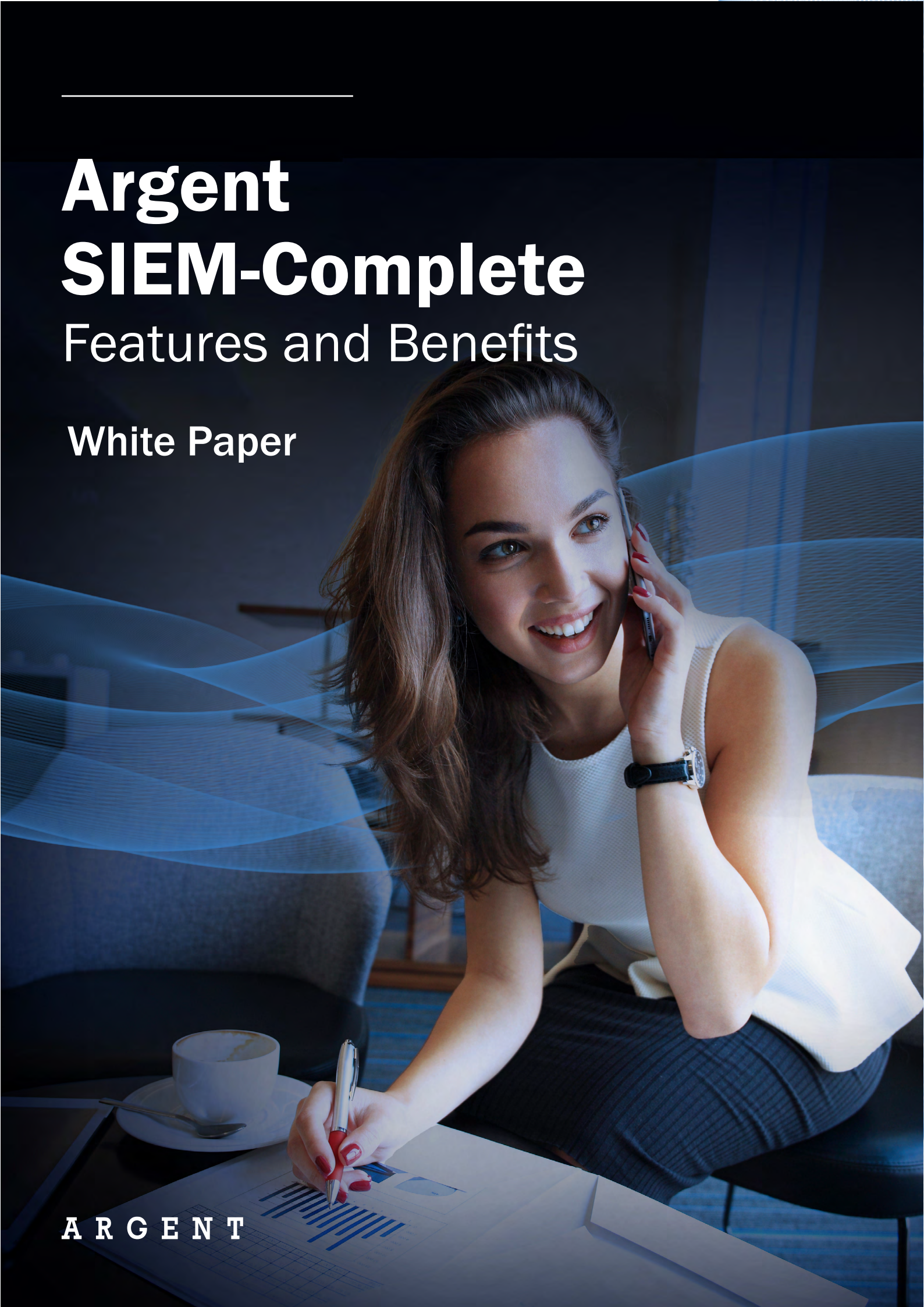
Argent SIEM-Complete

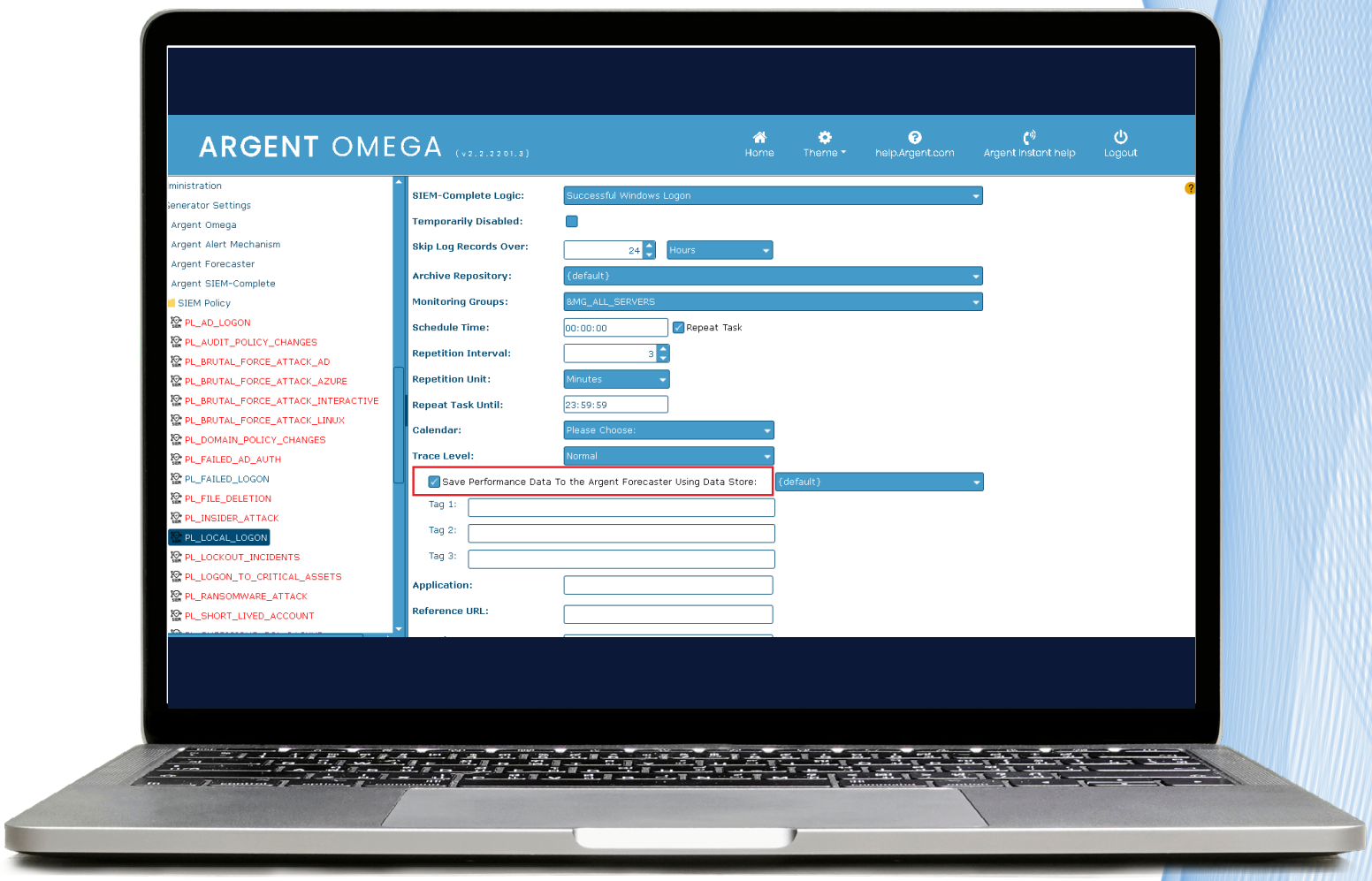
Features and Benefits

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.



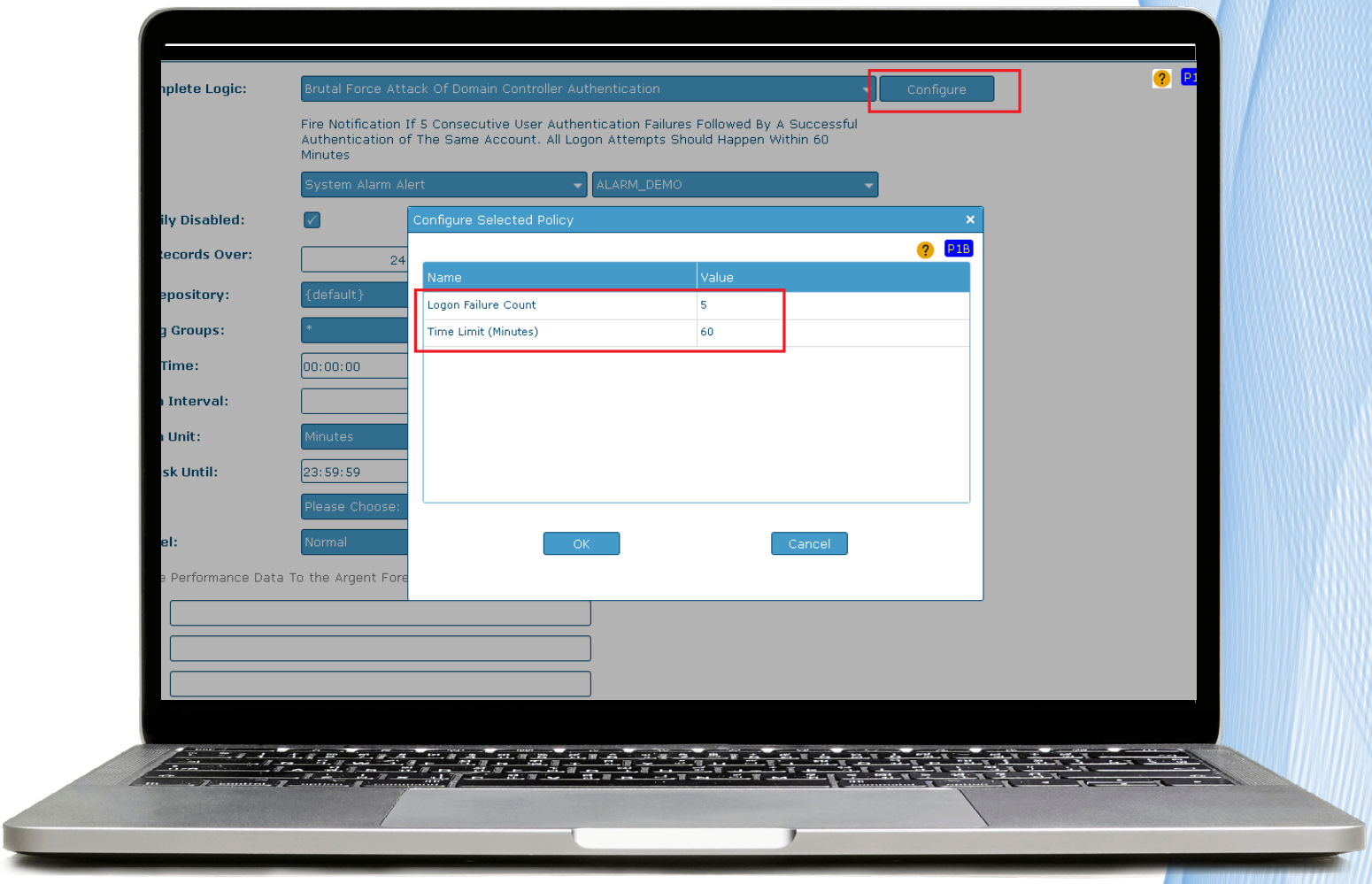
Historical Graph Reports are automatically generated for the saved event performance data.

For example, you can view historical metrics for Successful or Failed Logon Attempts.

SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected Logon events.

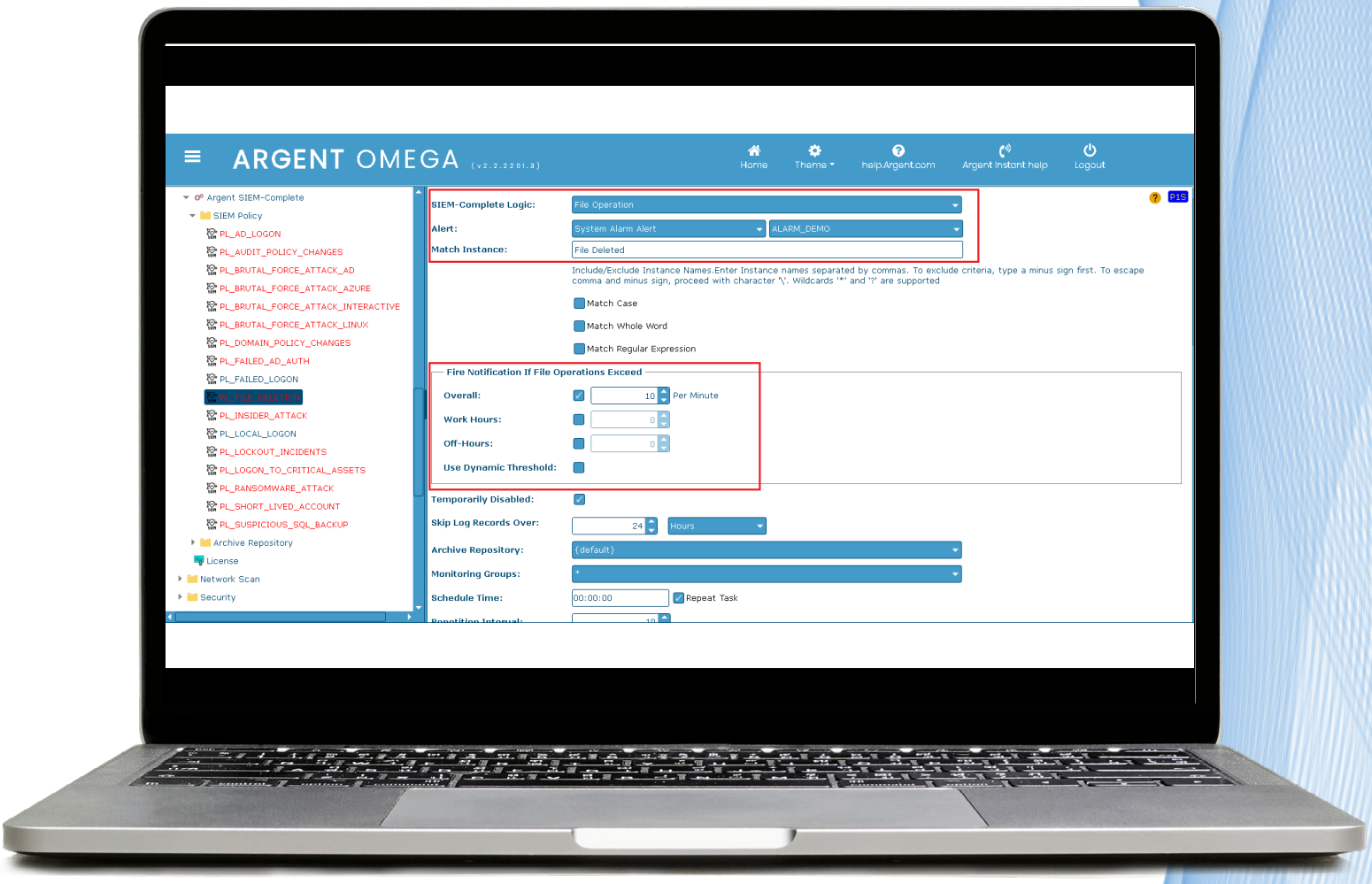
For example, you can trigger an alert if five consecutive authentication failures are followed by a successful authentication of the same account within a 60-minute time frame.

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

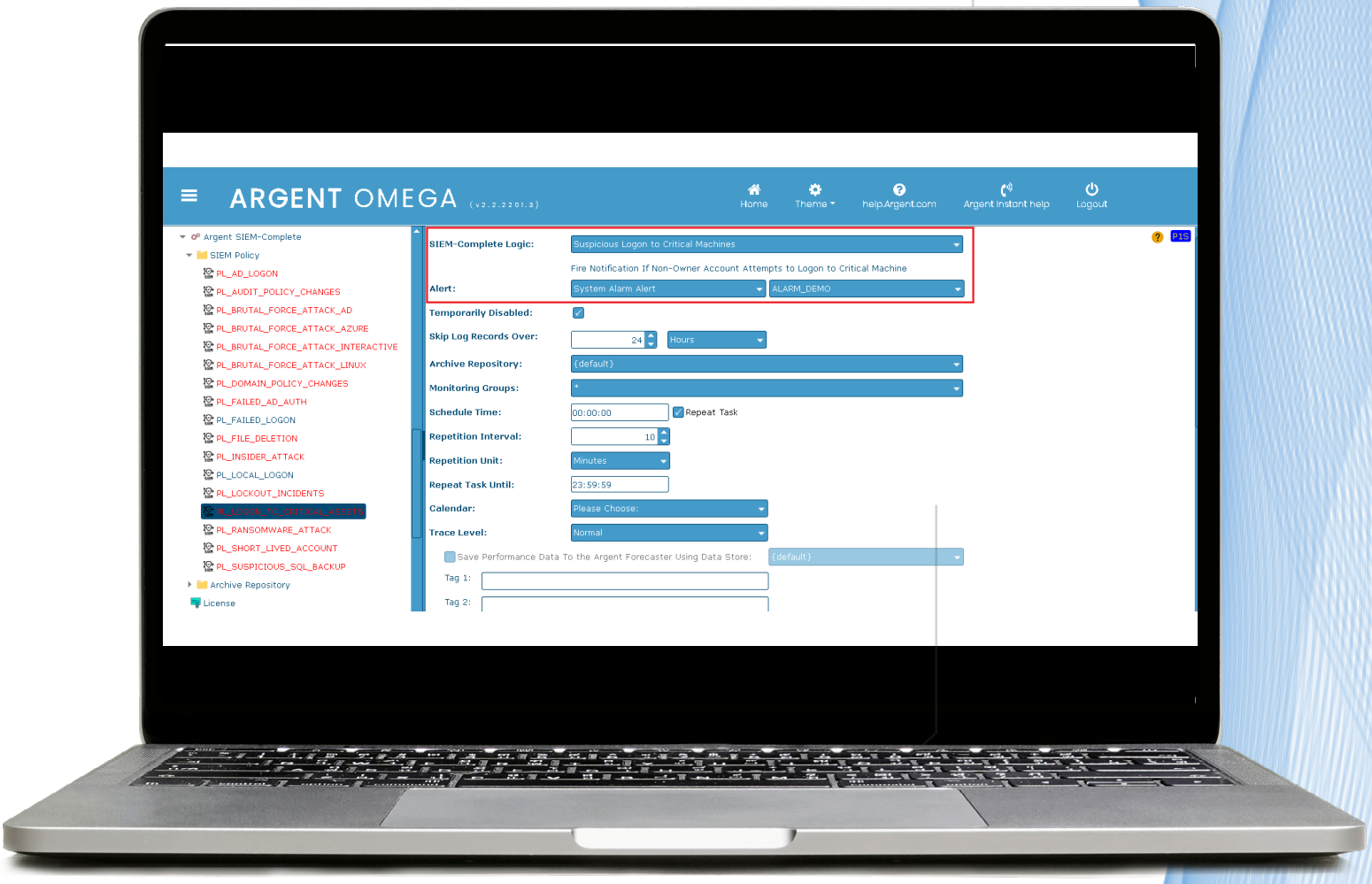


SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected File Operation events.

For example, you can trigger an alert if 10 file deletion operations per minute occur during specified hours.

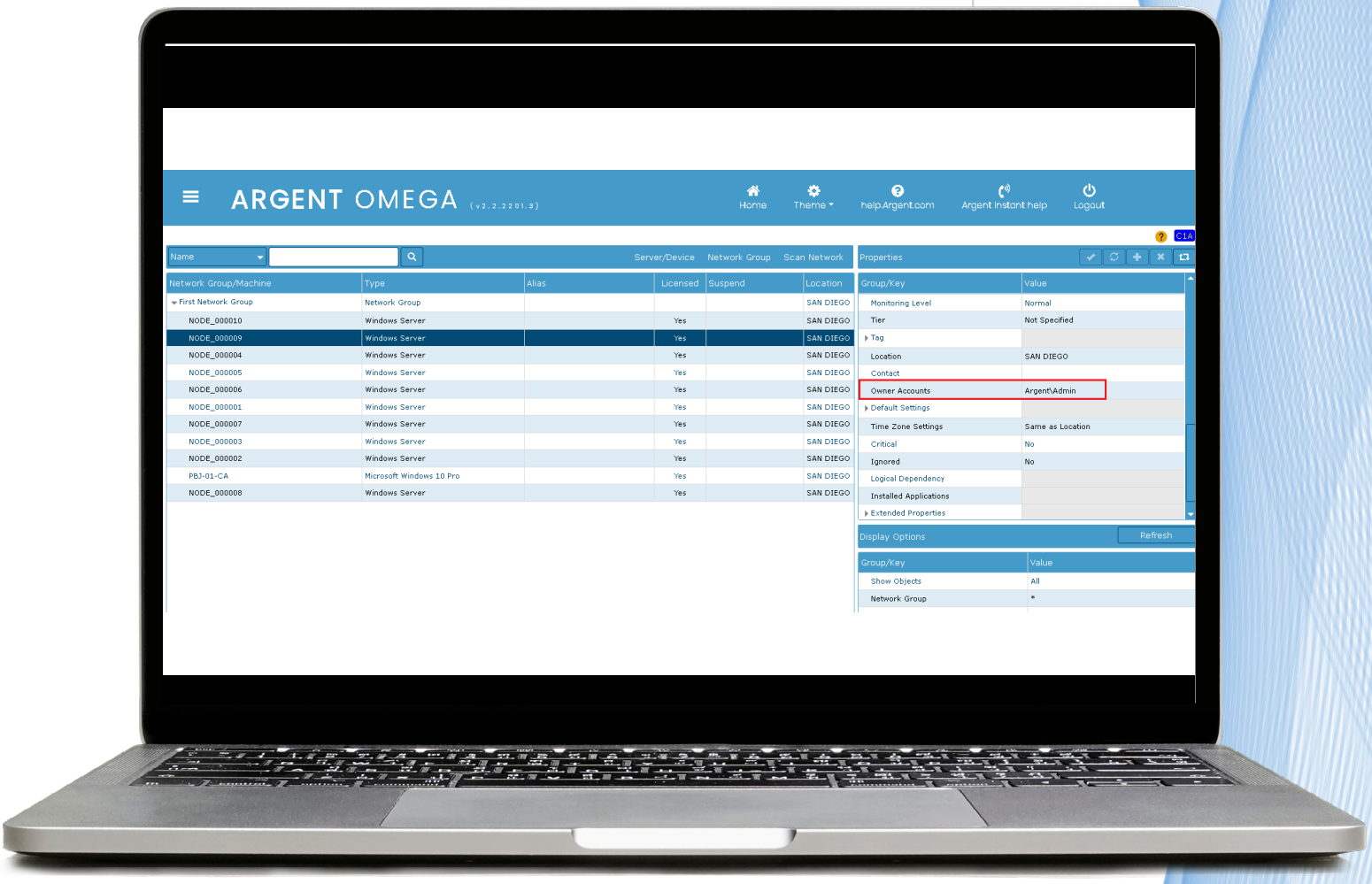


SIEM Policy definitions can trigger alerts based on Non-Owner Account logon attempts to critical machines.



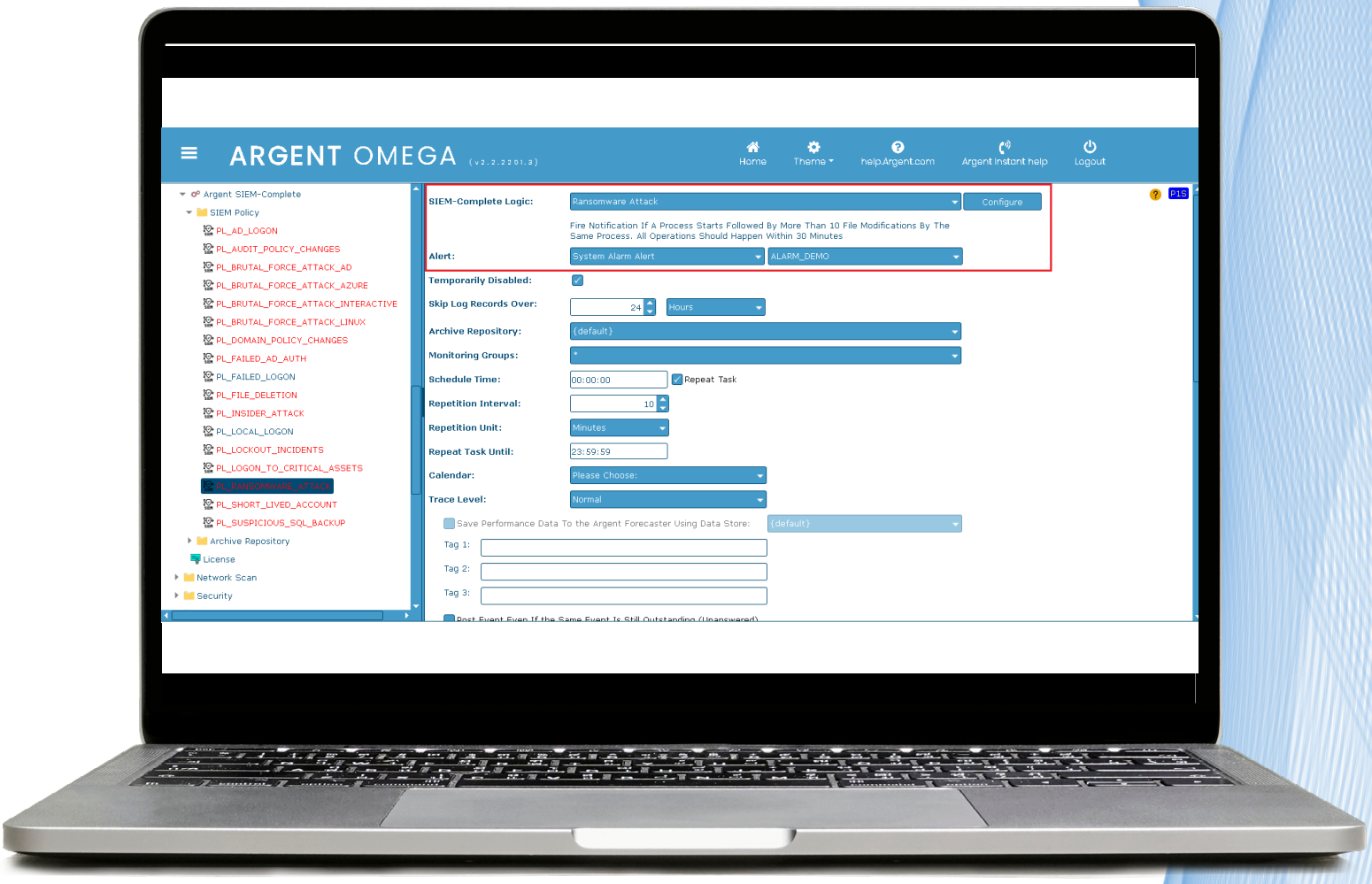
Owner accounts are easily defined for monitored servers in the CMDB-X.

Alerts will be triggered for any other unauthorized accounts attempting to logon to the server.



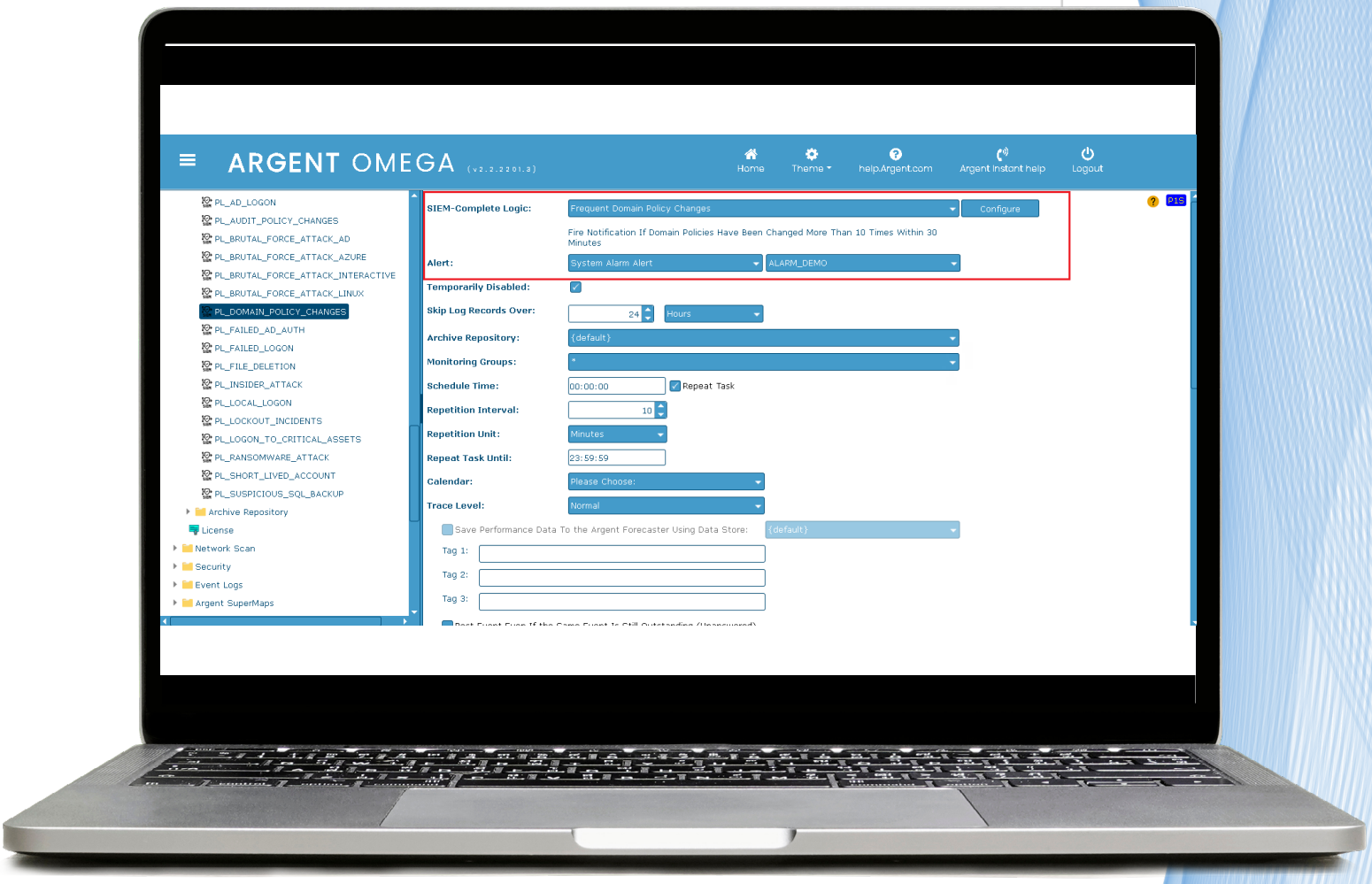
SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected events to look for Ransomware attacks.

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.



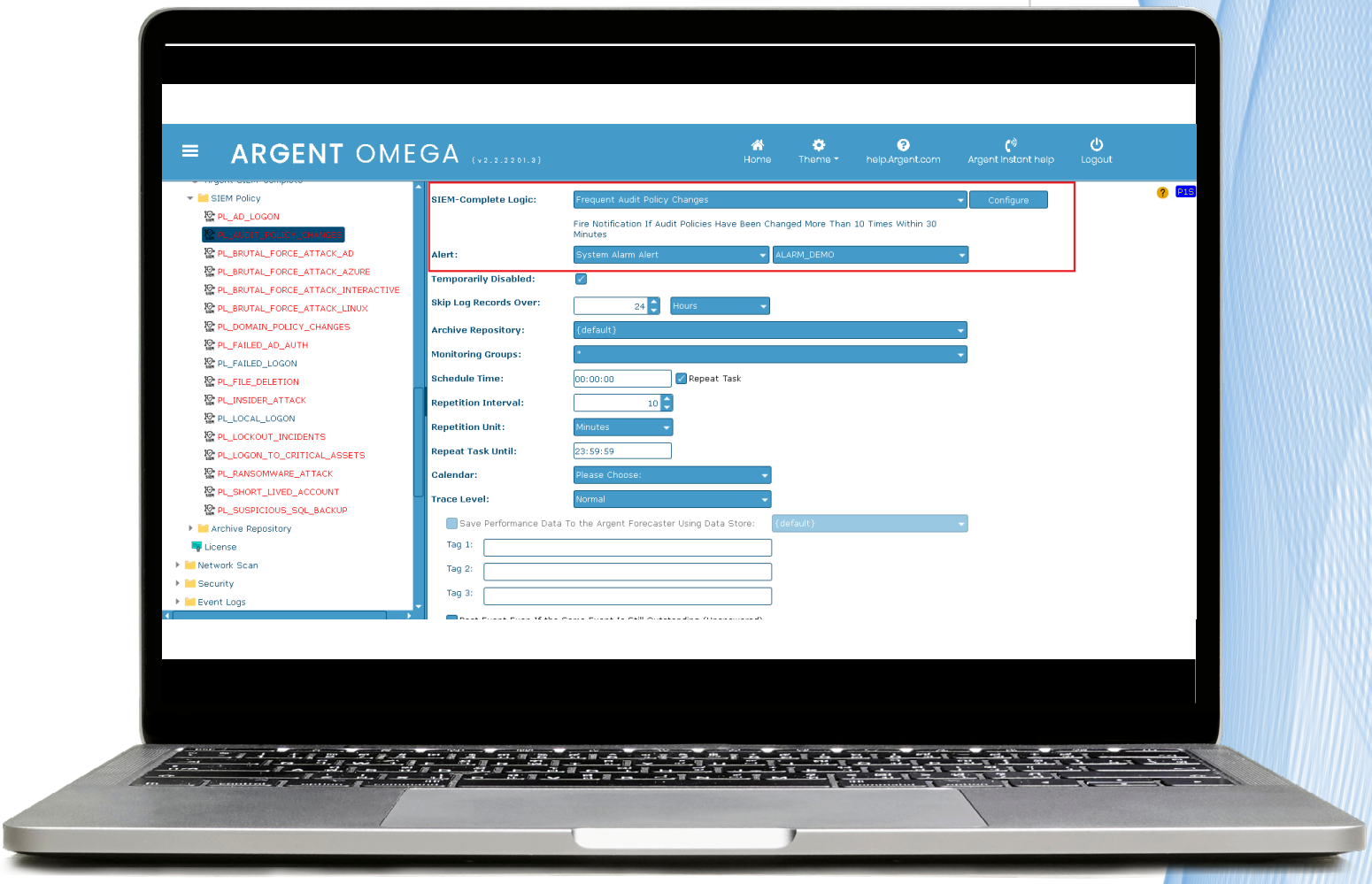
SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected events to look for frequent Domain Policy Changes.

For example, you can trigger an alert if domain policies have been changed more than 10 times within 30 minutes.



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.

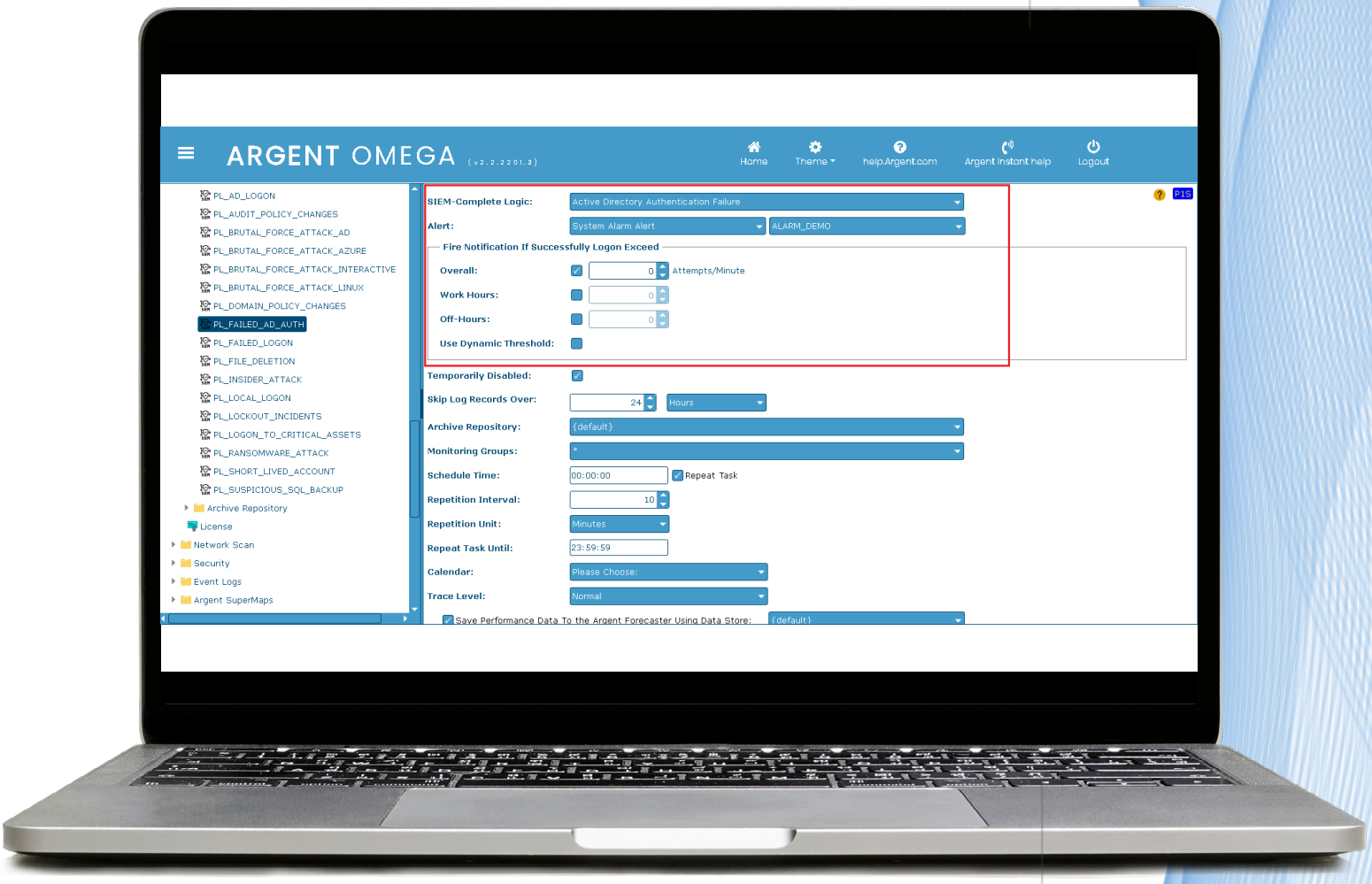


SIEM Policy definitions can trigger alerts based on customer-defined logic parsed from collected events to look for Short Lived Accounts.

For example, you can trigger an alert if an account was created and deleted within 30 minutes.

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.



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.