Activity.....	28
Account Created, Used, Deleted.....	29
New Administrator Activity.....	30
Audit Disabled by Admin.....	31
Concurrent VPN Connections.....	32
Password Modified By Another User.....	33
Abnormal Origin Location.....	34
Abnormal File Access.....	35
Abnormal Process Activity.....	36
Abnormal Authentication Behavior.....	37
Abnormal Amount Of Audit Failures.....	38

Behavioral Anomaly

New Common Event.....	39
Abnormal Process Activity by Host.....	40

Recon

Port Scan: Slow.....	41
Vulnerability	
Vulnerability After Software Install.....	42

Operations

Ops Warning: Abnormal Log Volume Fluctuation.....	43
---	----

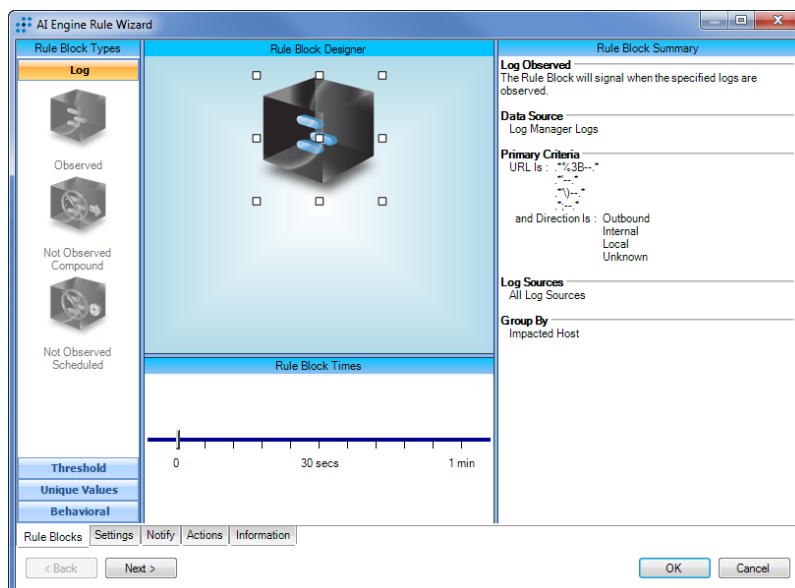
Attack SQL Injection

Because they are one of the few services on a network that accept inbound connections, Web Applications are a common entry point for attackers. SQL Injection attacks are one of the most prevalent threats that they face. In these attacks, the adversary attempts to execute commands on the remote host by sending commands to the back-end database through unprotected input channels. While attackers have many methods to obscure their attacks, the majority of the attacks will require use of a set of common characters. This LogRhythm AI Engine rule checks for common URL-encoded SQL Injection strings and alerts on attacks.

Log Requirements

This rule should be configured to watch Web Server logs, though if the environment has employed additional protections such as a Web Application Firewall, IDS/IPS, and/or a network Firewall, these logs should feed into the AIE rule as well to alert on all attacks.

- Web Server Logs
- Intrusion Detection / Prevention Logs
- Web Application Firewall Logs
- Perimeter Firewall Connection Logs



Knowledge Base Content

Type	Name	ID
AIE Rule	Ext:Host Atck:SQL Injection	95

Configuration

All Access Logs and Error Logs should be captured from the Web Application logs.

Actions

Any time these strings are observed either entering the network from an external source, this alarm will trigger. Attacks that make it past base-network defenses and are observed in the server logs should be evaluated to determine if the attack was successful, and if so, what the attacker was able to obtain using the SQL Injection attack. Any open SQL Injection vulnerabilities should be remediated in the application by accepting only parameterized queries in order.

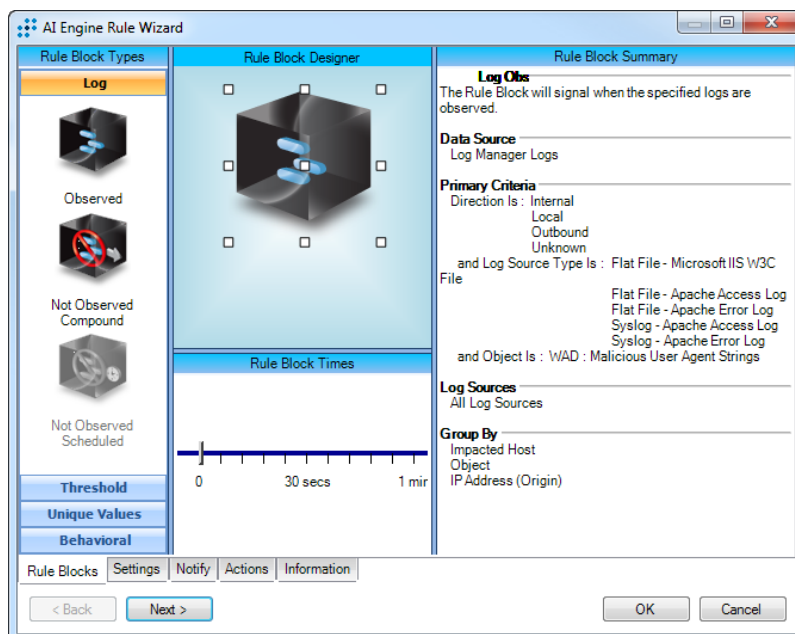
Attack Exploit Scanner User-Agents

There are many tools available for finding and exploiting vulnerabilities in web applications, and although changing User-Agent values is trivial, a significant portion of attackers don't bother changing the easily-identifiable defaults. For example, "Havij" is a tool that can automatically inject a SQLi attack into a vulnerable web server -- by default, the string "Havij" will be in the User-Agent and thus easily detected in server logs. Being aware of this malicious activity is the first step towards mitigation.

Log Requirements

At least one of the following web server logs must be collecting:

- Error logs
- Access logs



Knowledge Base Content

Type	Name	ID
AIE Rule	Ext:Malicious User-Agent	115

Configuration

By default, web server logs for Apache and IIS will be filtered. If the local deployment uses a custom log source that parses the User-Agent string to the <object> metadata field, it will work here as well.

Actions

Follow-up investigation can be performed by analyzing associated metadata and utilizing LogRhythm's expansive queries:

- Investigate the source IP address in the SIEM for other suspicious activity originating from that host
- Launch an additional investigation using the User-Agent string as the "object" field
- Utilize the "WAD: Attacking IPs" investigation layout for quicker visibility into the origin of this alarm
- Enable the smart response plugin "Add Item To List" -- described in the Activate Smart Response Plugin section of the deployment guide -- to automatically create and maintain a list of malicious IP addresses
- Use LogRhythm Network Monitor to search for additional traffic
- Use LogRhythm Network Monitor to collect packet capture for HTTP sessions

Attack

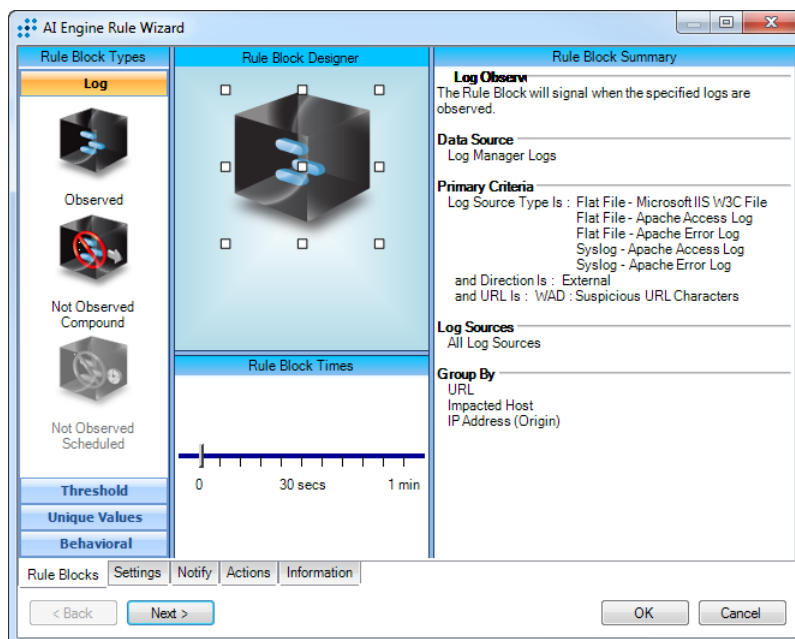
URL-Encoded Control Characters

Many web applications are vulnerable to code injection attacks -- in this case, attacks via HTTP requests that contain URL-encoded control characters in the URI. These requests can be identified by matching a list of suspicious URL-encoded characters with observed traffic. Some investigation may be required to eliminate false positives, but once malicious activity is identified, rules for blocking should be relatively easy to implement.

Log Requirements

One of the following types of web server Log Sources must be collecting:

- Error logs
- Access logs



Knowledge Base Content

Type	Name	ID
AIE Rule	Ext:Suspicious URL Characters	116
AIE Rule	Int:Suspicious URL Characters	117

Configuration

By default, web server logs for Apache and IIS will be filtered. If the local deployment uses a custom Log Source that parses the User-Agent string to the <object> metadata field, it will work here as well.

Actions

Once this rule is triggered, investigate the root cause by analyzing associated metadata and utilizing LogRhythm's expansive queries:

- Investigate the source IP address for other suspicious activity originating from that host
- Utilize the "WAD: Attacking IPs" investigation layout for quicker visibility into the origin of this alarm
- Enable the smart response plugin "Add Item To List" -- described in the Activate Smart Response Plugin section of the deployment guide -- to automatically create and maintain a list of malicious IP addresses
- Use LogRhythm Network Monitor to search for additional traffic
- Use LogRhythm Network Monitor to collect packet capture for HTTP sessions

Attack

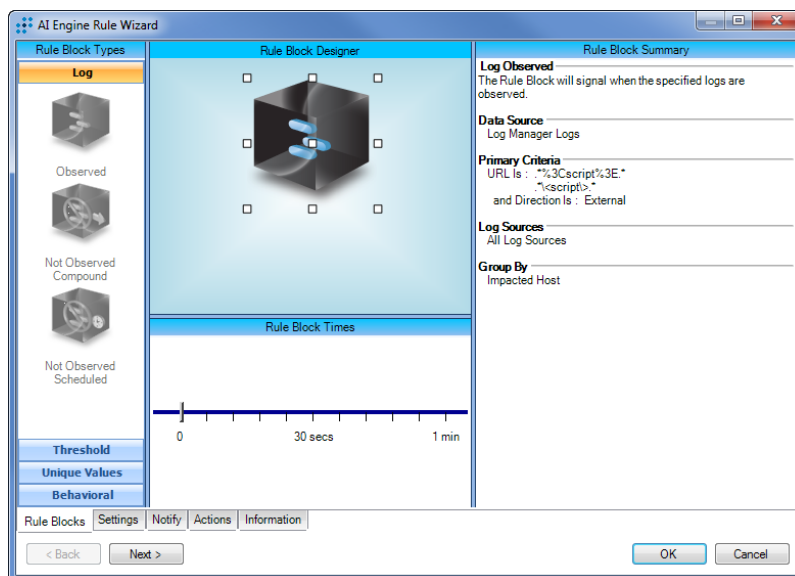
Cross-Site Scripting

Vulnerable Web Applications can be used to infect unsuspecting visitors in a Cross-Site Scripting attack (XSS) -- attackers can embed JavaScript within the application (persistent XSS) or utilize social engineering and a specially crafted link (reflected XSS). When a user clicks these links, or in some cases even visits a compromised web page, the client-side code will execute, and any number of actions can be performed: hijacking the user's browser, injecting malware, stealing session tokens, sniffing the user's traffic, and browsing intranet applications.

Log Requirements

The following combination of log sources covers both server and clients.

- Web Server Logs
- Intrusion Detection/ Prevention Logs
- Web Application Firewall Logs/Perimeter Firewall Connection Logs
- Web Proxy Logs
- User System Logs



Knowledge Base Content

Type	Name	ID
AIE Rule	Ext:Host Atck:XSS Attack	97
AIE Rule	Int:Host Atck:XSS Attack	98

Configuration

It is important to note that these attacks can happen both on internal, organization-run applications as well as popular, external applications. However, the most important logs to monitor for this activity on are the application logs -- all Access Logs and Error Logs should be captured.

Actions

This alarm will trigger any time the "<script>" tag is observed in one of two places: within a URL that a user is visiting or when an attacker attempts to inject into a web form. Attacks that make it past base-network defenses and are observed in the server logs should be evaluated to discover what may have resulted from the attack. Any XSS vulnerabilities discovered within company-owned applications should be remediated within the application by properly escaping all user supplied input.

Attack Excessive HTTP Errors

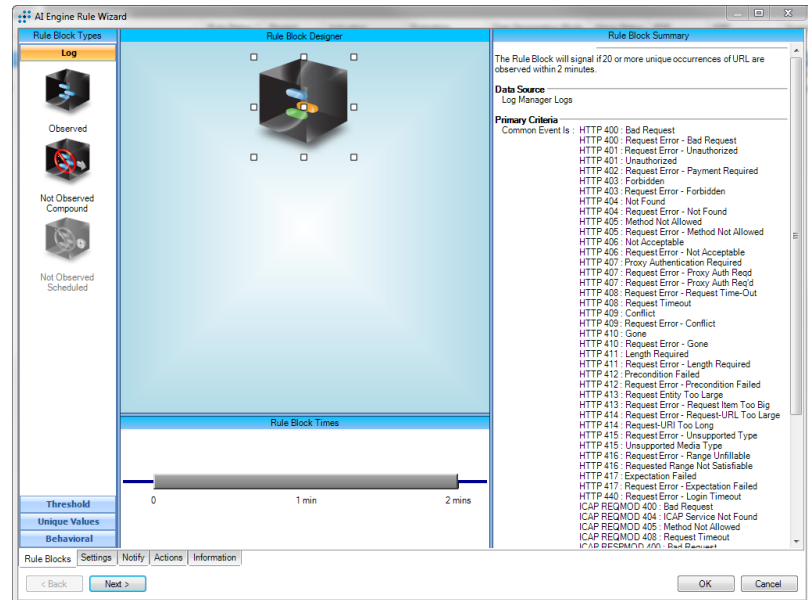
As an attacker probes web applications for vulnerabilities, the web servers may generate dozens or hundreds of HTTP errors. This rule looks for an origin host logging 20 or more unique HTTP errors in 2 minutes. In addition to preemptively detecting potential attacks, tracking HTTP errors can also find broken links and other problems with web servers affecting normal use.

Log Requirements

The following log source must be collecting:

- Web server

Knowledge Base Content



Type	Name	ID
AIE Rule	Ext:Recon:Excessive HTTP Errors	89

Configuration

The logs from your web server must use the common events listed in the AIE rule.

Optional: Broken links can cause web crawlers like Googlebot to trigger many of these alarms. If it's impractical to resolve all the known issues with a web site, it's advisable to add an exclude filter for repeated visits by crawler hosts.

Actions

Follow-up investigations should be done to determine if the web server was successfully compromised. Similarly, this rule should prompt closing of new vulnerabilities as they are discovered.

Attack Repeat Signature Detection

This AI Engine rule looks for 10 or more attack, malware, or other security activity logs in a short time span. Such redundancy reduces the chance of being bogged down by one-off false positives. Using the Vendor Message ID field as the Group By value will focus on devices like IDSs that assign signature values.

Log Requirements

The following log source types must be available

- Intrusion Detection System logs
- Malware Scanner logs

Knowledge Base Content

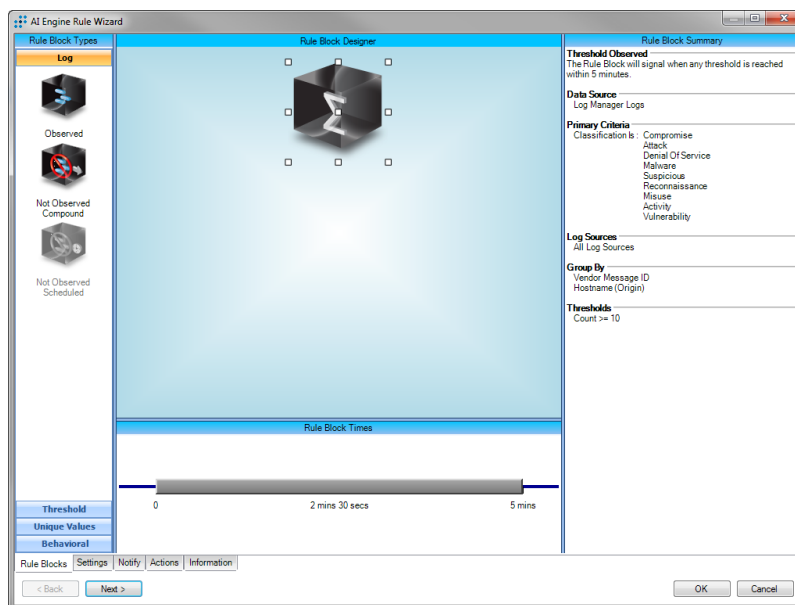
Type	Name	ID
AIE Rule	Ext:Host Atck:Repeat Signature Detected	496

Configuration

None required.

Actions

This alarm is a strong indication that a host has been compromised or infected with malware. To determine if the host is actually compromised, run an investigation on the target host looking for additional suspicious activity -- the target host may be either the origin or impacted, based on the signature that was detected. It may also be helpful to look for other alarms affecting the same host.



Attack

Bad Bot User-Agents

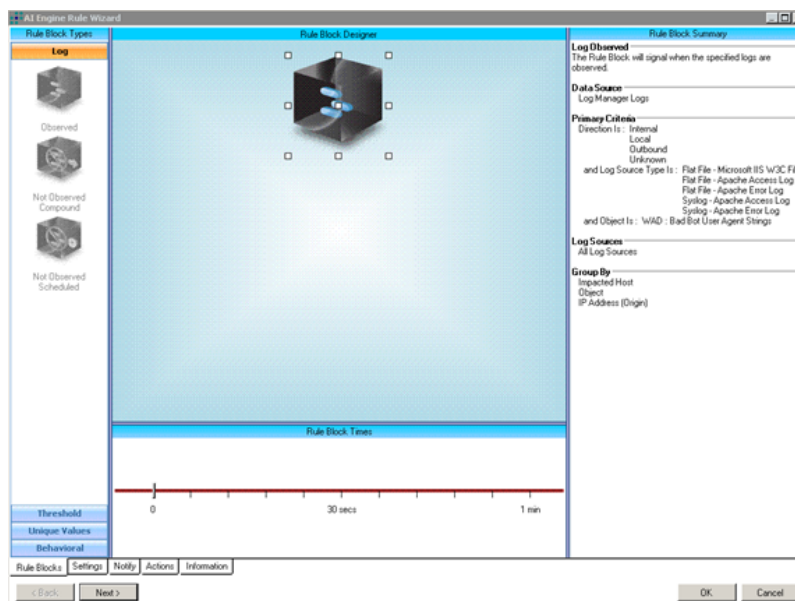
Many web crawlers, scrapers, crawlers, spiders, etc will constantly scan web servers for vulnerabilities -- these are collectively categorized as Bad Bots. Although their User-Agents can be easily changed, many will use their defaults. Using this rule will allow web server admins to block such scans as new ones arise.

Log Requirements

At least one of the following web server logs must be collecting:

- Error logs
- Access logs

Knowledge Base Content



Type	Name	ID
AIE Rule	Ext:Bad Bot User-Agent	487
AIE Rule	Int:Bad Bot User-Agent	486

Configuration

By default, web server logs for Apache and IIS will be filtered. If the local deployment uses a custom log source that parses the User-Agent string to the <object> metadata field, it will work here as well.

Actions

Once this rule is triggered, investigate the root cause by analyzing associated metadata and utilizing LogRhythm's expansive queries:

- Investigate the source IP address for other suspicious activity originating from that host
- Launch an additional investigation using the User-Agent string as the "object" field
- Utilize the "WAD: Attacking IPs" investigation layout for quicker visibility into the origin of this alarm
- Enable the smart response plugin "Add Item To List" -- described in the Activate Smart Response Plugin section of the deployment guide -- to automatically create and maintain a list of malicious IP addresses
- Use LogRhythm Network Monitor to search for additional traffic
- Use LogRhythm Network Monitor to collect packet capture for HTTP sessions

Denial of Service Web Server DDoS Attack

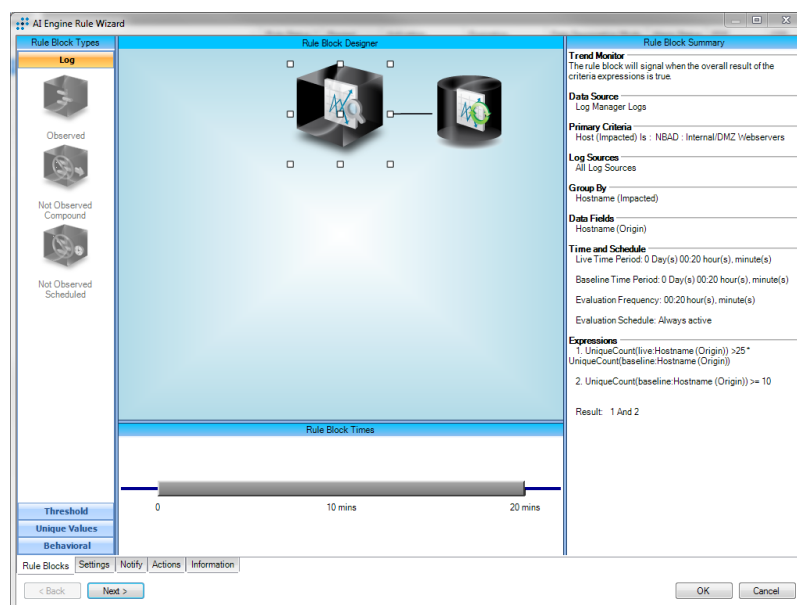
Distributed denial-of-service attacks (DDoS) involve a large number of remote hosts making many requests of a specific server with the intention of exhausting its resources or saturating the network connection to the point of effectively taking the server offline. This rule creates a 20 minute traffic baseline and alarms when the following 20 minute period contains at least 25 times the number of connections from unique remote hosts.

Log Requirements

Utilize the following log source types:

- Collection of network traffic logs impacting the web server

Knowledge Base Content



Type	Name	ID
AIE Rule	Susp:Web Server DDoS Attack	456
List	NBAD: Internal/DMZ Webservers	

Configuration

This AIE rule by default filters on a list of web servers. Populate this list with hosts the rule should analyze. Because of the high resource cost of behavioral rules, it is advised to only configure this rule to monitor hosts which are susceptible to external denial of service attacks.

Actions

Mitigating the effects of DDoS attacks typically requires specialized services

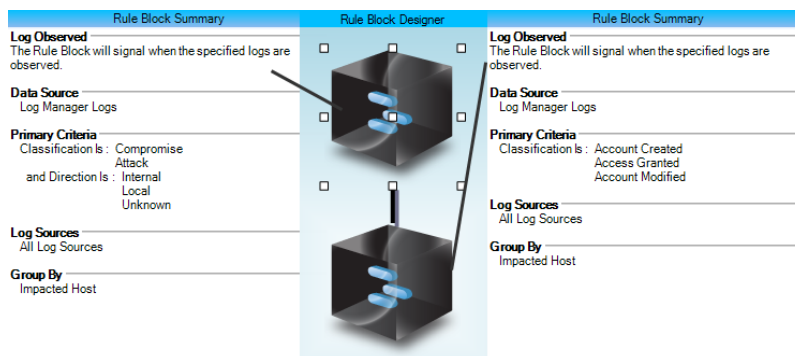
Compromise Internal Attack then Privilege Escalation

After a malicious actor has successfully carried out the first stages of attacking a system, they will frequently seek to escalate their privileges to gain further access and spread across the infected network. Fortunately, these account actions will be logged and can be detected when following an attack or compromise.

Log Requirements

The following log sources must be collecting:

- Windows Security Event Logs or Unix host logs
- Security devices, both network and host-based, that can identify successful compromises and attack events.



Knowledge Base Content

Type	Name	ID
AIE Rule	Compromise: Internal Attack then Privilege Escalation	63

Configuration

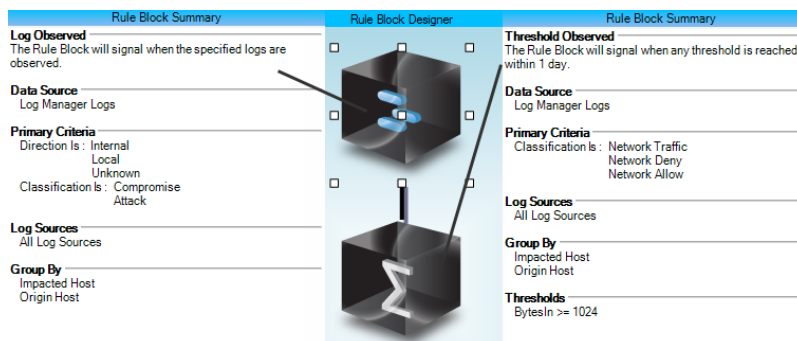
In the Local Security Policy on Windows hosts, make sure Audit Account Management is turned on.

Actions

If a system has been successfully compromised, and a malicious actor is actively creating and modifying accounts to gain access to more systems, it's extremely important to lock the impacted accounts and systems as quickly as possible.

Compromise Lateral Movement then External Connection

After compromising a system and strengthening their foothold, malicious actors will likely attempt to exfiltrate valuable data -- intellectual property, network enumeration, financial data, etc -- from the compromised network. LogRhythm Advanced Intelligence Engine can detect when a newly-compromised machine begins making outbound connections, and quickly reacting to this alarm can prevent excessive loss of an organization's data.



Log Requirements

The following log sources must be collecting:

- Network monitoring device tracking outbound connections
- Security devices, both network and host-based, that can identify successful compromises and attack events.

Knowledge Base Content

Type	Name	ID
AIE Rule	Compromise: Lateral Movement then External Connection	60

Configuration

This rule is dependent on other security devices in the network being able to detect Attack and Compromise events. For example, an IDS detecting an infected host beaconing to a known malware server or Anti-Virus triggering on successful malware execution.

Actions

Internal Attack and Compromise events should already be priorities for follow-up investigation, and this rule should be treated as an even more threatening. If this rule is triggered correctly, the infected machine has already begun to exfiltrate data and should be immediately disconnected from the network. The source of the compromise should be quickly identified and also stopped from further spread.

Compromise Vulnerability Exploited Internally

Vulnerability scanners allow security operations teams to actively find attack vectors before they are exploited. When this knowledge is integrated into LogRhythm, other corresponding events, such as Attacks, can be put into context. For example, this rule looks for attack events on a specific host. If that attack vector is a known vulnerability, based on scan results, then this rule will trigger.

Rule Block Summary
Log Observed The Rule Block will signal when the specified logs are observed.
Data Source Log Manager Logs
Primary Criteria Classification Is : Compromise Attack Denial Of Service Malware Reconnaissance and TCP/UDP Port (Impacted) Is Not : Nothing and Host (Impacted) Is Not : Nothing and Direction Is : Internal Local Unknown
Log Sources All Log Sources
Group By TCP/UDP Port (Impacted) Impacted Host

Rule Block Summary
Log Observed The Rule Block will signal when the specified logs are observed.
Data Source Log Manager Logs
Primary Criteria Classification Is : Vulnerability and TCP/UDP Port (Impacted) Is Not : Nothing and Host (Impacted) Is Not : Nothing
Log Sources All Log Sources
Group By TCP/UDP Port (Impacted) Impacted Host

Log Requirements

The following log sources must be collecting:

- Vulnerability Scanner
- Security devices, both network and host-based, that can identify attack events.

Knowledge Base Content

Type	Name	ID
AIE Rule	Compromise: Vuln Exploited Internally	109

Configuration

Collection from a vulnerability scanner to LogRhythm must be configured.

Actions

If a vulnerability and attack event are corroborated on the same host, there is a very high chance of malicious activity. This alarm should be quickly followed up with an investigation into the circumstances of the attack. Post-cleanup, it should be determined if the vulnerability can be eliminated or at least mitigated to prevent further incidents.

Malware

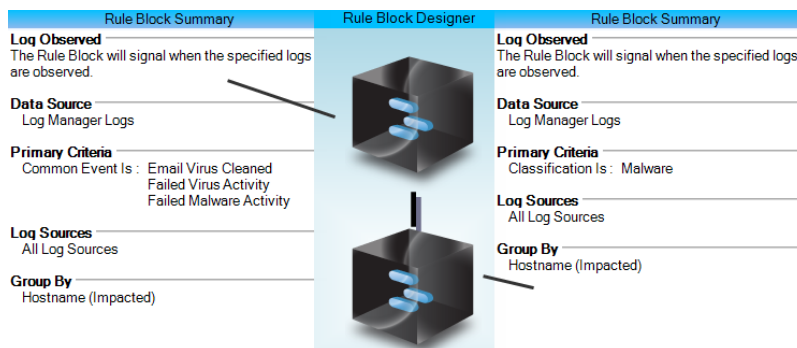
Malware Not Cleaned

In some cases, a malware removal tool will quarantine or delete malware only for it to pop back from memory or another hiding place. This rule will find instances where a malware cleaning event is followed by a malware detection event on the same host.

Log Requirements

One or more of the following Log Source types must be collecting:

- Antivirus
- Intrusion Detection Systems
- Email Gateway
- Any other device that can identify malware



Knowledge Base Content

Type	Name	ID
AIE Rule	Malware: Not Cleaned	509

Configuration

For antivirus software installed on individual hosts, each host will need to forward the AV logs to the SIEM. If the organization is using an AV system that already collects from all hosts, then this system's logs can be used.

Actions

Persistence in malware is a particularly dangerous sign -- on top of being hard to remove, it likely means that malware has other advanced capabilities and may be lurking elsewhere. In this case, reformatting the machine is likely the only solution.

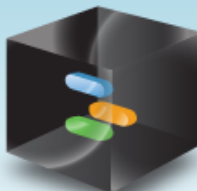
Malware Outbreak

Several malware events emanating from different hosts within the organization may be an indication that malware has begun to spread throughout the network. It may also mean those hosts are falling victim to an external zero-day exploit or other similar, external security event. In any case, an outbreak is more threatening than an isolated infection and should be treated accordingly.

Log Requirements

One or more of the following Log Source types must be collecting:

- Antivirus
- Intrusion Detection Systems
- Email Gateway
- Any other device that can identify malware

Rule Block Summary	Rule Block Designer
Unique Values Observed The Rule Block will signal if 3 or more unique occurrences of Impacted Host are observed within 30 minutes.	
Data Source Log Manager Logs	
Primary Criteria Classification Is: Malware Failed Malware	
Log Sources All Log Sources	
Group By Common Event	
Unique Values Impacted Host >= 3	

Knowledge Base Content

ID	Name
72	Malware: Outbreak

Configuration

For antivirus software installed on individual hosts, each host will need to forward the AV logs to the SIEM. If the organization is using an AV system that already collects from all hosts, then this system's logs can be used.

Actions

For a large infection, it's important to quickly stop the malware from spreading. Quarantine infected hosts before doing in depth analysis or remediation.

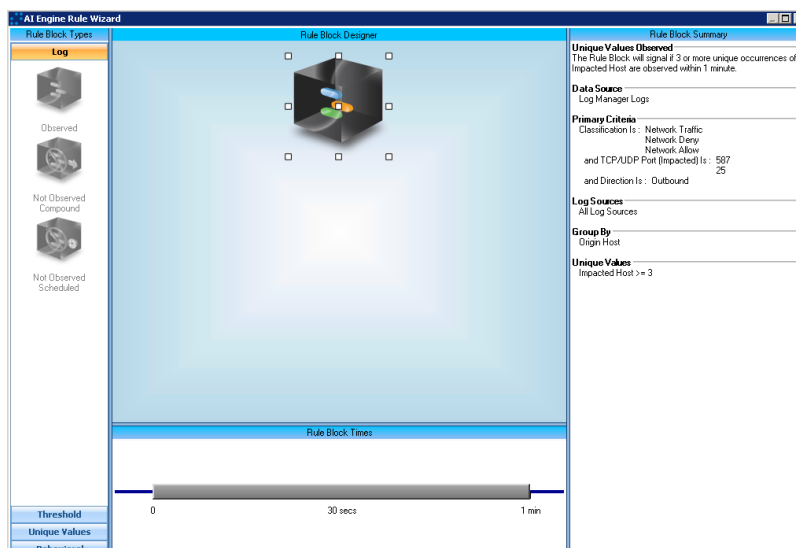
Malware Spamming Zombie

Spammers may find and use open SMTP relays to send spam -- this is generally done over SMTP connections on ports 25 or 587. On the organizational network, most e-mail traffic is workstations communicating with an Exchange server, and thus the organization's mail servers should be the only hosts making outbound SMTP connections (when users check their externally-hosted, personal e-mail, it's generally through a web UI over port 443). By monitoring for any systems other than mail servers attempting to make outbound SMTP connections, potential spamming activity can be discovered.

Log Requirements

One of the following log source types must be collecting:

- Perimeter Firewall Connection Logs
- LogRhythm Network Monitor or other perimeter flow data



Knowledge Base Content

Type	Name	ID
AIE Rule	Int:Host Comp:Spamming Zombie	53

Configuration

An exclude filter should be added where Origin Host = Mail Servers. It's best practice to create a list of mail servers and utilize this list in the exclude filter.

Actions

Any time a non-mail server attempts to make an SMTP connection, this AIE rule will fire. The origin host should then be investigated further to determine if it has been compromised.

Network Anomaly

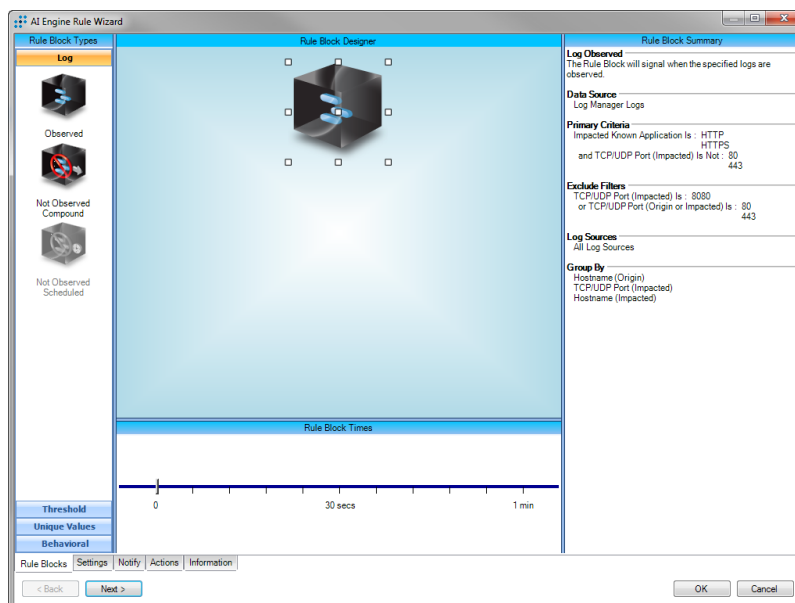
Common Applications on Non-Standard Ports

Malware may use common network protocols like HTTP and SSH to hide command and control communication among legitimate traffic. However, the malware operator may find it easier for configuration and collection purposes to use a non-standard port. By dissecting network traffic at the application layer, Network Monitor is able to properly label applications and find such port mismatches.

Log Requirements

At least one of the following Log Sources must be collecting:

- LogRhythm Network Monitor
- An equivalent network protocol analyzer



Knowledge Base Content

Type	Name	Detects	ID
AIE Rule	Susp:Port Misuse:HTTP	HTTP traffic not using standard port 80	428
AIE Rule	Susp:Port Misuse:SSH Out	Outbound SSH traffic not on standard SSH port 22	434
AIE Rule	Susp:Port Misuse:SSH In	Inbound SSH traffic not using standard SSH port 22	448

Configuration

Network Monitor can be configured for full packet captures per application of interest -- having this content will help with follow-up investigations.

The rules shown here can be used to detect other applications that might be used for covert channels -- this will allow for easy, customized expansion based on each enterprise's particular network footprint. Note that an alert does not necessarily mean that a host is infected, and it may be desirable to whitelist known hosts or IPs that trigger the alert.

Actions

Alerts generated by these rules may be indications of malware infection. This can be confirmed by examining the host machine exhibiting the behavior, looking for additional alerts, suspicious log activity, or by collecting and analyzing the content of the network traffic between the host and the traffic's destination.

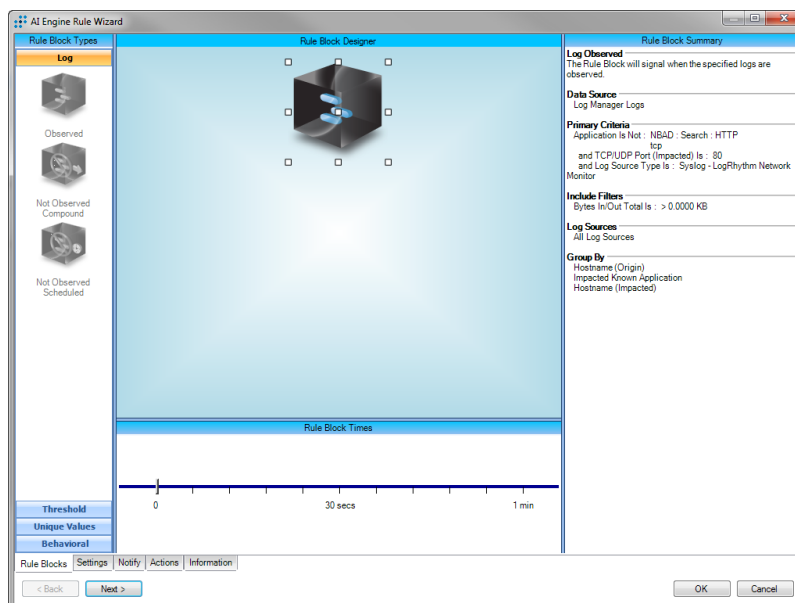
Network Anomaly Non-Standard Use of Common Ports

In order to hide command and control communication among legitimate traffic, malicious implants may use standard protocol ports even if their covert channels don't conform to protocol standards. Because LogRhythm Network Monitor can accurately identify protocols without relying solely on port, it is able to detect port misuse by such malware.

Log Requirements

At least one of the following Log Sources must be collecting:

- LogRhythm Network Monitor
- An equivalent network protocol analyzer



Knowledge Base Content

Type	Name	Detects	ID
AIE Rule	Susp:Port Misuse:80	non-HTTP traffic using standard HTTP port 80	436
AIE Rule	Susp:Port Misuse:53	non-DNS traffic using standard DNS port 53	437
AIE Rule	Susp:Port Misuse:22	non-SSH traffic using standard SSH port 22	532
AIE Rule	Susp:Port Misuse:443	non-SSL/TLS traffic using standard port 443	533
List	NBAD: Search: SSL/TLS	260+ Netmon-defined web apps that use 443 (eg gmail amazon netflix)	2171

Configuration

Network Monitor can be configured for full packet captures per application of interest -- having this content will help with follow-up investigations.

The rules shown here can be used for any combination of ports and protocols - this will allow for easy, customized expansion based on each enterprise's particular network footprint. Note that an alert does not necessarily mean that a host is infected, and it may be desirable to whitelist known, legitimate applications that trigger the alert. For HTTPS applications that use 443, the whitelist is already provided as NBAD Search SSL/TLS.

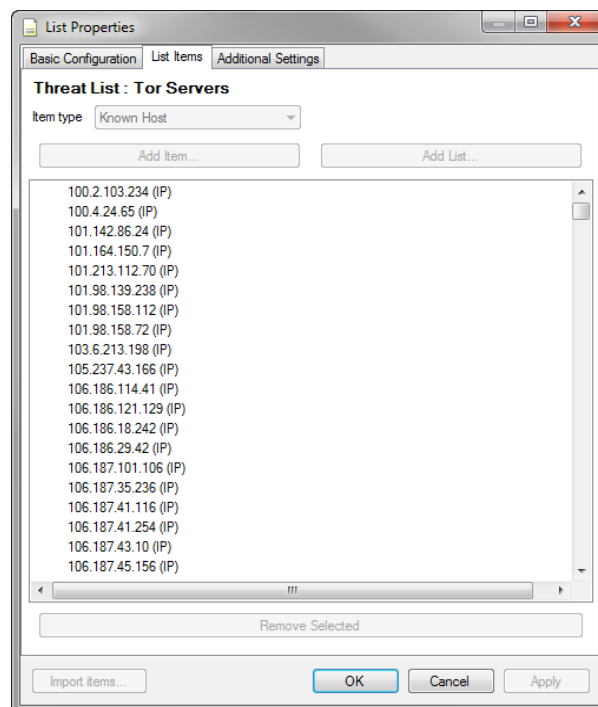
Actions

Alerts generated by these rules may be indications of infection. This can be confirmed by examining the host machine exhibiting the behavior and/or by collecting and analyzing the network traffic collected between the host and the traffic's destination.

Network Anomaly

Threat List-TOR Server or TOR Exit Node

This pair of AI Engine rules looks for communication involving hosts associated with the TOR network. Within most corporate networks, it is unlikely that hosts or users have acceptable reasons for utilizing TOR. Because these rules are designed to alarm on either inbound or outbound network traffic, one of two things may be occurring: a host on the TOR network is sending traffic to your network, which may indicate an attack or reconnaissance event; or a device on the network is communicating with a TOR host, which could indicate a network user joining the TOR network.



Log Requirements

Utilize the following log sources:

- Any log data that parses IP addresses or hostnames with IPtoName resolution enabled

Knowledge Base Content

Type	Name	ID
AIE Rule	Ext:Susp:Threat List:Tor Exit Node	484
AIE Rule	Ext:Susp:Threat List:Tor Server	485
List	Threat List: Tor Servers	-2183
List	Threat List: Tor Exit Nodes	-2184

Configuration

To use these threat lists, LogRhythm-provided PowerShell scripts must be scheduled to update the lists. See the Third Party Threat List Integration Guide for details.

Actions

Be mindful that the actual purpose for using TOR cannot be known by this alarm alone, and the internal or external TOR user could be using anonymity for benign purposes. To determine this, first look at directionality -- it should be clear whether the traffic is originating inside or outside of your network. For inbound traffic, run an investigation over the time period covering the traffic, and set origin or impacted host to the TOR host. If the traffic is outbound, an investigation on that host will help determine if it is compromised, or if there is a potential policy violation by a user joining a TOR network.

Network Anomaly Connection with Non-Whitelisted Country

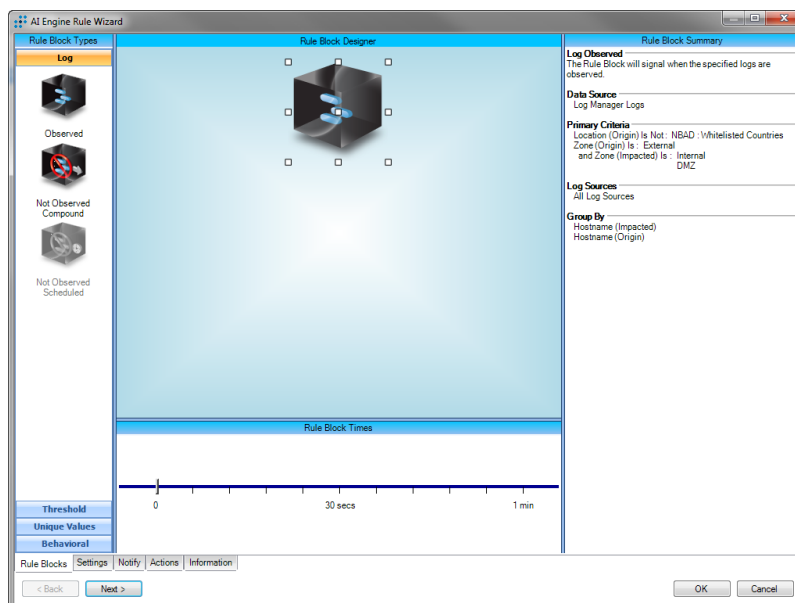
Although many organizations are multinational and regularly have VPN connections from external countries, connections from countries that don't have an organizational presence should be suspicious. This rule detects VPN connections from countries not in a custom whitelist.

Log Requirements

The following types Log Sources must be collecting:

- Firewall
- Perimeter Flow Data
- LogRhythm Network Monitor or equivalent network protocol analyzer

Knowledge Base Content



Type	Name	ID
AIE Rule	Susp:Inbound Connection With Non-Whitelisted Country	439
AIE Rule	Susp:Outbound Connection With Non-Whitelisted Country	454

Configuration

The "NBAD White Listed Countries" System List should be populated with allowed countries.

Actions

Whenever there is an inbound connection attempt from a country not on the whitelist, an AIE event will be generated. The origin IP should then be investigated for other suspicious activity.

Network Anomaly

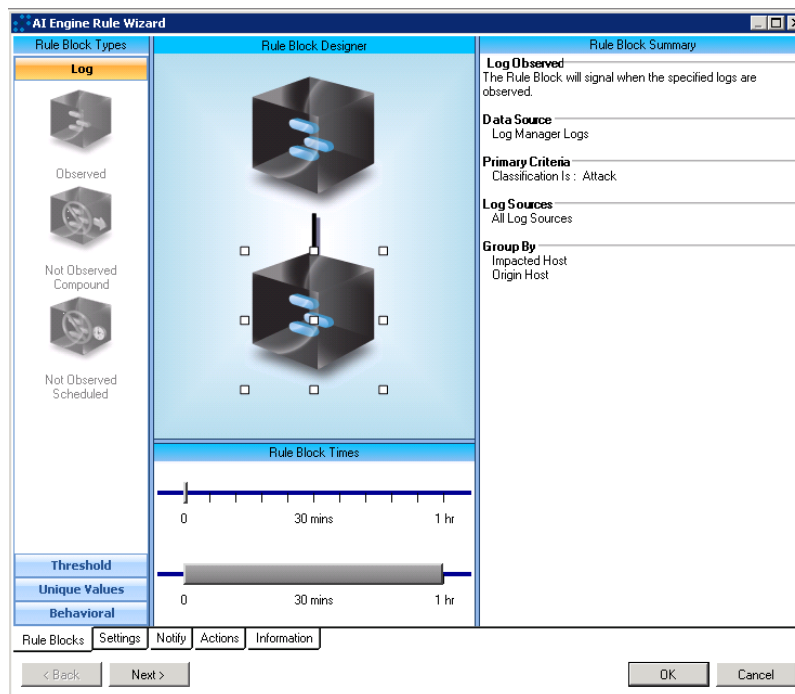
Host Compromised-Recon Followed By Attack

Generally, reconnaissance will be performed on a network before an attack is launched. Attackers will fingerprint hosts and applications to determine if any operating systems or applications are vulnerable before using known exploits against them. By utilizing network security monitors that can detect reconnaissance techniques, this activity can be detected.

Log Requirements

A combination of the following Log Sources can be used

- Intrusion detection devices
- Network security monitoring devices



Knowledge Base Content

Type	Name	ID
AIE Rule	Ext:Host Comp:Recon Followed By Attack	20
AIE Rule	Int:Host Atck:Recon Followed By Attack	54

Configuration

Optional: Create an Exclude Filter for Origin Host in Rule Block 1 and/or Rule Block 2 where the Origin Host is the name of any vulnerability scanners.

Actions

There are two versions of this rule: Internal and External. This rule will fire when external reconnaissance is followed by an attack on the same machine, indicating an attack pattern. The origin host should then be investigated further to determine if it has been compromised.

Network Anomaly Attack Followed by Firewall Allow

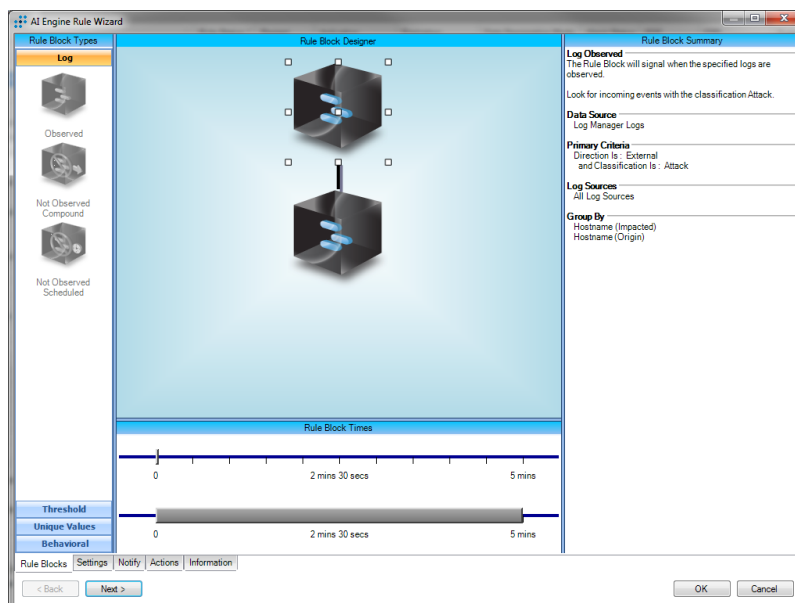
Intrusion Detection Systems are designed to detecting malicious activity traversing the network, but may not always be able to determine if an attack was successful. This rule looks for an Attack event followed by allowed traffic between the same two hosts. This could be an indication that an attack was successful and the attacker is exploiting the compromised system.

Log Requirements

The following log sources must be collecting:

- Intrusion Detection System
- LogRhythm Network Monitor or equivalent network protocol analyzer

Knowledge Base Content



Type	Name	ID
AIE Rule	Susp:Attack Followed By Firewall Allow	420

Configuration

Optional: Create an Exclude Filter in Rule Block 1 for publicly available services such as: Impacted Host is a web server and Impacted Port is 80.

Actions

The host should be further investigated for evidence of possible infection.

Network Anomaly Excessive Firewall Denies

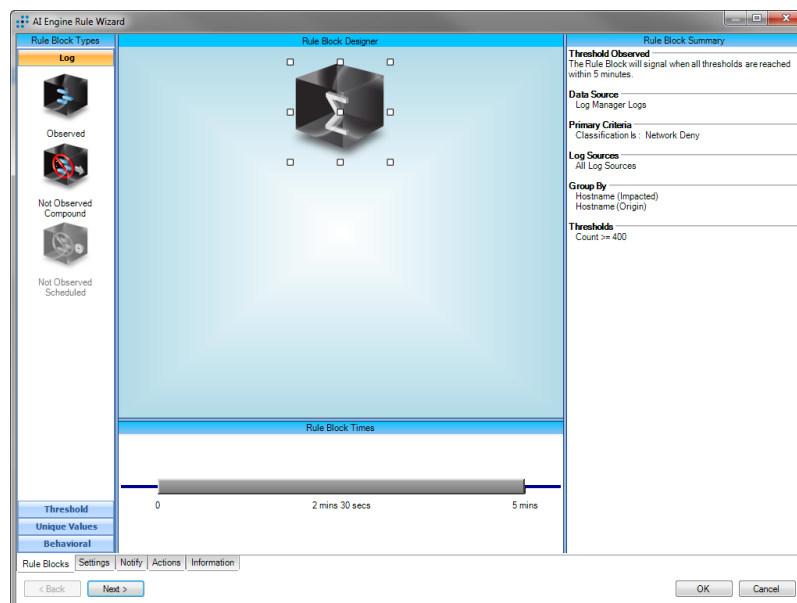
A spike in firewall denies can indicate any number of issues -- from external vulnerability scans, to malware beaconing, to users running non-standard services. This rule alerts security analysts to begin investigating this suspicious behavior.

Log Requirements

The following log sources must be collecting:

- Firewalls

Knowledge Base Content



Type	Name	ID
AIE Rule	Susp:Excessive External FW Denies	453
AIE Rule	Susp:Excessive External FW Denies Flwd By Allow	472
AIE Rule	Susp:Excessive FW Accepts to Multiple IHosts	423

Configuration

This rule will look for 400 or more firewall denies for a single origin host within a 5 minute window. The threshold should be adjusted based on use case. For instance, if looking for a user attempting to access an external FTP site for possible data exfiltration, the threshold should be set much lower.

Actions

Based on tuning, this rule should be the starting point for further investigation.

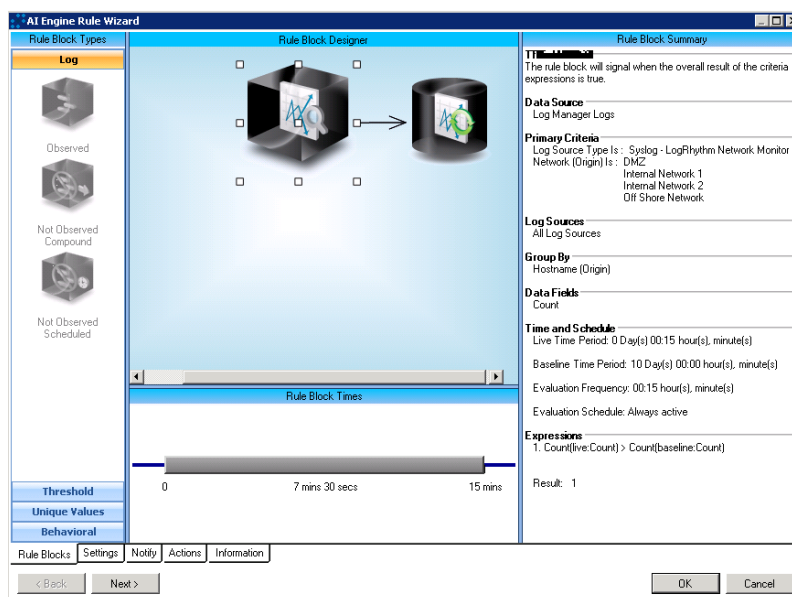
Network Anomaly Rogue Host Detection

New, unauthorized hosts are known as Rogue Hosts. These devices may be used by malicious actors as backdoors into the network or data exfiltration proxies leaving the network. Visibility into new hosts allows for such activity be detected before breaches spin out of control. This rule will alarm on all new host activity in the past 10 days and compare live data to past collection.

Log Requirements

The following prerequisites must be met:

- Collecting from a device that shows network traffic LogRhythm Network Monitor OR Firewall traffic OR Netflow, etc
- Define all internal networks ranges if possible. At the very least define your internal wireless network ranges
- In Log Manager advanced settings, turn on DNSIPToName resolution



Knowledge Base Content

Type	Name	ID
AIE Rule	Susp:Rogue Host Detection	383

Configuration

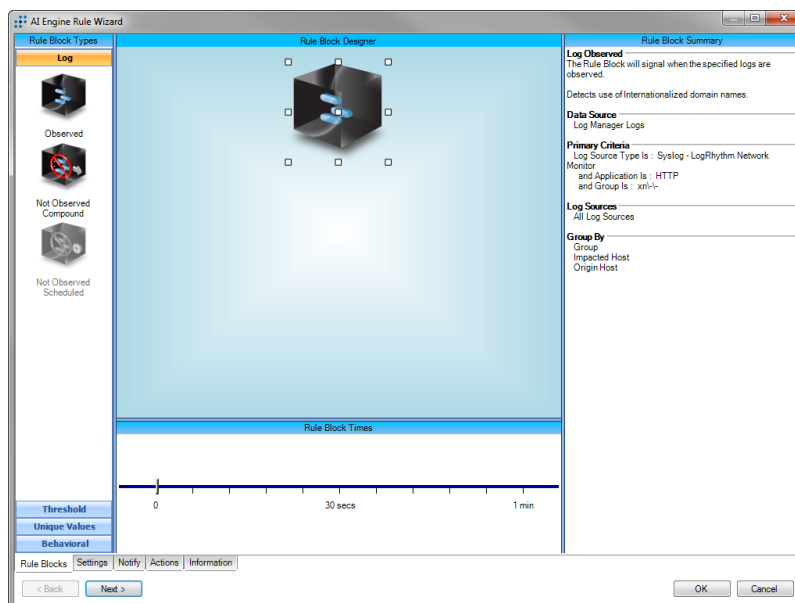
When turning on this rule for the first time, turn on suppression for 2 or 3 days to create an accurate baseline. After this period, turn off suppression.

Actions

Anytime a new host shows up that is not in the 10-day baseline, the LogRhythm user will be able to see this event. It's not uncommon for many false positives to be generated as the baseline continues to solidify. New hosts should be investigated to ensure they are authorized.

Network Anomaly Internationalized Domain Names

Since 2009, the Domain Name System has supported URLs that contain non-ASCII, Unicode characters from Cyrillic, Chinese, Arabic, etc. Even symbols are now included. These new domains are known as Internationalized Domain Names (IDN). These new characters allows for a potential 'Homographic Attacks' -- registering a malicious site using characters that are technically distinct yet visually identical to ASCII counterparts, and then exploiting this fact via phishing or other means. Additionally, the Punycode representation of Unicode may confuse users and result in a phish. For example, 'logrhythm.com' with a trademark symbol in Unicode will be represented as 'xn--logrhythm-cma.com' in Punycode/ASCII. Both may appear legitimate in the eyes of unsuspecting users.



Log Requirements

At least one of the following Log Sources must be collecting:

- LogRhythm Network Monitor
- An equivalent network protocol analyzer

Knowledge Base Content

Type	Name	ID
AIER	Susp:IDN	537

Configuration

Because most IDNs are not used for malicious purposes, legitimate domains that are frequently seen within the organization can be excluded in the AIE rule block to eliminate false positives.

Actions

When this alarm is seen from hosts within the network, they should be investigated for signs of an infection or successful phishing attempt.

Network Anomaly

Suspicious Top Level Domains

Many Top Level Domains (TLDs) have been identified as having an inordinate amount of malicious domains. Malicious entities (eg, botnet controllers or exploit kits landing pages) will frequently exploit lax registration policies to create their malicious infrastructure using these TLDs. In addition to supplying a list of several suspect TLDs, this rule allows each organization to specify their own in an ad hoc fashion.

Log Requirements

At least one of the following Log Sources must be collecting:

- LogRhythm Network Monitor
- An equivalent network protocol analyzer

Knowledge Base Content

Type	Name	ID
AIER	Susp:Atypical TLDs	538

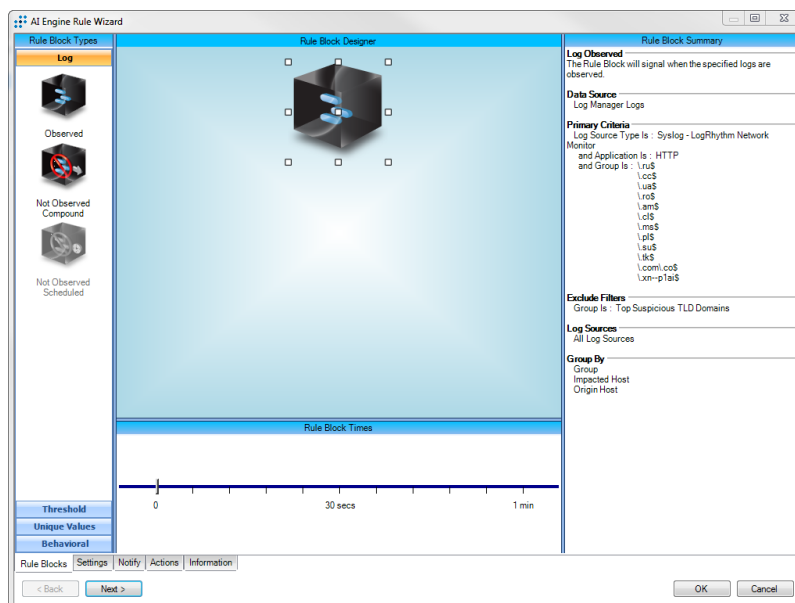
Configuration

The default suspicious domains are ru, cc, ua, ro, am, cl, ms, pl, su, tk, com.co, xn--p1ai -- any additions can be customized, but should following the same regex formatting.

It's likely that false positives will occur before tuning to the organization's network. TLDs can either be removed from this list or individual domains can be added to the exclude section of the AIE rule block. A whitelist of legitimate domains using these TLDs is also provided as the list 'Top Common Domains on Suspicious TLDs'.

Actions

Traffic to these suspicious TLDs should be further investigated to see if the domain should be whitelisted or is actually malicious. Hosts visiting these malicious sites should then be examined to determine if they are compromised.



Account Anomaly

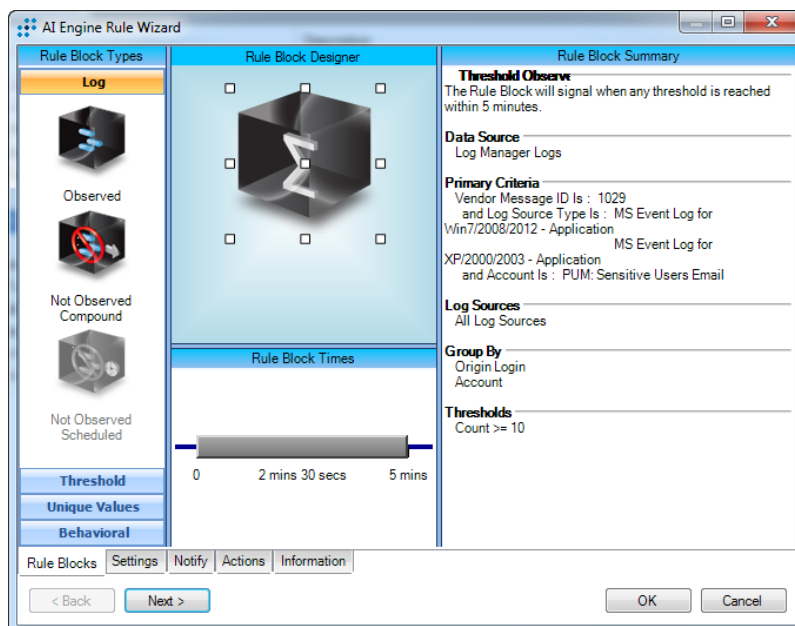
Failed Non-Primary Exchange Account Authentication

Restricting and tracking IT administrator access to sensitive data is difficult. Fortunately, in addition to having visibility into the audit trails necessary to track such activity, LogRhythm also prevents that trail from being deleted. This alarm rule detects attempts by a user to access specified Exchange accounts specified in the "PUM: Sensitive Users Emails", assuming that user isn't also the primary user on the machine initiating the authentication.

Log Requirements

The following types of Log Sources must be collecting:

- Windows Security Event Logs



Knowledge Base Content

Type	Name	ID
AIE Rule	Acnt Susp:Multiple Failed Attempts To Logon To Non-Primary Exchange Account	163

Configuration

Ensure MS Exchange is configured to audit access control and logon activity. This is documented in the "Privileged User Monitoring" deployment guide.

Actions

Once this rule is triggered, investigate the root cause by analyzing associated metadata and utilizing LogRhythm's expansive queries:

- Launch an additional investigation by setting origin login to the suspect user, targeting all log sources to find other activity from the account.
- To build a more complete picture on what the user has been up to, launch an additional investigation by setting account to the suspect user.
- Utilize the "PUM: Privileged User Activity" investigation layout for quicker visibility into the origin of the alarm
- Enable the smart response plugin "Disable Local windows Account" to automatically disable the user account. This is described in the "Activate Smart Response Plugin" section of the deployment guide.

Account Anomaly

Recently Disabled Account Access Activity

When a privileged user leaves an organization, it can be difficult to find and remove all previous accesses and authorizations. Monitoring for account deleted or account disabled events allows for correlations to be made when these events are followed by access failures or authentication failures -- these are indications that a individual is probing for any old access privileges still present in the network.

Log Requirements

One of the following log source types must be collecting:

- Windows Security Event Logs
- \nix host logs

Knowledge Base Content

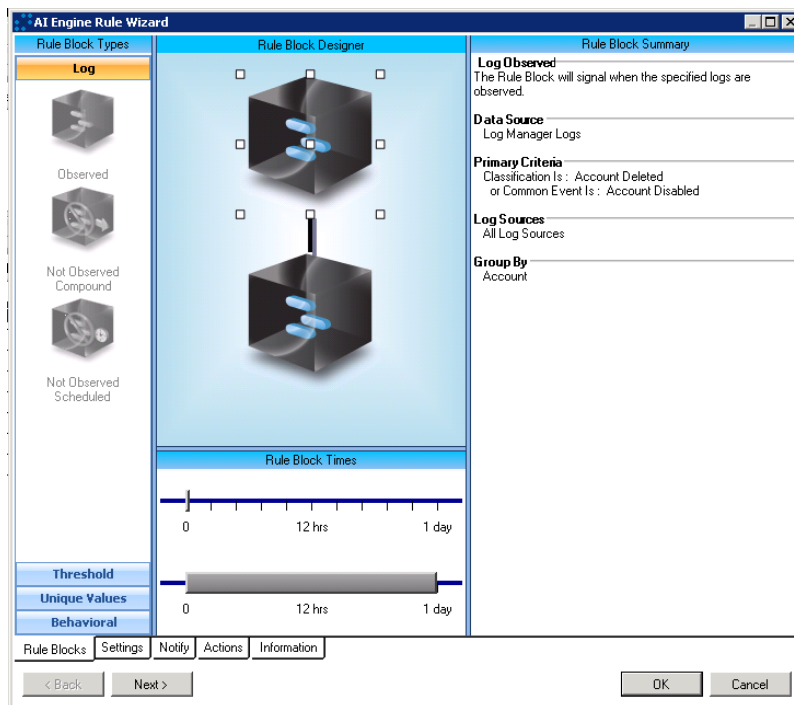
Type	Name	ID
AIE Rule	Acnt Susp:Recently Disabled Account Access Failures	76
AIE Rule	Acnt Susp:Recently Disabled Account Access Success	88
AIE Rule	Acnt Susp:Recently Disabled Priv Acnt Access Failures	513
AIE Rule	Acnt Susp:Recently Disabled Priv Acnt Access Success	512

Configuration

In the Local Security Policy on Windows hosts, make sure Audit Account Management is turned on for successes and Audit Account Logon events is turned on for success and failures.

Actions

After an employee has left an organization and unsuccessfully attempts to access network resources, this alarm will trigger. First, verify all access has been removed from that user's account. Additionally, the user should then be investigated in LogRhythm to see why they were attempting unauthorized access.



Account Anomaly Account Created, Used, Deleted

Attempting to hide their tracks, a malicious insider might create a temporary account for performing malicious activity. This will allow them to access data or some other resource through this proxy account before deleting it. This rule will detect such activity and maintain the evidence trail.

Log Requirements

Utilize the following log sources:

- Windows Domain Control Security Event Logs

Knowledge Base Content

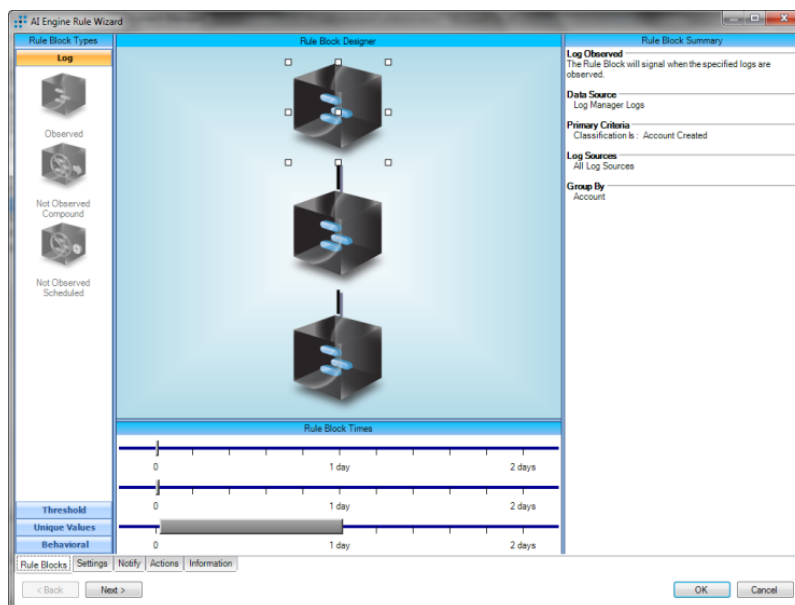
Type	Name	ID
AIE Rule	Acnt Susp:Account Created Used Deleted	37

Configuration

None required.

Actions

If suspicious, users that trigger this alarm should be questioned about their activity. An Investigation should be launched to determine the activity performed by the temporary account, and this should be used to verify the original user's story.



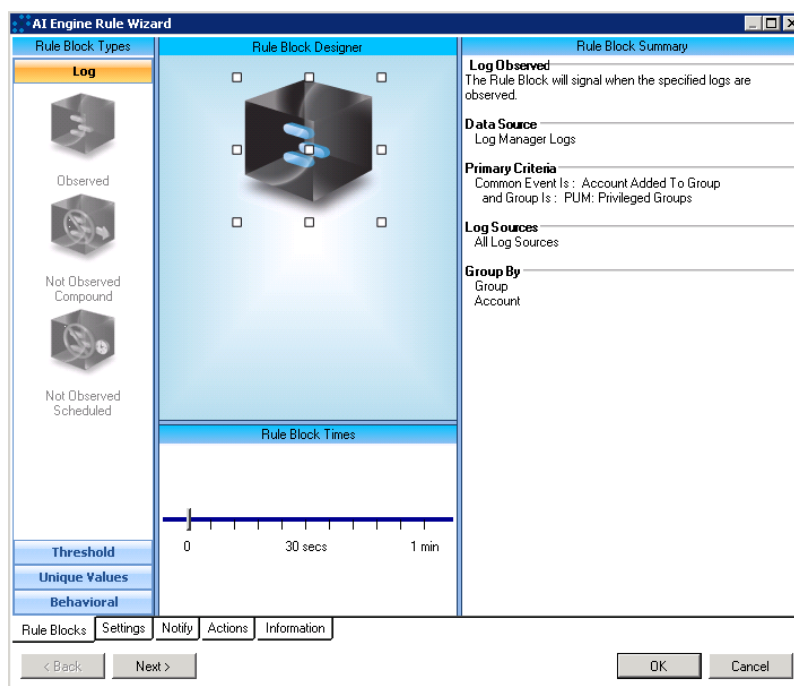
Account Anomaly New Administrator Activity

Tracking administrator actions is useful for both auditing potential privilege abuse and for security monitoring. This rule is part of the Privileged User Monitoring (PUM) module and will alarm when accounts are added to groups that have elevated privileges. Both malicious actors and rogue administrators may create additional accounts in order to hide their trail -- but they will not escape this rule.

Log Requirements

Utilize the following log sources:

- Populate the list PUM: Privileged Groups with privileged groups relevant to your organization
- Windows Security Event Logs
- \nix host logs



Knowledge Base Content

Type	Name	ID
AIE Rule	Acnt Audit:New Administrator Activity	164

Configuration

In the Local Security Policy on Windows hosts, make sure Audit Account Management is turned on for successes.

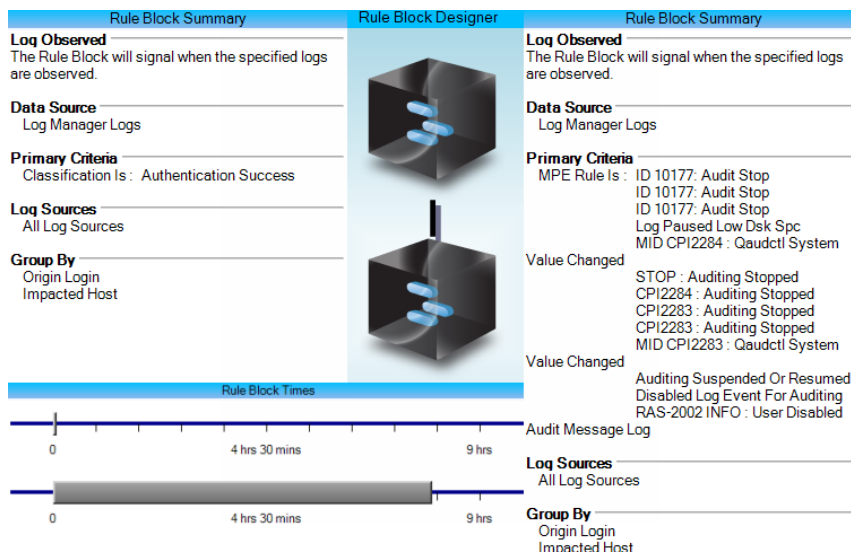
Optional: Configure smart response to automatically add this user to the privileged user list for use with other PUM AI Engine rules.

Actions

New users added to a privileged group should be confirmed as legitimate -- otherwise, they should be considered malicious and deleted before determining their origin.

Account Anomaly Audit Disabled by Admin

After achieving privilege escalation, a malicious actor will attempt to hide their tracks. This means removing data from logs, hiding malicious files, and disabling audits. Fortunately, LogRhythm collects from logs in real time, meaning that these events can be tracked.



Log Requirements

Utilize the following log sources:

- Windows Security Event Logs
- \nix host logs

Knowledge Base Content

Type	Name	ID
AIE Rule	Int:Susp:Audit Disabled By Privileged User	36

Configuration

In Windows, make sure the audit object access setting is turned on for successes and failures in the local security policy.

Actions

If audits are being disabled, it's highly likely that malicious activity is taking place. Immediately launch LogRhythm investigations on the Log Source where this is occurring.

Account Anomaly Concurrent VPN Connections

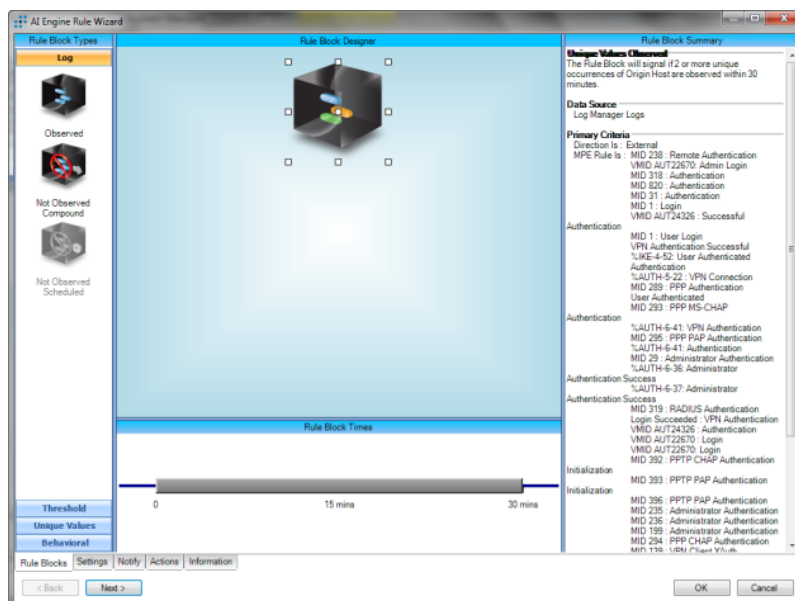
Users will typically only have a VPN connection from one IP address at a time. If a parallel VPN connection is detected from a different source, this may be indication that the credentials of that user have been compromised and are being used by a malicious actor. This rule will detect such concurrent connections.

Log Requirements

Utilize the following log source:

- VPN Logs

Knowledge Base Content



Type	Name	ID
AIE Rule	Ext:Acnt Comp:Concurrent VPN Auths From Same User	75

Configuration

Optional: Users that have legitimate, concurrent VPN connections can be whitelisted for reduced false positives.

Actions

When this rule fires, an investigation should be launched against the user in question to discover any malicious activity.

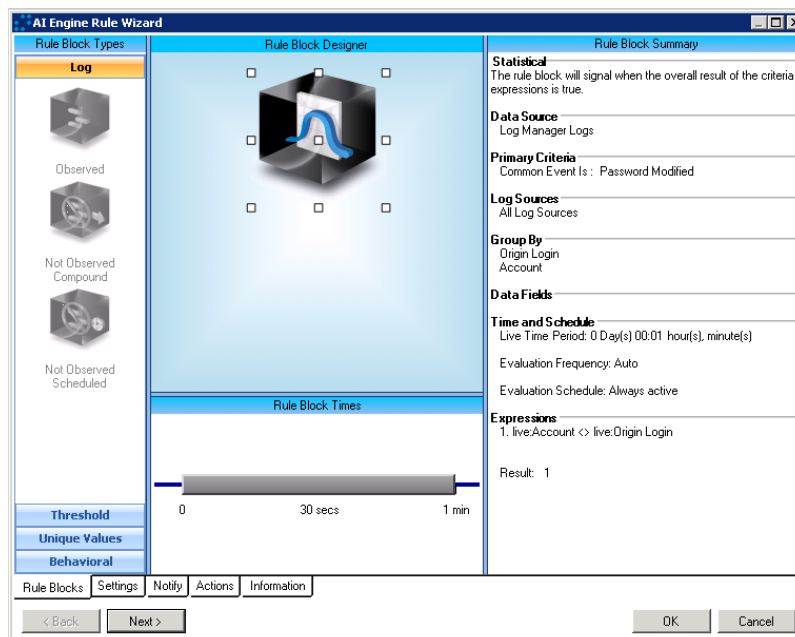
Account Anomaly Password Modified By Another User

Typically, users should only be modifying their own password, and awareness of external password changes could be indication of an account compromise. For example, this rule will fire if a malicious user is changing passwords for easier access.

Log Requirements

One of the following log source types must be collecting:

- Windows Security Event Logs
- \nix host logs



Knowledge Base Content

Type	Name	ID
AIE Rule	Acnt Audit:Password Modified By Another User	250

Configuration

For Windows hosts, make sure Audit Account Management is turned on for successes in the local security policy.

To eliminate potential false-positive alarms for IT administrators changing passwords, create a list of all IT admins and then exclude that list from the origin logins. Although this will cut down on excessive alarms, keep in mind that it may also leave a blind spot if an administrator is compromised.

Actions

Anytime a user is seen modifying a password on an account that is not their own this rule will trigger. The origin login field will show the user who modified the password; the account field will show the account that has been modified. The user modifying another account's password should be investigated to make sure it is legitimate activity.

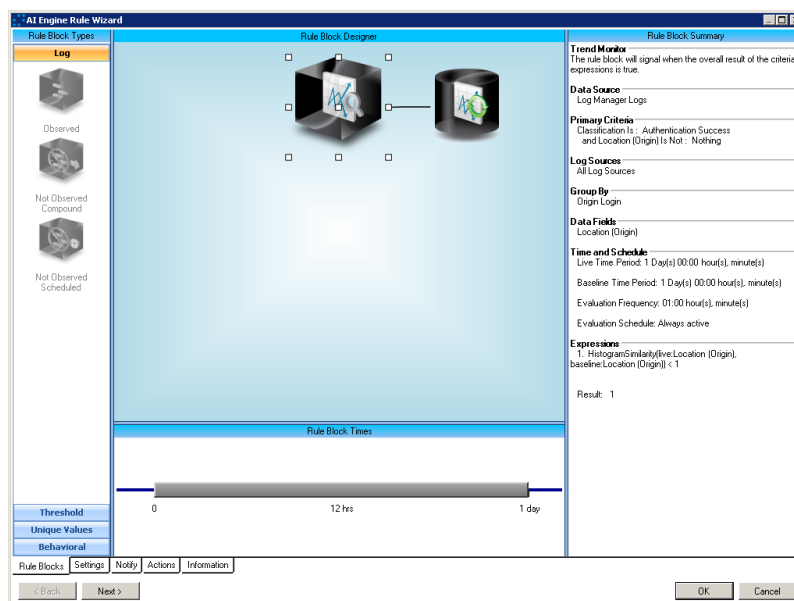
Account Anomaly Abnormal Origin Location

If a user authenticates to the network from an atypical physical location, this may be a sign that the user's account has been compromised and is being accessed by a malicious actor. This rule will track locations on a per user basis, baselining log in origins for the past 30 days. Once a user authenticates from a location not seen in that period, the rule will trigger.

Log Requirements

One or more of the following Log Source types must be collecting:

- Windows Security Event Logs
- \nix host logs
- Any logs tracking authentication activity



Knowledge Base Content

Type	Name	ID
AIE Rule	Acnt Susp:Abnormal Origin Location	288

Configuration

In Windows, make sure the audit object access setting is turned on for successes and failures in the local security policy.

This rule will most likely be activated frequently as users travel and log into the network remotely -- the first step to reducing these false positives will be to create a list of frequent travelers that can be excluded from this rule. A secondary exclude list could be made for locations where individual users will infrequently visit, but still see regular access by the company as a whole (eg, a training center where several employees only visit once per year).

Actions

By default, this rule will create an event and not an alarm. Ultimately, this rule is best used when paired with additional indications of account compromise.

If investigating a suspicious login, perform the following:

- Launch an additional investigation using the suspect username as origin login
- Launch an additional investigation using the suspect username as account
- Enable the smart response plugin "Disable Local Windows Account" to automatically disable bad acting users. This is described in the Activate Smart Response Plugin section of the deployment guide.

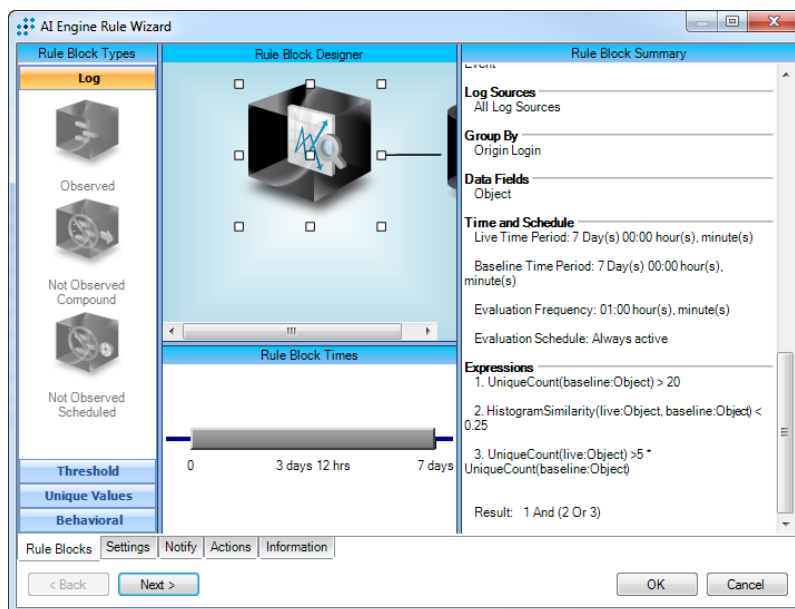
Account Anomaly Abnormal File Access

File Integrity Monitoring (FIM) allows LogRhythm to track access and changes to important files. Additionally, by trending an individual user's weekly access to files under FIM protection, LogRhythm can find deviations from week to week that may be indications of account compromise or an insider threat -- specifically, accessing either a different set of sensitive files (only 25% similarity) between weeks or accessing many more unique objects than the week before (tuned to trigger at five times as many).

Log Requirements

One or more of the following Log Source types must be collecting:

- Windows Security Event Logs
- \nix host logs
- Any logs showing FIM activity



Knowledge Base Content

Type	Name	ID
AIE Rule	Acnt Susp:Abnormal File Access	287

Configuration

In Windows Agents, turn on object access successes and failures in the local security policy.

This rule will likely generate false positives, particularly in environments where users are constantly working on new projects, referencing new guides/design specs, and using new tools. This rule is not set to trigger an alarm by default -- only an event will be generated when it fires. This event can then be used for more advanced, highly correlated account compromised scenarios.

Actions

If investigating this event:

- Launch an additional investigation using the suspect username as origin login
- Launch an additional investigation using the suspect username as account
- Enable the smart response plugin "Disable Local windows Account" to automatically disable suspicious or compromised users. This process is described in the Activate Smart Response Plugin section of the deployment guide.

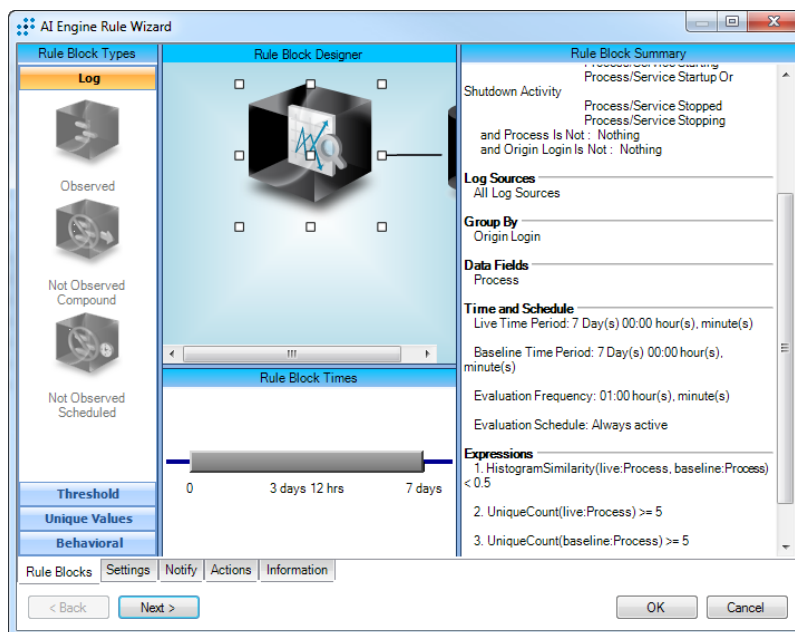
Account Anomaly Abnormal Process Activity

This rule compares processes run by a user on a week to week basis. Significant weekly deviations, in this case a 75% difference in processes, may be an indication that the account is being controlled by an external entity.

Log Requirements

One or more of the following Log Source types must be collecting:

- Windows Security Event Logs
- \nix host logs
- Any other process monitoring logs



Knowledge Base Content

Type	Name	ID
AIE Rule	Acnt Susp:Abnormal Process Activity	289

Configuration

Ensure Audit Process Tracking is enabled for successes and failures in the Windows local security policy.

This rule can generate false positives as users switch tasks between weeks -- therefore, it's best to use these events in conjunction with other indicators of compromise.

Actions

To aid investigations into these events:

- Launch an additional investigation using the suspect username as origin login
- Launch an additional investigation using the suspect username as account
- Enable the smart response plugin \u201cDisable Local Windows Account\u201d to automatically disable suspicious users. This is described in the Activate Smart Response Plugin section of the deployment guide.

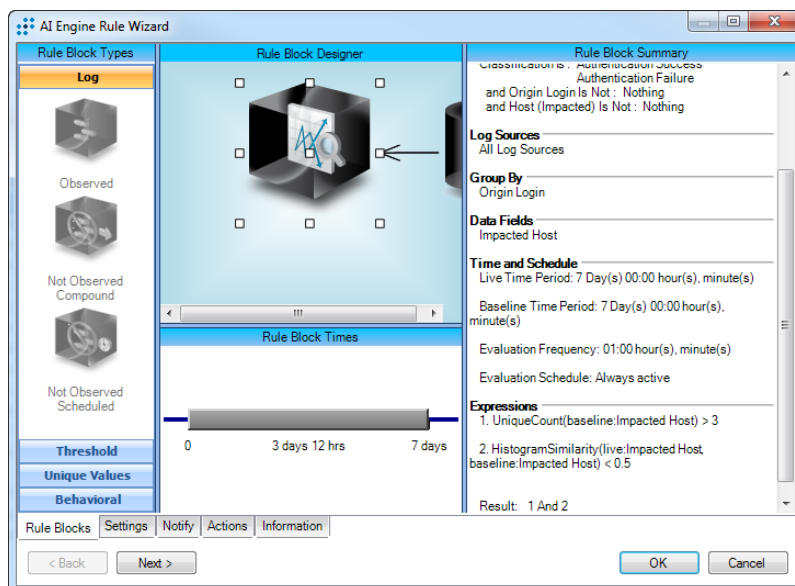
Account Anomaly Abnormal Authentication Behavior

A user that significantly changes the services they use may be an indication of compromise -- specifically, a malicious actor that is using the new account to access as many parts of the local infrastructure as possible. This rule tracks the hosts that a user authenticates with in a seven day period and sets a baseline. If in the next seven-day period the user has less than fifty-percent overlap between hosts, this rule will trigger.

Log Requirements

One or more of the following Log Source types must be collecting:

- Windows Security Event Logs
- \nix host logs
- Any logs showing authentication activity.



Knowledge Base Content

Type	Name	ID
AIE Rule	Acnt Susp:Abnormal Authentication Behavior	286

Configuration

In Windows, make sure Audit Account Management is activated for successes in the Local Security Policy.

This rule is designed to be noisy -- for example, it's not uncommon to see this rule fire in a development environment where users are connecting to new hosts each week. When this rule does fire, it will only create -- not alarm. This will allow for the event to be fed back into the master corroborated rule for more advanced highly correlated account compromised scenarios.

Actions

To aid investigations into events triggered by this rule:

- Launch an additional investigation using the suspect username as origin login
- Launch an additional investigation using the suspect username as account
- Enable the smart response plugin "Disable Local windows Account" to automatically disable bad acting users. This is described in the Activate Smart Response Plugin section of the deployment guide.

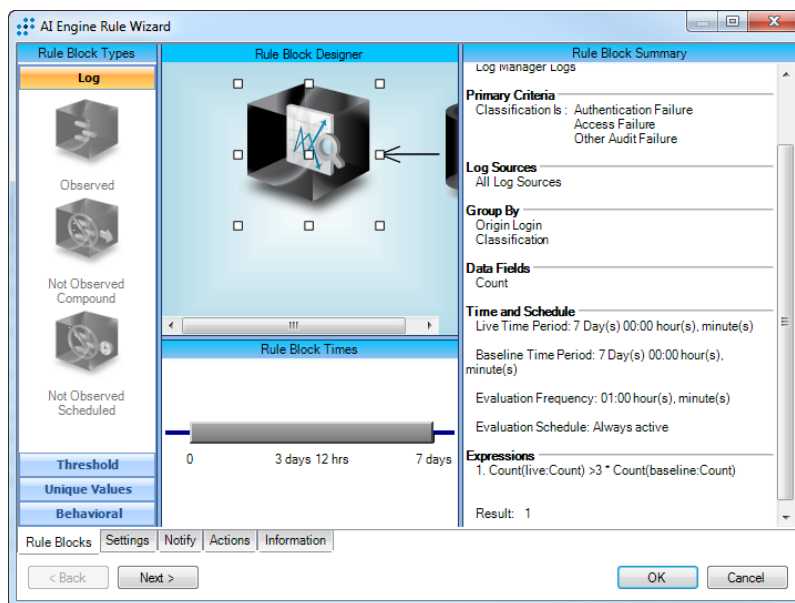
Account Anomaly Abnormal Amount Of Audit Failures

Abnormal amounts of audit failures can be an indication of an account compromise. This rule analyzes such failures by baselining normal audit failures for individual users each seven day period. If the next seven day period sees a three-fold increase in audit failures, the event will trigger.

Log Requirements

One or more of the following Log Source types must be collecting:

- Windows Security Event Logs
- \nix host logs
- Any logs showing authentication activity.



Knowledge Base Content

Type	Name	ID
AIE Rule	Acnt Susp:Abnormal Amount Of Audit Failures	285

Configuration

In Windows, make sure Audit Account Management is activated for successes in the Local Security Policy.

Like many statistical analytics, this rule is can be noisy. It's not uncommon to see this rule fire as users mistype their password more one week than the previous week. By default, this rule will not trigger an alarm -- only an event will be created. This allows the event to be fed back into the master corroboration rule for more advanced, highly-correlated account compromised scenarios.

Actions

To aid investigations into these events:

- Launch an additional investigation using the suspect username as origin login
- Launch an additional investigation using the suspect username as account
- Enable the smart response plugin "Disable Local windows Account" to automatically disable bad acting users. This is described in the Activate Smart Response Plugin section of the deployment guide.

General Activity

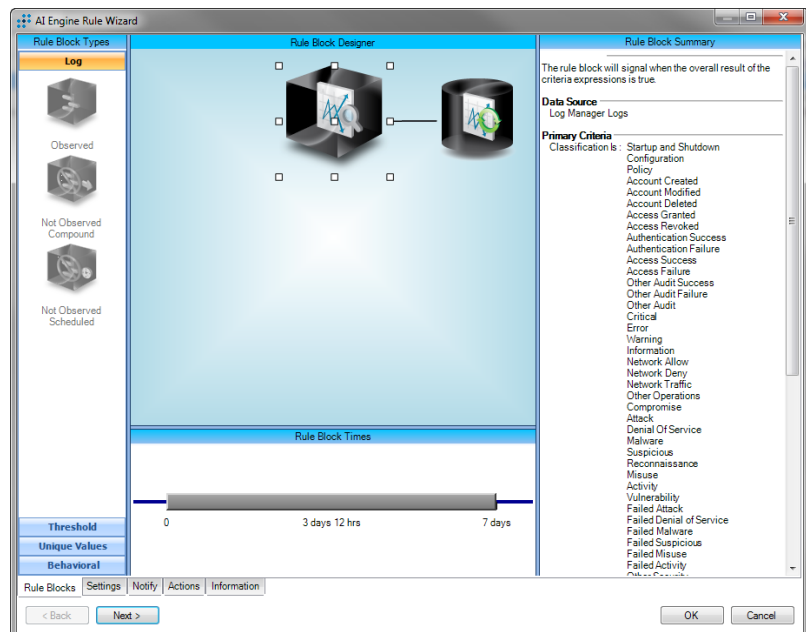
New Common Event

Identifying new Common Events generated by a single log source can help find many types of issues. For instance, if a configuration change is made that causes a new type of Operations Information Common Event to be generated, it could be indicative of a misconfiguration. Or, when a new IDS is deployed and churning away false positives, a new type of IDS event is something that would be interesting to investigate. This rule is designed to monitor generated Common Events separately for each Log Source and generate an event when a new Common Event is observed. Specifically, it will alarm on Common Events not seen in the preceding 7 days.

Log Requirements

General log collection should be configured:

- General logs



Knowledge Base Content

Type	Name	ID
AIE Rule	General:New Common Event	468

Configuration

Optional Configuration: This rule is configured to monitor all log sources for new Common Events. If it's desirable to track only specific log sources (eg, a new device deployment), a log source filter can be used.

Actions

Actions will be dependent on the use-case -- debugging a new device will have a different follow-up than security-related events.

Host Anomaly Abnormal Process Activity by Host

This rule compares processes run by a host on a week to week basis. Significant weekly deviations, in this case a 50% difference in processes, may be an indication that the account is being controlled by an external entity and malicious tools are running on the infected machine.

Log Requirements

One or more of the following Log Source types must be collecting:

- Windows Security Event Logs
- \nix host logs
- Any other process monitoring logs

Rule Block Summary

Trend Monitor
The rule block will signal when the overall result of the criteria expressions is true.

Data Source
Log Manager Logs

Primary Criteria
Common Event Is : Process/Service Restarted
Process/Service Restarting
Process/Service Started
Process/Service Starting
Process/Service Startup Or Shutdown Activity
Process/Service Stopped
Process/Service Stopping
and Process Is Not : Nothing
and Host (Impacted) Is Not : Nothing

Log Sources
All Log Sources

Group By
Impacted Host

Data Fields
Process

Time and Schedule
Live Time Period: 7 Day(s) 00:00 hour(s), minute(s)
Baseline Time Period: 7 Day(s) 00:00 hour(s), minute(s)
Evaluation Frequency: 01:00 hour(s), minute(s)
Evaluation Schedule: Always active

Expressions
1. HistogramSimilarity(live.Process, baseline.Process) < 5
2. UniqueCount(live.Process) >= 5
3. UniqueCount(baseline.Process) >= 5
Result: 1 And 2 And 3

Rule Block Designer

Data Block Summary

Trend Baseline
The linked data for the associated rule block.

Data Source
Log Manager Logs

Primary Criteria
Common Event Is : Process/Service Restarted
Process/Service Restarting
Process/Service Started
Process/Service Starting
Process/Service Startup Or Shutdown Activity
Process/Service Stopped
Process/Service Stopping
and Process Is Not : Nothing
and Host (Impacted) Is Not : Nothing

Log Sources
All Log Sources

Group By
Impacted Host

Data Fields
Process

Time and Schedule
Live Time Period: 7 Day(s) 00:00 hour(s), minute(s)
Evaluation Frequency: 00:00 hour(s), minute(s)
Evaluation Schedule: Always active

Rule Block Times
3 days 12 hrs

Knowledge Base Content

Type	Name	ID
AIE Rule	Behavioral Anomaly: Abnormal Process Activity by Host	295

Configuration

Ensure Audit Process Tracking is enabled for successes and failures in the Windows local security policy.

This rule can generate false positives on hosts that frequently switch tasks between weeks -- therefore, it's best to use this rule on machines that are relatively stable.

Actions

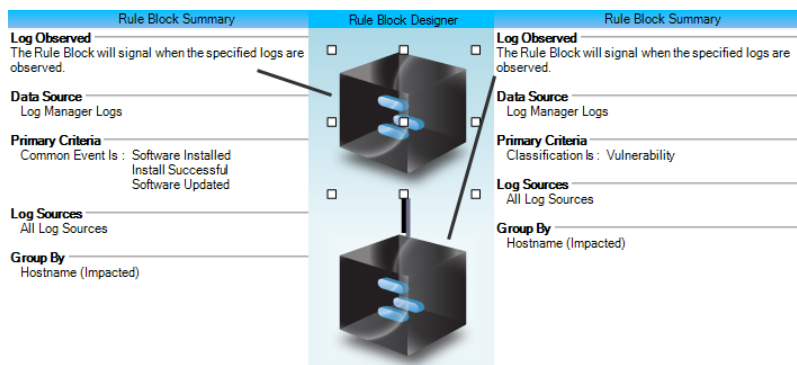
To aid investigations into these events:

- Launch an additional investigation using the suspect username as origin login
- Launch an additional investigation using the suspect username as account
- Enable the smart response plugin \u201cDisable Local Windows Account\u201d to automatically disable suspicious users. This is described in the Activate Smart Response Plugin section of the deployment guide.

Vulnerability

Vulnerability After Software Install

New software installations or updates can introduce known vulnerabilities. When vulnerability scanners detect software versions susceptible to exploits, LogRhythm can correlate that information to recent changes to the system.



Log Requirements

The following log sources are required:

- Windows event logs
- A Vulnerability Scanner

Knowledge Base Content

Type	Name	ID
AIE Rule	Vulnerability: After Software Install	494

Configuration

Certain devices that run outdated software versions but are properly hardened can be whitelisted from this rule to cut down on repeated false positives.

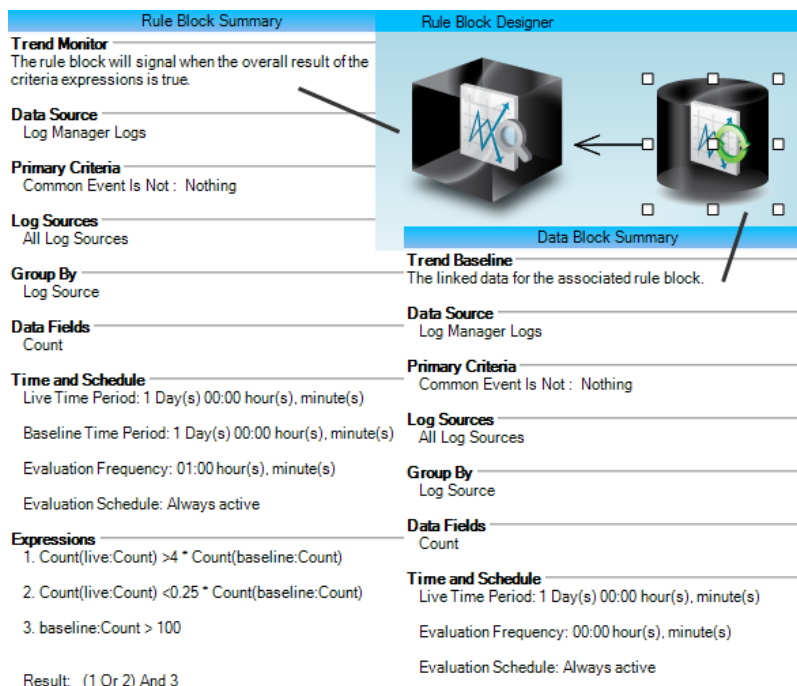
Actions

Vulnerable software should be immediately updated to a secure version or hardened in such a way to remove any possibility of exploitation. For more information on the specific vulnerability, search the National Vulnerability Database (<https://nvd.nist.gov/>).

Operations

Ops Warning: Abnormal Log Volume Fluctuation

Large fluctuations in the number of logs generated by a system can be cause for concern. An increasing log volume may indicate a malware outbreak, denial of service attack, or other noisy malicious activity. Significant log decreases may mean configuration errors, hardware failures, or other problems. Because LogRhythm is already tracking incoming logs, it's very easy to keep tabs on logging metadata.



Log Requirements

General log collection should be configured:

- General logs

Knowledge Base Content

Type	Name	ID
AIE Rule	Ops Warning: Abnormal Log Volume Fluctuation	248

Configuration

Add include filters for specific higher risk hosts of interest, or exclude filters for log sources that frequent have large fluctuations.

Actions

The first step after seeing this alarm should be to find other alarms from the same log source -- although it might not always be the case, hopefully other alarms were triggered that can help diagnose the issue.