
Argent SIEM-Complete

Features and Benefits

White Paper



ARGENT



SIEM Policy definitions provide the ability to save collected events as Performance Data that are easily displayed in the Historical Graph Reports.

ARGENT OMEGA (v2.2.2202.8)

Home Theme help.Argent.com Argent Instant help Logout

Administration

- Generator Settings
 - Argent Omega
 - Argent Alert Mechanism
 - Argent Forecaster
 - Argent SIEM-Complete
 - SIEM Policy
 - Active Directory Authentication
 - Active Directory Objects
 - Brutal Force Attack
 - File Deletion
 - Hacker Alert
 - Windows Logon
 - PL_FAILED_INTERACTIVE_LOGON
 - PL_INTERACTIVE_LOGON**
 - PL_LOCKOUT_INCIDENTS
 - PL_LOGON_TO_CRITICAL_ASSETS
 - Archive Repository
 - License
 - Network Scan
 - Security
 - Event Logs
 - Argent SuperMaps
 - Topology Maps
 - Locations
 - Contacts

SIEM-Complete Logic: Successful Windows Logon

Temporarily Disabled:

Skip Log Records Over: 24 Hours

Archive Repository: {default}

Monitoring Groups: &MG_WINDOWS_SERVERS

Schedule Time: 00:00:00 Repeat Task

Repetition Interval: 10

Repetition Unit: Minutes

Repeat Task Until: 23:59:59

Calendar: CAL_ALL_DAYS

Trace Level: Normal

Save Performance Data To the Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

Application:

Reference URL:

Console Comment: {default}

Copyright © 2022 Argent Software. All Rights Reserved Admin User: administrator

Copyright 2022 Argent Software
All rights reserved



Historical Graph Reports are automatically generated for the saved event performance data. For example, you can view historical metrics for Successful or Failed Logon Attempts.

The screenshot displays the ARGENT OMEGA interface (v2.2.2202.8). The top navigation bar includes Home, Theme, help.Argent.com, Argent Instant help, and Logout. The main content area is titled "NODE_000010" and shows a "Past 24 Hours" view. On the left, a "Select Data Store" dropdown is set to "DS_DEMO", and a tree view lists various system components, with "Windows Logon -- Successful Logon Attempts/Minute" (instance: Interactive) selected. The main panel features a "Historical Average" graph showing "Successful Logon Attempts/Minute (Interactive)" over time, with a peak of 2. The bottom status bar indicates "Copyright © 2022 Argent Software. All Rights Reserved" and "Admin User: administrator".

Copyright 2022 Argent Software
All rights reserved



SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected Logon events. For example, you can trigger an alert if five consecutive authentication failures are followed by a successful authentication of the same account within a 60-minute time frame.

ARGENT OMEGA (v2.2.2202.8)

Home Theme help.Argent.com Argent Instant help Logout

- Administration
 - Generator Settings
 - Argent Omega
 - Argent Alert Mechanism
 - Argent Forecaster
 - Argent SIEM-Complete
 - SIEM Policy
 - Active Directory Authentication
 - Active Directory Objects
 - Brutal Force Attack
 - PL_BRUTAL_FORCE_ATTACK_AD**
 - PL_BRUTAL_FORCE_ATTACK_AZURE
 - PL_BRUTAL_FORCE_ATTACK_INTERACTIVE
 - PL_BRUTAL_FORCE_ATTACK_LINUX
 - File Deletion
 - Hacker Alert
 - Windows Logon
 - Archive Repository
 - License
 - Network Scan
 - Security
 - Event Logs
 - Argent SuperMaps
 - Topology Maps
 - Locations

SIEM-Complete Logic: Brutal Force Attack Of Domain Controller Authentication [Configure](#)

Fire Notification If 5 Consecutive User Authentication Failures Followed By A Successful Authentication Of The Same Account. All Logon Attempts Should Happen Within 60 Minutes

Alert: System Alarm Alert ALARM_DEMO

Temporarily Disabled:

Skip Log Records Over: 24 Hours

Archive Repository: {default}

Monitoring Groups: *

Schedule Time: 00:00:00 Repeat Task

Repetition Interval: 10

Repetition Unit: Minutes

Repeat Task Until: 23:59:59

Calendar: CAL_ALL_DAYS

Trace Level: Normal

Save Performance Data To the Argent Forecaster Using Data Store: {default}

Tag 1:

Tag 2:

Tag 3:

Post Event Even If the Same Event Is Still Outstanding (Unanswered)

Do So Only After Hour Minute Since Event Is Post

Copyright © 2022 Argent Software. All Rights Reserved Admin User: administrator

Copyright 2022 Argent Software
All rights reserved



The logic for Logon Failure Count and Time Limit is configurable.

The screenshot displays the ARGENT OMEGA (v2.2.2202.8) interface. The left sidebar shows a navigation tree with categories like Administration, Generator Settings, and SIEM-Complete. The main area shows the configuration for a SIEM-Complete Logic rule named 'Brutal Force Attack Of Domain Controller Authentication'. A 'Configure Selected Policy' dialog box is open, showing a table with the following data:

Name	Value
Logon Failure Count	5
Time Limit (Minutes)	60

The dialog box also includes 'OK' and 'Cancel' buttons. The background configuration shows various settings like Alert, Temporarily Disabled, Skip Log Records Over, Archive Repository, Monitoring Groups, Schedule Time, Repetition Interval, Repetition Unit, Repeat Task Until, Calendar, and Trace Level.

Copyright 2022 Argent Software
All rights reserved



SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected File Operation events. For example, you can trigger an alert if 10 file deletion operations per minute occur during specified hours.

The screenshot displays the ARGENT OMEGA (v2.2.2202.8) interface. The left sidebar shows a navigation tree with 'SIEM Policy' expanded to 'File Deletion', where 'PL_EXCESSIVE_FILE_DELETION' is selected. The main panel shows the configuration for this policy:

- SIEM-Complete Logic:** File Operation
- Alert:** System Alarm Alert (ALARM_DEMO)
- Match Instance:** File Deleted
- Match Options:** Match Case, Match Whole Word, Match Regular Expression (all unchecked).
- Fire Notification If File Operations Exceed:**
 - Overall: 10 Per Minute
 - Work Hours: 0
 - Off-Hours: 0
 - Use Dynamic Threshold:
- Temporarily Disabled:**
- Skip Log Records Over:** 24 Hours
- Archive Repository:** (default)
- Monitoring Groups:** *
- Schedule Time:** 00:00:00 Repeat Task
- Repetition Interval:** 10

Copyright © 2022 Argent Software. All Rights Reserved. Admin User: administrator

Copyright 2022 Argent Software
All rights reserved



SIEM Policy definitions can trigger alerts based on Non-Owner Account logon attempts to critical machines.

The screenshot displays the ARGENT OMEGA (v2.2.2202.8) interface. The left sidebar shows a navigation tree with 'SIEM Policy' expanded to 'PL_LOGON_TO_CRITICAL_ASSETS'. The main panel shows the configuration for the 'SIEM-Complete Logic' policy:

- SIEM-Complete Logic:** Suspicious Logon to Critical Machines
- Alert:** System Alarm Alert (ALARM_DEMO)
- Temporarily Disabled:**
- Skip Log Records Over:** 24 Hours
- Archive Repository:** (default)
- Monitoring Groups:** *
- Schedule Time:** 00:00:00 Repeat Task
- Repetition Interval:** 10
- Repetition Unit:** Minutes
- Repeat Task Until:** 23:59:59
- Calendar:** CAL_ALL_DAYS
- Trace Level:** Normal
- Save Performance Data To the Argent Forecaster Using Data Store: (default)
- Tag 1:
- Tag 2:
- Tag 3:
- Post Event Even If the Same Event Is Still Outstanding (Unanswered)
- Do So Only After 1 Hour 0 Minute Since Event Is Post

Copyright © 2022 Argent Software. All Rights Reserved. Admin User: administrator

Copyright 2022 Argent Software
All rights reserved



Owner accounts are easily defined for monitored servers in the CMDB-X. Alerts will be triggered for any other unauthorized accounts attempting to logon to the server.

ARGENT OMEGA (v2.2.2202.8) Home Theme help.Argent.com Argent Instant help Logout

Name	Server/Device	Network Group	Scan Network	Properties			
Network Group/Machine	Type	Alias	Licensed	Suspend	Location	Group/Key	Value
First Network Group	Network Group				MELBOURNE	Monitoring Level	Normal
NODE_000001	Microsoft Windows Server 2016 Standard		Yes		MELBOURNE	Tier	Not Specified
NODE_000002	Microsoft Windows Server 2016 Standard		Yes		MELBOURNE	Tag	
NODE_000003	Microsoft Windows Server 2016 Standard		Yes		MELBOURNE	Location	MELBOURNE
NODE_000004	Microsoft Windows Server 2016 Standard		Yes		MELBOURNE	Contact	
NODE_000005	Microsoft Windows Server 2016 Standard		Yes		MELBOURNE	Owner Accounts	Domain Name\Admin Name
NODE_000006	Microsoft Windows Server 2016 Standard		Yes		MELBOURNE	Default Settings	
NODE_000007	Microsoft Windows Server 2016 Standard		Yes		MELBOURNE	Time Zone Settings	Same as Location
NODE_000008	Microsoft Windows Server 2016 Standard		Yes		MELBOURNE	Critical	No
NODE_000009	Microsoft Windows Server 2016 Standard		Yes		MELBOURNE	Ignored	No
NODE_000010	Microsoft Windows Server 2016 Standard		Yes		MELBOURNE	Logical Dependency	
WIN2016-TEST	Windows Server		Yes		MELBOURNE	Installed Applications	
						Extended Properties	
						Description	

Display Options Refresh

Group/Key	Value
Show Objects	All
Network Group	*
Monitoring Group	*
Type	*

Copyright © 2022 Argent Software. All Rights Reserved Admin User: administrator

Copyright 2022 Argent Software
All rights reserved



SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected events to look for Ransomware attacks. For example, you can trigger an alert if a process starts followed by more than 10 file modifications by the same process within 30 minutes.

ARGENT OMEGA (v2.2.2202.8)

Home Theme help.Argent.com Argent Instant help Logout

- Administration
 - Generator Settings
 - Argent Omega
 - Argent Alert Mechanism
 - Argent Forecaster
 - Argent SIEM-Complete
 - SIEM Policy
 - Active Directory Authentication
 - Active Directory Objects
 - Brutal Force Attack
 - File Deletion
 - Hacker Alert
 - PL_RANSOMWARE_ATTACK**
 - PL_SHORT_LIVED_ACCOUNT
 - PL_SUSPICIOUS_SQL_BACKUP
 - Windows Logon
 - Archive Repository
 - License
 - Network Scan
 - Security
 - Event Logs
 - Argent SuperMaps
 - Topology Maps
 - Locations
 - Contacts
 - Argent Reporter

SIEM-Complete Logic: Ransomware Attack Configure

Fire Notification If A Process Starts Followed By More Than 10 File Modifications By The Same Process. All Operations Should Happen Within 30 Minutes

Alert: System Alarm Alert ALARM_DEMO

Temporarily Disabled:

Skip Log Records Over: 24 Hours

Archive Repository: { default }

Monitoring Groups: *

Schedule Time: 00:00:00 Repeat Task

Repetition Interval: 10

Repetition Unit: Minutes

Repeat Task Until: 23:59:59

Calendar: CAL_ALL_DAYS

Trace Level: Normal

Save Performance Data To the Argent Forecaster Using Data Store: { default }

Tag 1:

Tag 2:

Tag 3:

Post Event Even If the Same Event Is Still Outstanding (Unanswered)

Do So Only After 1 Hour 0 Minute Since Event Is Post

Copyright © 2022 Argent Software. All Rights Reserved Admin User: administrator



SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected events to look for frequent Domain Policy Changes. For example, you can trigger an alert if domain policies have been changed more than 10 times within 30 minutes.

The screenshot displays the Argent Omega configuration interface. The top navigation bar includes the Argent Omega logo (v2.2.2202.8) and links for Home, Theme, help.Argent.com, Argent Instant help, and Logout. The left sidebar shows a tree view of configuration categories, with 'SIEM Policy' expanded to show 'PL_DOMAIN_POLICY_CHANGES' selected. The main content area shows the configuration for 'SIEM-Complete Logic' with the following settings:

- SIEM-Complete Logic:** Frequent Domain Policy Changes (with a 'Configure' button)
- Alert:** System Alarm Alert (ALARM_DEMO)
- Temporarily Disabled:**
- Skip Log Records Over:** 24 Hours
- Archive Repository:** { default }
- Monitoring Groups:** *
- Schedule Time:** 00:00:00 (with 'Repeat Task' checked)
- Repetition Interval:** 10
- Repetition Unit:** Minutes
- Repeat Task Until:** 23:59:59
- Calendar:** CAL_ALL_DAYS
- Trace Level:** Normal
- Save Performance Data To the Argent Forecaster Using Data Store:** { default }
- Tag 1:** []
- Tag 2:** []
- Tag 3:** []
- Post Event Even If the Same Event Is Still Outstanding (Unanswered):**
- Do So Only After:** 1 Hour 0 Minute Since Event Is Post

Copyright © 2022 Argent Software. All Rights Reserved. Admin User: administrator

Copyright 2022 Argent Software
All rights reserved



SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected events to look for Audit Policy Changes. For example, you can trigger an alert if more than 10 audit policy changes have occurred within 30 minutes.

ARGENT OMEGA (v2.2.2202.8)

Home Theme help.Argent.com Argent Instant help Logout

Administration

- Generator Settings
 - Argent Omega
 - Argent Alert Mechanism
 - Argent Forecaster
 - Argent SIEM-Complete
 - SIEM Policy
 - Active Directory Authentication
 - Active Directory Objects
 - PL AUDIT POLICY CHANGES**
 - PL DOMAIN POLICY CHANGES
 - Brutal Force Attack
 - File Deletion
 - Hacker Alert
 - Windows Logon
 - Archive Repository
 - License
 - Network Scan
 - Security
 - Event Logs
 - Argent SuperMaps
 - Topology Maps
 - Locations
 - Contacts
 - Argent Reporter

SIEM-Complete Logic: Frequent Audit Policy Changes [Configure](#)

Fire Notification If Audit Policies Have Been Changed More Than 10 Times Within 30 Minutes

Alert: System Alarm Alert ALARM_DEMO

Temporarily Disabled:

Skip Log Records Over: 24 Hours

Archive Repository: { default }

Monitoring Groups: *

Schedule Time: 00:00:00 Repeat Task

Repetition Interval: 10

Repetition Unit: Minutes

Repeat Task Until: 23:59:59

Calendar: CAL_ALL_DAYS

Trace Level: Normal

Save Performance Data To the Argent Forecaster Using Data Store: { default }

Tag 1:

Tag 2:

Tag 3:

Post Event Even If the Same Event Is Still Outstanding (Unanswered)

Do So Only After 1 Hour 0 Minute Since Event Is Post

Copyright © 2022 Argent Software. All Rights Reserved Admin User: administrator

Copyright 2022 Argent Software
All rights reserved



SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected events to look for Short Lived Accounts. For example, you can trigger an alert if an account was created and deleted within 30 minutes.

The screenshot displays the ARGENT OMEGA (v2.2.2202.8) interface. The left navigation pane shows the 'SIEM Policy' section expanded to 'PL_SHORT_LIVED_ACCOUNT'. The main configuration area is titled 'SIEM-Complete Logic' and includes the following settings:

- SIEM-Complete Logic:** Short Lived Account (with a 'Configure' button)
- Alert:** System Alarm Alert (with a dropdown menu showing 'ALARM_DEMO')
- Temporarily Disabled:**
- Skip Log Records Over:** 24 Hours
- Archive Repository:** (default)
- Monitoring Groups:** *
- Schedule Time:** 00:00:00 (with a checked 'Repeat Task' option)
- Repetition Interval:** 10
- Repetition Unit:** Minutes
- Repeat Task Until:** 23:59:59
- Calendar:** CAL_ALL_DAYS
- Trace Level:** Normal
- Save Performance Data To the Argent Forecaster Using Data Store: (default)
- Tag 1:
- Tag 2:
- Tag 3:
- Post Event Even If the Same Event Is Still Outstanding (Unanswered)
- Do So Only After 1 Hour 0 Minute Since Event Is Post

Copyright © 2022 Argent Software. All Rights Reserved. Admin User: administrator



SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected events to look for an excessive number of failed authentication attempts within a specified timeframe. This is often an indicator of a hacking attempt.

The screenshot displays the ARGENT OMEGA (v2.2.2202.8) web interface. The left sidebar shows a navigation tree with 'SIEM Policy' expanded to 'Active Directory Authentication' and 'PL_AD_AUTH_FAILURE' selected. The main content area is titled 'SIEM-Complete Logic' and is outlined in red. It contains the following configuration options:

- SIEM-Complete Logic:** Active Directory Authentication Failure
- Alert:** System Alarm Alert (ALARM_DEMO)
- Fire Notification If Successfully Logon Exceed:**
 - Overall:** 0 Attempts/Minute
 - Work Hours:** 0
 - Off-Hours:** 0
 - Use Dynamic Threshold:**
- Temporarily Disabled:**
- Skip Log Records Over:** 24 Hours
- Archive Repository:** {default}
- Monitoring Groups:** *
- Schedule Time:** 00:00:00 Repeat Task
- Repetition Interval:** 10
- Repetition Unit:** Minutes
- Repeat Task Until:** 23:59:59
- Calendar:** CAL_ALL_DAYS
- Trace Level:** Normal
- Save Performance Data To the Argent Forecaster Using Data Store: {default}
- Tag 1:** []

Copyright © 2022 Argent Software. All Rights Reserved. Admin User: administrator



SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected events to look for suspicious SQL backup activity. For example, you can trigger an alert if an unscheduled SQL backup has occurred during a specified time frame.

The screenshot displays the ARGENT OMEGA (v2.2.2202.8) configuration interface. The left sidebar shows a navigation tree with 'SIEM Policy' expanded to 'PL_SUSPICIOUS_SQL_BACKUP'. The main panel shows the configuration for this policy:

- SIEM-Complete Logic:** Suspicious SQL Backup Activity (with a 'Configure' button)
- Alert:** System Alarm Alert (ALARM_DEMO)
- Temporarily Disabled:**
- Skip Log Records Over:** 24 Hours
- Archive Repository:** (default)
- Monitoring Groups:** *
- Schedule Time:** 00:00:00 (with 'Repeat Task' checked)
- Repetition Interval:** 10 Minutes
- Repetition Unit:** Minutes
- Repeat Task Until:** 23:59:59
- Calendar:** Please Choose
- Trace Level:** Normal
- Save Performance Data To the Argent Forecaster Using Data Store: (default)
- Tag 1:
- Tag 2:
- Tag 3:
- Post Event Even If the Same Event Is Still Outstanding (Unanswered)
- Do So Only After 1 Hours 0 Minutes Since Event Is Post

Copyright © 2022 Argent Software. All Rights Reserved. Admin User: administrator