Argent SIEM-Complete

Key Facilities

ARGENT

This Argent White Paper summarizes the key facilities Argent's apt-named **SIEM-Complete** product, a part of the new Argent Omega family of cloud-oriented products.

SIEM technology aggregates logs, security alerts, and events into a centralized database to provide real-time analysis for security monitoring.

Compliance data is always voluminous – a very small school in Australia archives 200 GB of SIEM data per month -- planning the required capacities is the essential first step for all SIEM.

Argent SIEM-Complete has 3 basic functions:

- **Archive** data in Archive Repositories
- **Analyze** data to create reports on trends and performance
- **Alert** on security breaches

Argent SIEM-Complete uses the following facilities:

Archive Repository

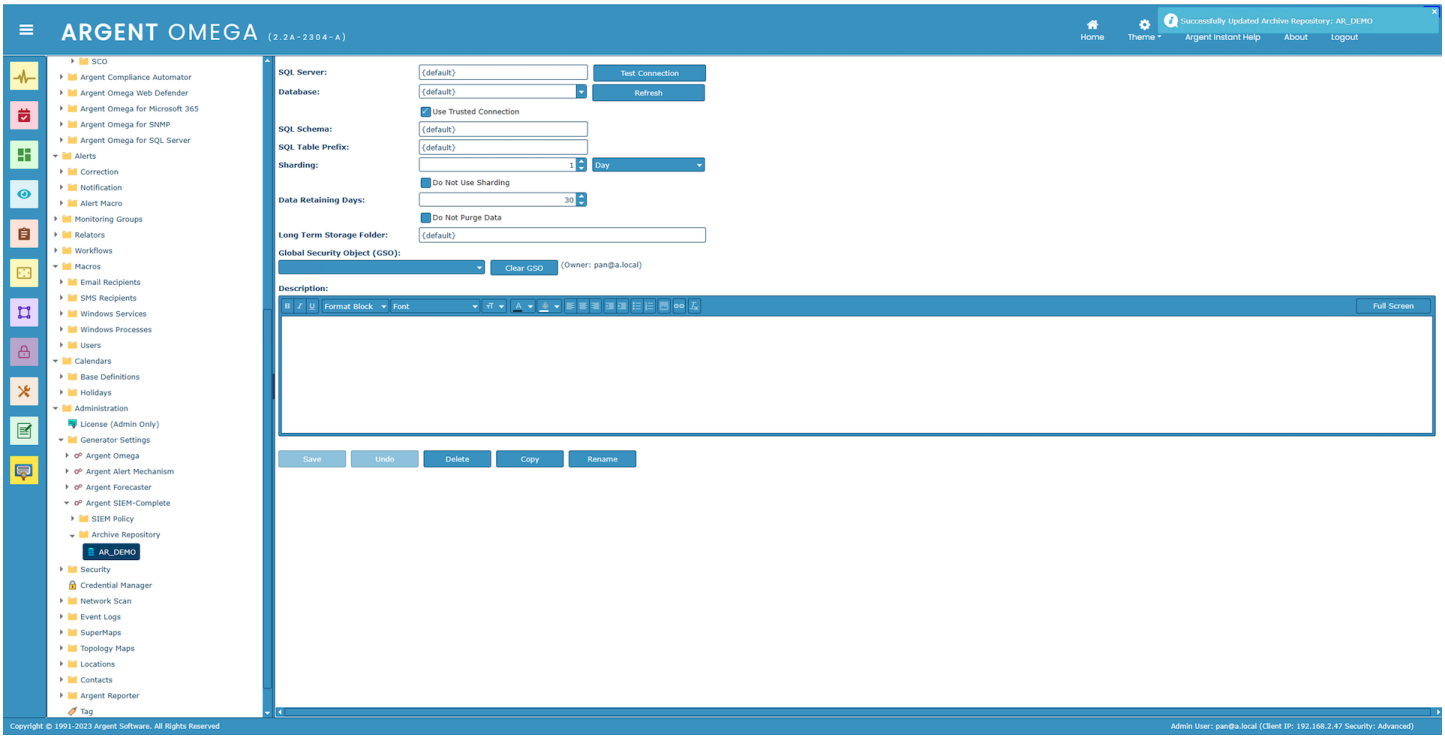
When the default Archive Repository is used, archive data is saved in the Argent Omega database with default table names. For example, the logon activities are saved in the "ARGSOFT_COMPLIANCE_AUDIT_LOGON_LOGOFF" SQL table.

There are 18 Compliance SQL Tables for each dataset.

- ARGSOFT_COMPLIANCE_AUDIT_ACCOUNT_MANAGEMENT
- ARGSOFT_COMPLIANCE_AUDIT_COMPUTER_MANAGEMENT
- ARGSOFT_COMPLIANCE_AUDIT_DS_OBJECT
- ARGSOFT_COMPLIANCE_AUDIT_FILE_SYSTEM
- ARGSOFT_COMPLIANCE_AUDIT_GROUP_MANAGEMENT
- ARGSOFT_COMPLIANCE_AUDIT_HOST_SESSION
- ARGSOFT_COMPLIANCE_AUDIT_INSTALLED_HOTFIX
- ARGSOFT_COMPLIANCE_AUDIT_INSTALLED_MSI
- ARGSOFT_COMPLIANCE_AUDIT_KERBEROS_AUTH

- ARGSOFT_COMPLIANCE_AUDIT_LOGON_LOGOFF
- ARGSOFT_COMPLIANCE_AUDIT_NPS_OPERATION
- ARGSOFT_COMPLIANCE_AUDIT_POLICY_CHANGE
- ARGSOFT_COMPLIANCE_AUDIT_PROCESS_EVENT
- ARGSOFT_COMPLIANCE_AUDIT_SHARE
- ARGSOFT_COMPLIANCE_AUDIT_SHARE_DACL
- ARGSOFT_COMPLIANCE_AUDIT_SYSTEM_EVENT
- ARGSOFT_COMPLIANCE_AUDIT_TASK_EVENT
- ARGSOFT_COMPLIANCE_LOG_ARCHIVE

“ARGSOFT_COMPLIANCE_” is the default SQL Table prefix. It can be changed using Archive Repository.



Argent Compliance Automator Rules use the Archive Repository.

Compliance data can also be saved into:

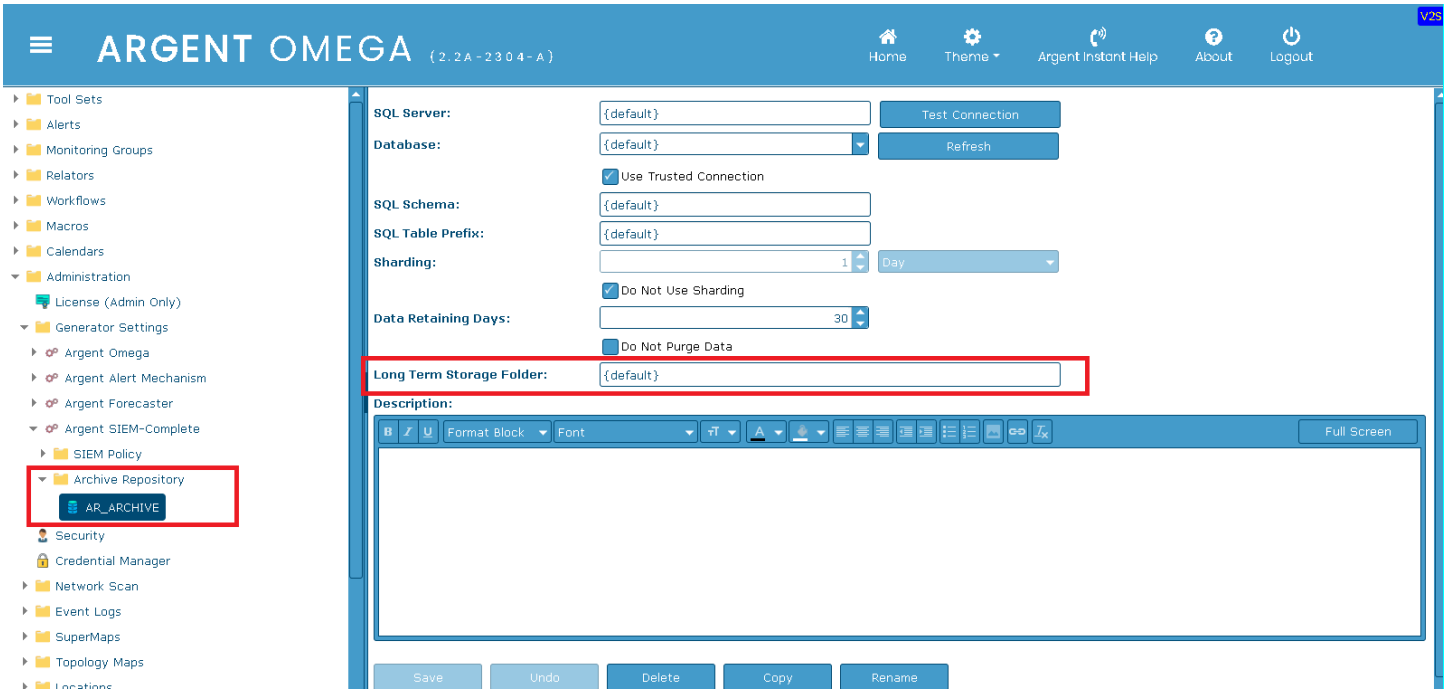
- Different databases
- Datasets with different SQL schema or SQL Table prefix
- Different shards based on date time

(In general, the word “shard” refers to a sliver of glass, as when a window is hit with a sledgehammer; in the language of computer databases, it means spreading a single massive dataset over multiple sub-databases on different servers, often located in different countries.)

Archive Repository can also define the Data Retention Policy -- data older than a certain number of days will be purged from the database.

Another useful feature is the **“Long Term Storage Folder.”** All Work Orders for saving Compliance data will be moved to this folder; when an Argent Compliance Automator Rule executes a Log Rule against a monitored server, it first stores the result of the collected log message as a Work Order file in the x:\Argent\ArgentOmega\ARCHIVE_DATA directory for processing, at which point the log message data is then saved to the Argent SQL database and the Work Order file is deleted.

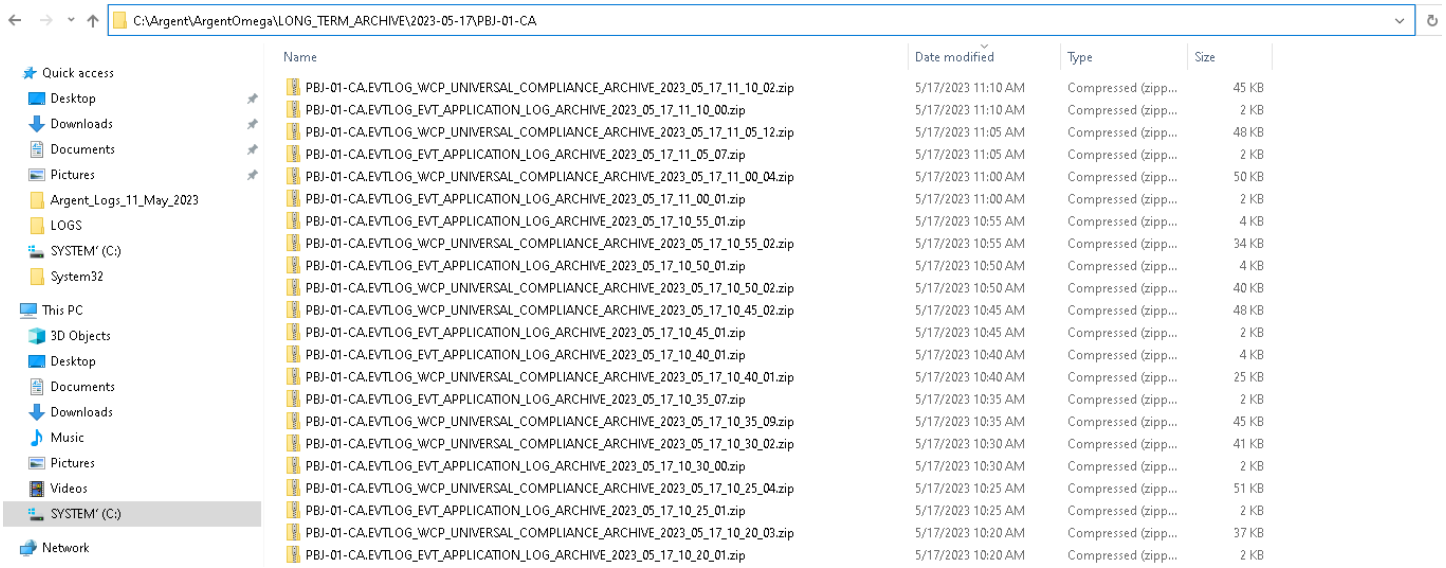
There is an option to retain these Work Order files under “**Long Term Storage Folder**” as a secondary log event stored outside the SQL database; see screenshot below.



When this option is used, the Work Order files are not deleted after saving the log data into the SQL database, but rather they are saved to the directory specified by **"Long Term Storage Folder"**; the data is initially duplicated.

This feature retains a copy of the log after the SQL database has been purged. For example, if the SQL purge rate for a specific cohort of log data is 180 days, then for the first 180 days the log data will be duplicated; after 180 days the copy in the SQL database will be deleted, but the flat-file Work Order copy will remain.

By default, this is located in the x:\Argent\ArgentOmega\LONG_TERM_ARCHIVE folder.



Opening one of the Work Order files will show the details of the saved log data.

If the log data in the SQL database has been automatically purged (such as the 180-day example described above), it is possible to **re-add** the log data to the Argent SQL database by copying it from the archived Work Order files.

A scenario where this is useful is if a customer has an audit requirement to retain 5 years of collected log data, but keeps the SQL database purge rate at 180 days; the friendly external auditors arrive – unannounced – one morning for a snap inspection. The auditors request log files from July three years ago, not currently in the SQL database, but present in the **Long Term Storage Folder** directory; this feature allows you to easily and quickly restore the requested data to the SQL database and generate the required reports.

The retention policy for the folder is controlled externally. For example, you can use inexpensive AWS S3 storage and keep the data for decades.

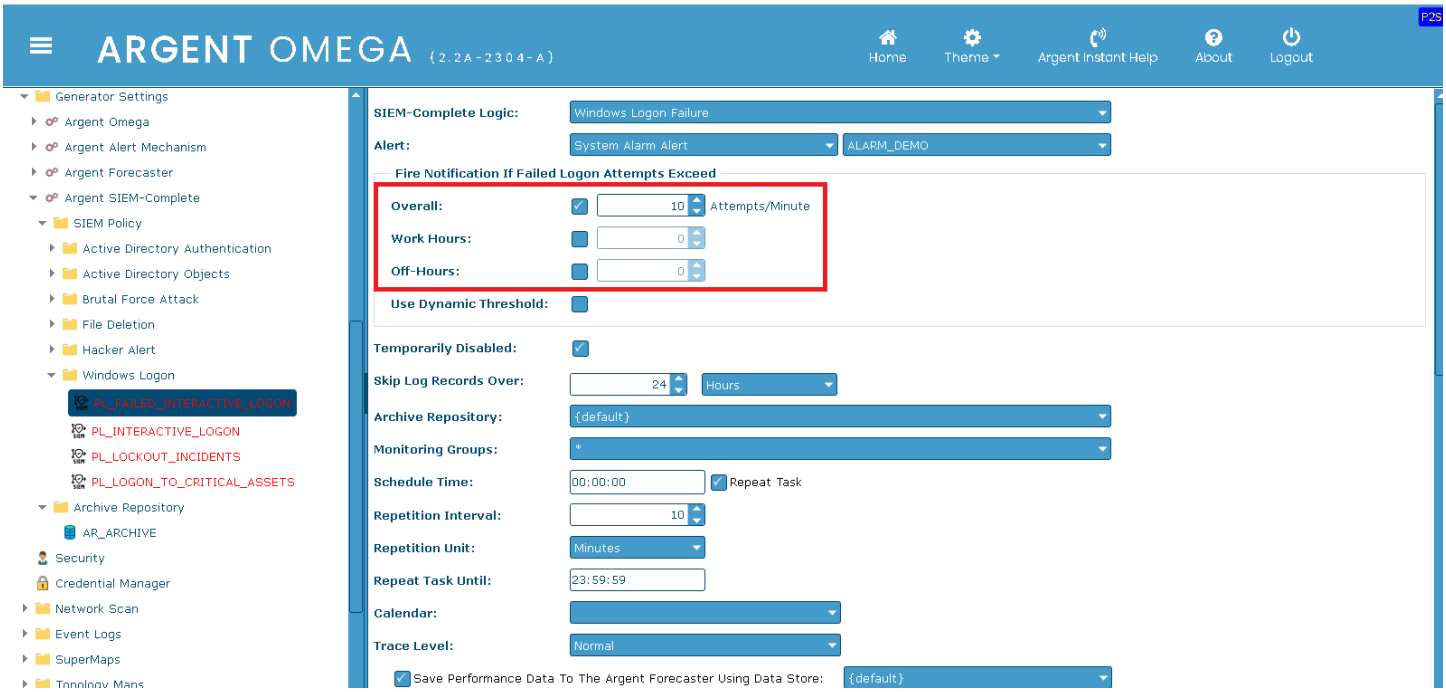
As mentioned with the small school in Australia, ***"planning the required capacities is the essential first step for all SIEM."*** Argent provides a wide range of options to best suit the customer's needs for the particular cohort of data; it is completely fine to use only the SQL Server data base for all data BUT after five years, the small school's SQL database would have ballooned to 12,000 gigabytes...

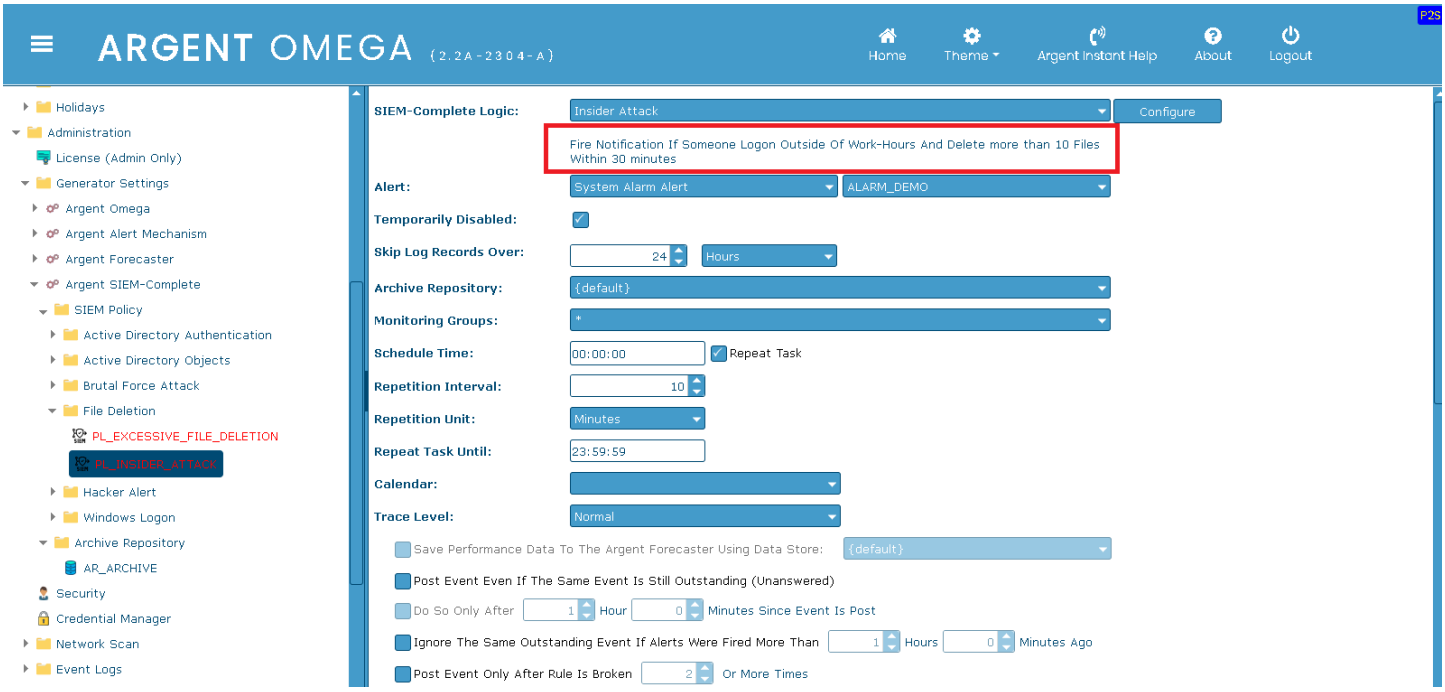
Work Hours and Off-Hours

The importance of security events can be very different between Work Hours and Off-Hours -- most security events are generated from user activity such as logons, logoffs, accessing files, etc., and **most of these events normally occur during normal work hours – typically 9 to 5** -- when employees are logging into the network.

So a flurry of these types of events happening outside normal working hours might be abnormal or suspicious.

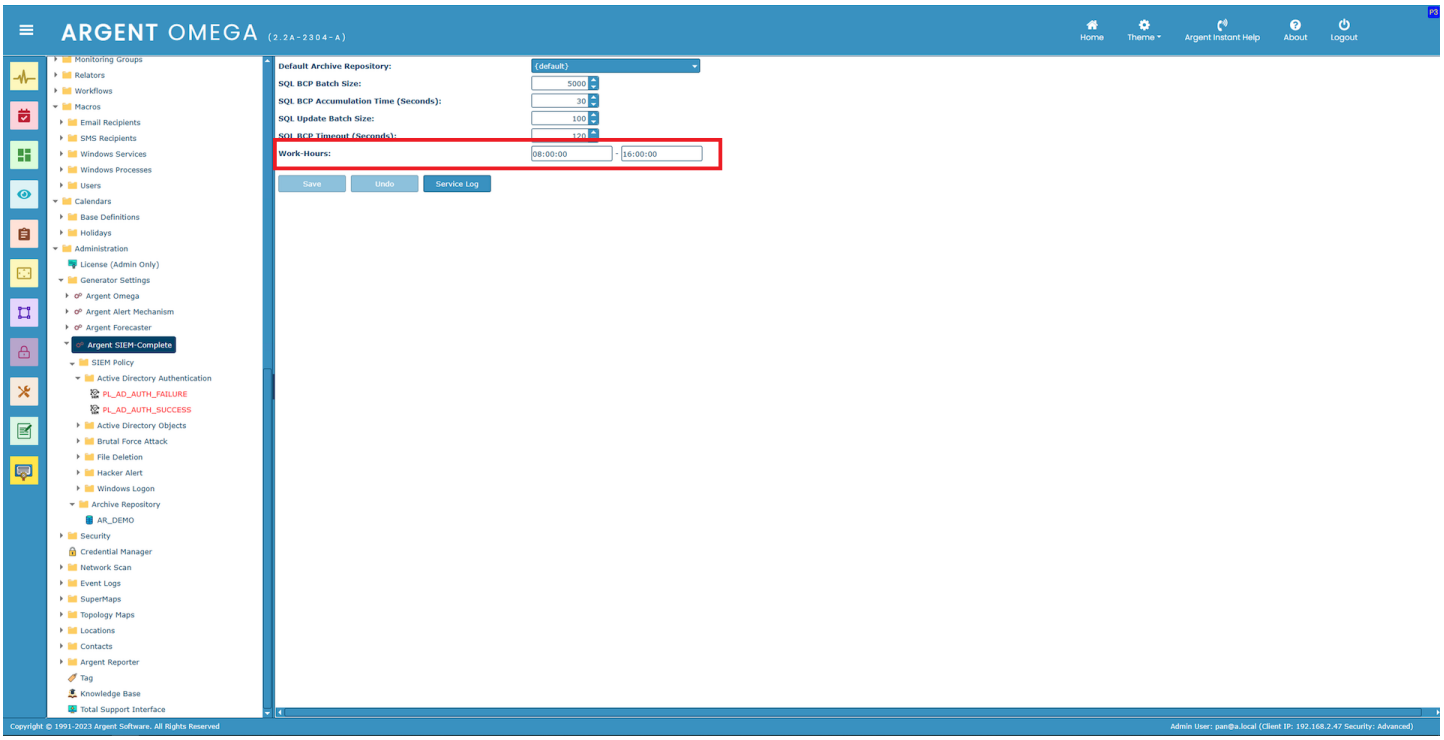
A number of the SIEM Policy Rules use logic that examines activity during “Work Hours” and “Off-Hours.”





These Rules will use the “Work Hours” times that are configured in the Argent SIEM-Complete Generator screen to specify “Work Hours” and “Off-Hours” parameters.

User-defined Work Hours and Off-Hours in Argent SIEM-Complete Generator screen.


ARGENT OMEGA (2.2A-2304-A)
Home
Theme
Argent Instant Help
About
Logout
Monitoring Groups
Relators
Workflows
Macros
Email Recipients
SMS Recipients
Windows Services
Windows Processes
Users
Calendars
Base Definitions
Holidays
Administration
License (Admin Only)
Generator Settings
Argent Omega
Argent Alert Mechanism
Argent Forecaster
Argent SIEM-Complete
SIEM Policy
Active Directory Authentication
PL_AD_AUTH_FAILURE
PL_AD_AUTH_SUCCESS
Active Directory Objects
Brutal Force Attack
File Deletion
Hacker Alert
Windows Logon
Archive Repository
AR_DEMO
Security
Credential Manager
Network Scan
Event Logs
SuperMaps
Topology Maps
Locations
Contacts
Argent Reporter
Tag
Knowledge Base
Total Support Interface
Default Archive Repository:
{default}
SQL BCP Batch Size:
5000
SQL BCP Accumulation Time (Seconds):
30
SQL Update Batch Size:
100
SQL BCP Timeout (Seconds):
120
Work-Hours:
08:00:00
16:00:00
Save
Undo
Service Log
Copyright © 1991-2023 Argent Software. All Rights Reserved
Admin User: pan@a.local (Client IP: 192.168.2.47 Security: Advanced)

SIEM Policy

At the center of Argent SIEM-Complete is a set of policies.

Depending on the query result, Argent Forecaster data is generated and saved; any number of Security Alerts can be raised based on customer-specified thresholds.

Argent SIEM-Complete has 17 built-in Policies:

Successful Windows Logon

This policy saves logon activity into Argent Forecaster for real-time display and trend analysis.

Windows Logon Failure

This policy detects machine console logon failure or remote logon to the machine; it also saves logon failure metrics to Argent Forecaster for real-time display and trend analysis.

Successful Active Directory Authentication

This policy saves Active Directory logon activity into Argent Forecaster for real-time display and trend analysis.

Active Directory Authentication Failure

This policy detects domain logon failure events.

File Operation

Instances include:

- Failed to Access
- File Read
- File Attributes Changed
- File Modified
- File Deleted
- File Created
- File Renamed

Two of the common scenarios are:

- **Someone deletes a large number of files within a specified period of time during Off-Work hours (the parameters are configurable by the user). Hacker?**
- **Someone repeatedly deletes a large number of files. User mistake?**

Brute Force Attack Of Interactive Logon On Windows Machines

Repeated logon attempts to the same account within y minutes.

This is likely a hacker trying passwords.

Brute Force Attack Of Domain Controller Authentication

Same as above but for Domain Controllers.

Brute Force Attack Of Logon On Linux Server

Same as above but for Linux/UNIX servers.

Brute Force Attack Of Microsoft 365 Logon

Same as above but for Azure Accounts.

Ransomware Attack

This policy alerts if any process changes more than x files within y minutes.

Insider Attack

This policy alerts if someone logs on outside of work hours **and** deletes more than x files within y minutes.

Suspicious SQL Backup Activity

This policy alerts if unscheduled SQL backup is found outside of allowed time.

Suspicious Logon to Critical Machines

This policy alerts if other than a machine's owner attempts to logon to a critical machine.

Short-Lived Account

This policy alerts if an account was created and deleted within y minutes.

Account Lockout Incidents

This policy alerts if an account is locked, which is usually caused by consecutive failed logon attempts.

Frequent Domain Policy Changes

This policy alerts if domain policies have been changed more than x times within y minutes.

Frequent Audit Policy Changes

This policy alerts if audit policies have been changed more than x times within y minutes.

When a customer needs new policies, these can be created at no cost by Argent.

Data Visualizer

What happens when a user needs to see a trend that is not included in the built-in Policy?

The Argent Data Visualizer comes to the rescue.

The Argent Data Visualizer can analyze any archived compliance data by applying custom filters.

Data is displayed as a table as well as various graphs.