



Engage. Explore. Empower.
Connecting Visionaries in Radiation Safety, Science and Industry

MIRION
Connect **24**
Annual Users' Conference

July 29 - August 2 | Omni Dallas Hotel, Dallas, TX



MIRION
TECHNOLOGIES

SIEM and NMS Configuration and Administration

Ben Ranayhossaini P.E.

Manager – System Architecture

Mirion Connect | Annual Users' Conference 2024

Dallas, Texas

Ben Ranayhossaini P.E.

Manager, System Architecture, Secure Integrated Solutions

- B.S. in Electrical Engineering, Penn State University
- M.S. in Electrical Engineering, University of Pittsburgh
- Registered Professional Engineer, TX - PE-136350, OH - PE-82892
- CompTIA A+ - COMP001002734935
- Nuclear Power Tenure +16 years
 - Westinghouse Electric Company – Class Non-1E - Ovation Distributed Control and Information Systems (10 yrs)
 - Mirion - Secure Integrated Solutions – Nuclear Security (6 yrs)

- Sites Visited / Worked

- International

- Koeberg Nuclear Power Plant, Capetown South Africa, - Ovation Plant Computer Upgrade
- Beznau Nuclear Power Station, Dottengen Switzerland, - Ovation Plant Computer Upgrade
- Barakah Nuclear Power Plant, U.A.E., - APR 1400 Non-Safety Ovation Digital I&C, and Cyber Security
- Shin Kori 3 & 4, APR 1400 Non-Safety Ovation Digital I&C

- US

- Vogtle 3&4, AIM SCS Project & Units 1 - 4 Transition/Cutover
- J.A. Fitzpatrick, AIM SCS Project & Site Transition/Cutover
- Riverbend, AIM SCS Project & Transition/Cutover
- North Anna, AIM SCS Project & Backend Site Transition Support
- Oconee Nuclear Station, AIM SCS Site Transition Support
- Catawba Nuclear Station, AIM SCS Site Support
- Davis Besse Nuclear Power Station, Site PSCS Walkdown
- Palisades Nuclear Generating Station, Site PSCS Walkdown
- Comanche Peak Nuclear Power Plant, Site PSCS Walkdown

Agenda

- SIEM Configuration and Administration
 - SIEM Overview
 - SIEM Configuration
 - SIEM Administration
- NMS Configuration and Administration
 - NMS Overview
 - WhatsUp Gold Configuration
 - WhatsUp Gold Administration
- SIEM and NMS Dataflow
- Final Exam
- Questions

SIEM Configuration and Administration



- The Security Information and Event Manager (SIEM) is a device that provides real-time analysis of security alerts generated by network hardware and applications. Often used on several Nuclear systems to satisfy NEI 08-09 controls for centralized logging of events on systems.
 - Mirion SIS currently uses Trellix SIEM as the solution on AIM SCS systems (projected to be going to Splunk in 2025)
 - Trellix SIEM architecture consists of an Enterprise Log Manager (ELM) and Enterprise Security Manager (ESM)
- The ELM logs and parses the data from various sources (Workstations, Servers, Switches, NIDS, Anti Virus) on an AIM SCS system.
 - Source → Datasource
 - Data → Syslogs, WMI, Databases
 - Parsing → Parses the data obtained
 - Log → Logs the parsed data
- The ESM aggregates and correlates the logs to identify security threats and alarm on these events.
- If a threat is detected, the ESM is configured to alarm on the security incident(s) so that a site may investigate and respond.
 - Alarms and Notification → SIEM Alarms, Notifications
 - Reporting → Weekly autogenerated reports, Incident response
- Alarms
 - Some are configured as local alarms on the SIEM
 - Some are automatically forwarded to AIM.

- Common SIEM Datasources on an AIM SCS System
 - Network Switches and Devices
 - Servers and Workstations (Running Windows, Linux, etc.)
 - Cyber Security Devices and Software Applications (NIDS, Firewalls (HW and SW), Endpoint Protection, etc.)

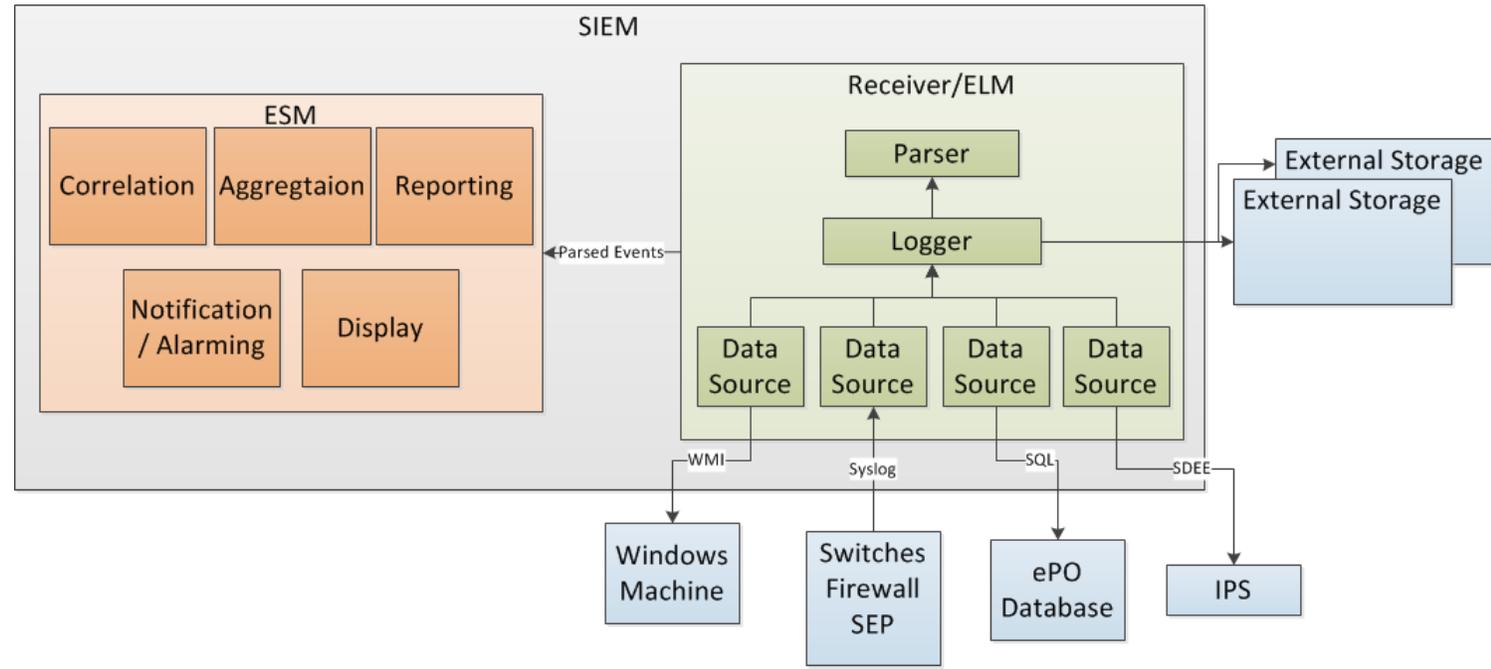
- Encoders
- Other SIEMs

▪ Datasources provide data to the SIEM by

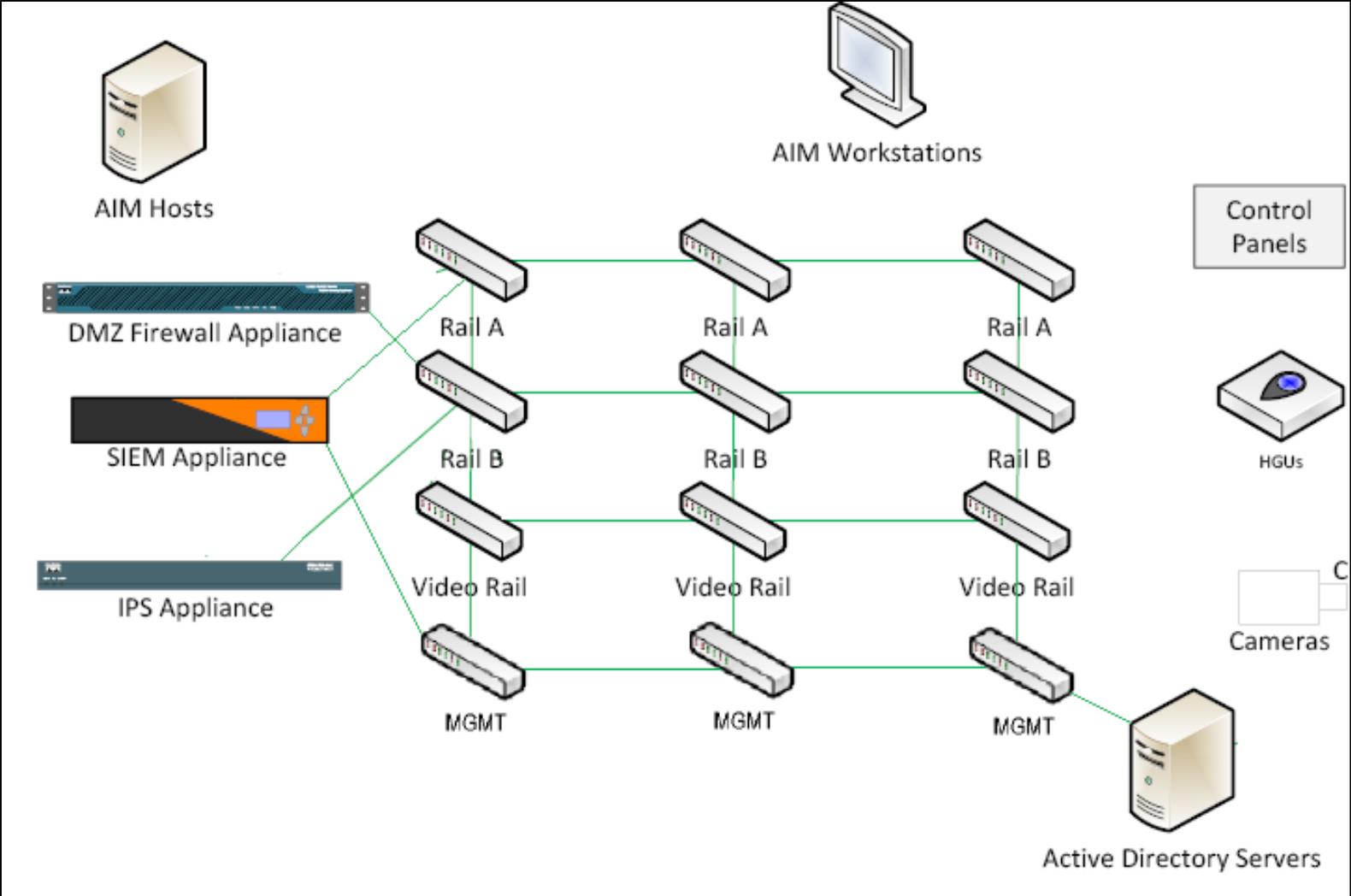
- RFC 5424 Syslog
- WMI (Windows Servers and Workstations)
- Databases (Trellix ePO, Trellix IPS)

▪ WMI and Database Log Collection Process

- Log retrieval occurs using credential based access
 - Access to the WMI on the machine
 - Access to Databases
- Permissions controlled by Group Policy
- Denied Local Logon



SIEM Overview – AIM SCS Architecture



The screenshot displays the ESX 11.3.2 20200730 interface. At the top, there are tabs for 'Configuration' and 'Normalized Dashboard'. The main area shows a list of 'Triggered Alarms' with columns for Alarm Name, Summary, Assignee, Severity, Trigger Date, Acknowledge Date, and Acknowledged By. A red box labeled 'Properties' points to the gear icon in the top left. A red box labeled 'Policy Editor' points to the refresh icon. A red box labeled 'Retrieve Events' points to the refresh icon. A red box labeled 'Data Sources' points to the left-hand navigation pane. A red box labeled 'Alarm Details' points to the details section for the selected alarm. A red box labeled 'Unacknowledged Alarms' points to the 'Alarms' list at the bottom left.

Alarm Name	Summary	Assignee	Severity	Trigger Date	Acknowledge Date	Acknowledged By
SIEM Critical St	Local Receiver-ELM status changed from Active to Critical	SIEM_Admin	75	07/13/2021 20:53:15		
Rogue System	Signature ID '1000-mcafee_rsd' (43-2299997294) match found	SIEM_Admin	75	07/13/2021 10:07:54		
SIEM Critical St	Local Receiver-ELM status changed from Active to Critical	SIEM_Admin	75	07/13/2021 02:06:32		
Rogue System	Signature ID '1000-mcafee_rsd' (43-2299997294) match found	SIEM_Admin	75	07/08/2021 18:30:39		
Rogue System	Signature ID '1000-mcafee_rsd' (43-2299997294) match found	SIEM_Admin	75	07/08/2021 09:37:01		
ALARM-REMOVE	Signature ID 'Disabled Task Scheduler task' (43-297001420) match found	aimscsadmin	100	07/07/2021 13:56:55	07/07/2021 14:18:19	aimscsadmin
Rogue System	Signature ID '1000-mcafee_rsd' (43-2299997294) match found	SIEM_Admin	75	07/07/2021 13:17:09		
Rogue System	Signature ID '1000-mcafee_rsd' (43-2299997294) match found	SIEM_Admin	75	07/02/2021 13:04:12		
Required Servi	Signature ID 'Service Startup Configuration Change' (43-5000014) match found	SIEM_Admin	75	07/02/2021 12:22:26		
Required Servi	Signature ID 'Service Startup Configuration Change' (43-5000014) match found	SIEM_Admin	75	07/02/2021 12:21:26		
SIEM Critical St	Local Receiver-ELM status changed from Active to Critical	SIEM_Admin	75	07/02/2021 08:17:17		
Rogue System	Signature ID '1000-mcafee_rsd' (43-2299997294) match found	SIEM_Admin	75	07/01/2021 12:45:00		

Alarm Details:
 Signature ID '1000-mcafee_rsd' (43-2299997294) match found
 Associated Indicator:
 Alarm Name: Rogue System(s) Detected | Trigger Date: 07/13/2021 10:07:54 | Escalation Date:
 Status: Unacknowledged | Acknowledge Date:
 Assignee: SIEM_Admin | Acknowledged By:
 Severity: 75 | Case: [Create Case](#)

Initial conditions assume a Trellix SIEM with the latest version of SIEM ESM is installed and ready to configure:

- Add Datasources to the SIEM
 - Syslog Datasources need to be configured to forward logs to SIEM.
 - WMI and Database Datasources need to have an account created with the service account credentials
- Configure Rule sets
 - Mirion SIS has a standard ruleset which is imported
 - Create custom rules for any custom datasources
- Import Dashboards and Reports
 - Mirion SIS has standard Dashboards and Reports which are imported
- Configure Alarming
 - Mirion SIS has standard SIEM Alarms and Templates configured
 - SIEM Alarms can either be locally reported on the SIEM or configured to send an alarm to AIM

Name	Clients	Type	Parsing	ELM
.Correlation Engine	0	Correlation I	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ADA	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ADB	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ADMINWS	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AMS	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CASAIM	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CASVID	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CLIP	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CYBERAPP	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
EPO Server	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HOSTA	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HOSTB	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
McAfee NSM Audit Logs	0	Network Set	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NAS01	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NAS02	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NVR1	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NVR2	0	Windows Ev	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Searching the ELM Logs (Enterprise Log Manager)

The screenshot displays the ELM search interface for 'Local ESM - McAfee ePO - McAfee ePO_ePO Audit Log (ePO)'. The search criteria are set to 'Current Day' and 'Enhanced ELM Search'. The search results show 57 entries (100%) from the 'McAfee ePO_ePO Audit Log (ePO)' data source.

Results Time Distribution: A bar chart showing the distribution of search results over time. The x-axis represents time intervals from 01:00 to 22:00 on 05/24/2019 and 00:00:00 to 00:00:00 on 05/25/2019. The y-axis represents the number of results, ranging from 0 to 4. The total number of results is 57 (100%).

Data Source Results: A summary panel showing 57 (100%) results from the 'McAfee ePO_ePO Audit Log (ePO)' data source.

Device Type Results: A summary panel showing 57 (100%) results from the 'ePO Audit Log (ePO)' device type.

Search Results Table:

Data Source	Insert Time	Text
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 00:09:18	AutoID="43961" ProductFamily="ORIONAUDITLOG" UserName="epo_admin" UserId="1" Priority="2" CmdName="LdapSync: Sync across users fr
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 00:09:18	AutoID="43962" ProductFamily="ORIONAUDITLOG" UserName="system" UserId="2" Priority="3" CmdName="Endpoint Security Firewall Property
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 00:24:21	AutoID="43963" ProductFamily="ORIONAUDITLOG" UserName="system" UserId="2" Priority="3" CmdName="Endpoint Security Firewall Property
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 00:44:24	AutoID="43964" ProductFamily="ORIONAUDITLOG" UserName="system" UserId="2" Priority="3" CmdName="Endpoint Security Firewall Property
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 00:54:26	AutoID="43965" ProductFamily="ORIONAUDITLOG" UserName="system" UserId="2" Priority="3" CmdName="Endpoint Security Firewall Property
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 01:09:29	AutoID="43966" ProductFamily="ORIONAUDITLOG" UserName="system" UserId="2" Priority="3" CmdName="Endpoint Security Firewall Property
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 01:29:33	AutoID="43967" ProductFamily="ORIONAUDITLOG" UserName="system" UserId="2" Priority="3" CmdName="Endpoint Security Firewall Property
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 01:44:35	AutoID="43968" ProductFamily="ORIONAUDITLOG" UserName="system" UserId="2" Priority="3" CmdName="Endpoint Security Firewall Property
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 01:54:36	AutoID="43969" ProductFamily="ORIONAUDITLOG" UserName="system" UserId="2" Priority="3" CmdName="Endpoint Security Firewall Property
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 02:09:39	AutoID="43970" ProductFamily="ORIONAUDITLOG" UserName="system" UserId="2" Priority="3" CmdName="Endpoint Security Firewall Property
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 02:29:42	AutoID="43971" ProductFamily="ORIONAUDITLOG" UserName="system" UserId="2" Priority="3" CmdName="Endpoint Security Firewall Property
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 02:44:44	AutoID="43972" ProductFamily="ORIONAUDITLOG" UserName="system" UserId="2" Priority="3" CmdName="Endpoint Security Firewall Property
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 02:44:44	AutoID="43973" ProductFamily="ORIONAUDITLOG" UserName="epo_admin" UserId="1" Priority="2" CmdName="Download Software Product List
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 02:44:44	AutoID="43974" ProductFamily="ORIONAUDITLOG" UserName="epo_admin" UserId="1" Priority="1" CmdName="Repository Pull" Success="0" S
McAfee ePO_ePO Audit Log (ePO)	05/24/2019 02:54:46	AutoID="43975" ProductFamily="ORIONAUDITLOG" UserName="system" UserId="3" Priority="3" CmdName="Endpoint Security Firewall Property

McAfee ESM 11.3.2 20200730

Configuration | Normalized Dashboard | Alarms Dashboard

Local ESM - Local Receiver-ELM - ADA

RTX - Account Modification Summary

All User Account Changes Events

Bound to Events 4 (100%)

A computer accou... 3

System Successful... 1

Event Distribution

Bound to Events 4 (100%)

2000 2004 2008 2012 2016 2020

12/31/1999 09/18/2021

20:00:00 14:00:00

Source User

Bound to Events 4 (100%)

ANONYMOUS L... 3

1

Destination User

Bound to Events 4 (100%)

ADA\$ 1

ADB\$ 1

HOSTA\$ 1

Others 1

Severity	Rule Message	Source IP	Device Name	Last Time	Event Subtype
25	A computer account wa:	192.168.100.100	ADA	09/10/2021 08:44:12	modify
25	A computer account wa:	192.168.100.100	ADA	09/07/2021 13:44:04	modify
25	System Successfully Ch	192.168.100.100	ADA	09/07/2021 13:44:04	informational
25	A computer account wa:	192.168.100.100	ADA	09/02/2021 14:33:53	modify

Details

First Time:

Source IP:

Source Port:

Source MAC:

Advanced Details

Last Time:

Dest. IP:

Dest. Port:

Dest. MAC:

Geolocation

Duration:

Protocol:

Event Subtype:

VLAN:

Description

Notes

Custom Types

Packet

Page 1

- SIS - Account Modification Summary
- SIS - Administrator Logon Summary
- SIS - Application Control Summary
- SIS - Audit Trail Modification Summary
- SIS - Backup Summary
- SIS - Critical Linux Events
- SIS - Failed Logon Summary
- SIS - Malware Exploit Summary
- SIS - Network Security Summary
- SIS - Policy Changes
- SIS - RADIUS Summary
- SIS - SIEM Alarm Summary
- SIS - USB Usage Summary

- Mirion Technologies' philosophy on alarms is to limit to two types:
 - Events that require immediate action by a cyber security incident response team
 - The system is under cyber attack
 - The cyber security posture of the system may be compromised/tampered with
 - Events to be brought to system administrators' attention but otherwise may be overlooked
 - Situations not monitored by AIM software
- Case Management
 - Cases can track investigation/incident response
 - Created automatically on alarms or manually

The screenshot shows the 'System Properties' dialog box with the 'Alarms Settings' tab selected. The left sidebar lists various system configuration categories. The main area contains a table of alarm conditions and their status, with a vertical scrollbar on the right. To the right of the table are buttons for 'Add', 'Edit', 'Remove', 'Copy', 'Import', and 'Export', along with a checked 'Enabled' checkbox. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Name	Condition	Status
Account Lockout	Internal Event Match	Enabled
Application Control Violation	Internal Event Match	Enabled
Backup Disk Space Not Available	Internal Event Match	Disabled
Correlation Event Severity	Specified Event Rate	Disabled
Device Failure	Device Failure	Disabled
Device Health	Device Status Change	Disabled
EPS Rate Exceeded	Specified Event Rate	Disabled
Failed Login Attempts	Internal Event Match	Disabled
File Screen Policy Violation	Internal Event Match	Enabled
Policy Change	Internal Event Match	Disabled
Possible Event Time Mismatch	Event Delta	Disabled
Required Service State Change	Internal Event Match	Enabled
Rogue System(s) Detected	Internal Event Match	Enabled
Rule Push Events	Internal Event Match	Disabled
Scheduled Task Created	Internal Event Match	Disabled
Scheduled Task Deleted	Internal Event Match	Disabled
Security Log Tampering	Internal Event Match	Enabled
SIEM Critical Status	Device Status Change	Enabled
Suspicious Network Activity	Internal Event Match	Enabled
System Log Tampering	Internal Event Match	Enabled
USB Violation	Internal Event Match	Enabled
USB Violation Detected	Internal Event Match	Enabled
User Added	Internal Event Match	Disabled
User Modified	Internal Event Match	Disabled

- Incident response/investigation best practices:
 - Start at SIEM
 - Drill down into data sources, events
 - Capture ELM logs (raw logs), store offline
 - Investigate at originating device if needed (e.g., at A/V manager)
 - Physical security and cyber security personnel working together!
 - Physical evidence may be needed
 - Who was sitting at the computer?
 - Badge records
 - AIM user logons
 - Alarm History (Cabinet Tamper Alarms)

Configuration X | Normalized Dashboard X | Incident Management X | Alarms Dashboard X

Physical Display

Cases Displaying 1 of 1 Rows

Search current table data

Case ID	Case Summary	Assignee	Case Severity	Organization	Status	Case Created
1	app control violation	SIEM_Admin	1	None	Open	09/02/2021 15:50:27

- What reports run?
- When do they run?
- Stored locally on SIEM or a file share.

The screenshot shows the 'System Properties' window with a sidebar on the left containing various system settings categories. The 'Reports' section is selected, displaying a table of reports and their configurations.

Name	Condition	Status
Weekly Administrative Access	Monday at 12:00 AM	Enabled
Weekly Anti-Virus Event Sum	Monday at 12:10 AM	Enabled
Weekly Network Change Sum	Monday at 12:20 AM	Enabled
Weekly NIDS Summary	Monday at 12:30 AM	Enabled
Weekly SIEM Alarm Summary	Monday at 12:40 AM	Enabled

Below the table, there are several action buttons:

- Disable**: Disable reporting. Reports are currently enabled.
- Conditions**: Manage report conditions
- Recipients**: Manage email addresses for report recipients
- View**: View currently running reports with the option to cancel them
- Files**: View generated report files

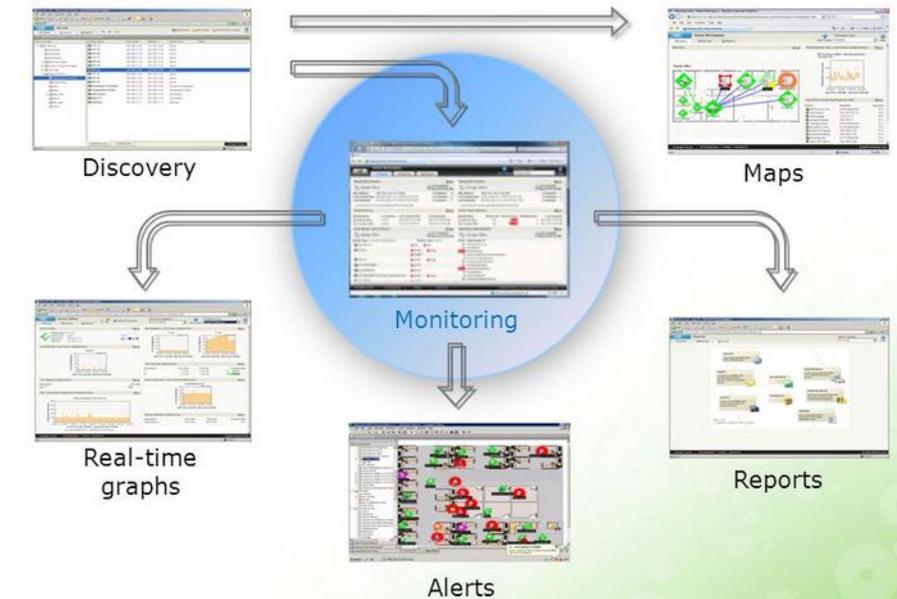
On the right side of the interface, there is a vertical toolbar with buttons: Add, Edit, Remove, Run Now, Share, Import, Export, and a checkbox labeled 'Enabled' which is checked.

NMS Configuration and Administration



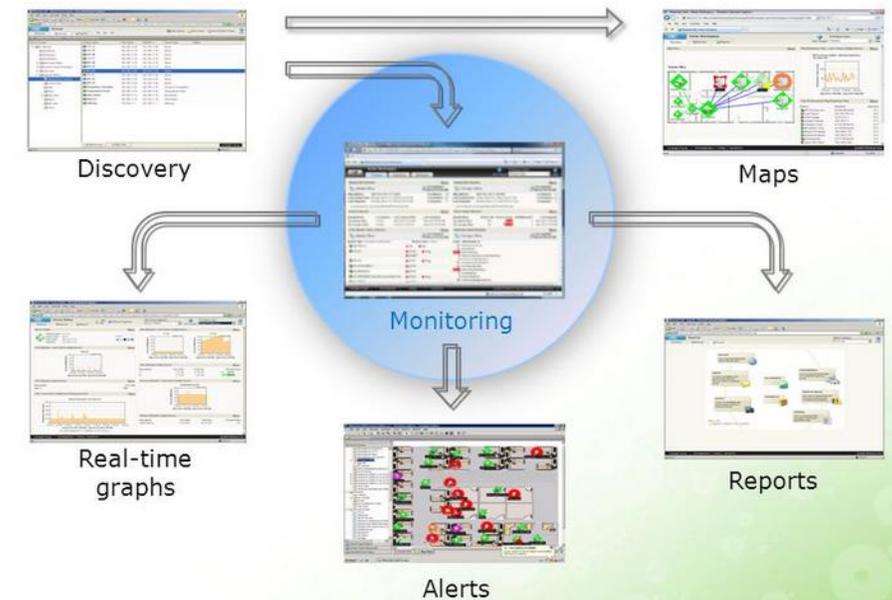
- The Network Management System (NMS) is a comprehensive network monitoring and management tool for optimizing and maintaining network infrastructure on a system.
 - Mirion SIS uses WhatsUp Gold as the NMS solution on AIM SCS systems.
- Using SNMP (Simple Network Management Protocol) and MIB (Management Information Base) the NMS interrogates network connected devices to obtain and monitor information of network attached devices including network status, hardware health and activity, and other performance indicators (disk space, memory utilization, processor utilization, network latency, and bandwidth utilization).
 - Interrogation → Polling
 - Monitoring Information → Active, Passive, and Performance monitors
- Depending on the returned value of the Active, Passive, or Performance monitors upon polling, the NMS is configured to take action by to sending a notification to AIM if an alarm threshold is met.
 - Active Monitors → Action Policies
 - Passive Monitors → SNMP trap messages
 - Performance Monitors → Mirion SIS configures a custom scheduled task and script to obtain the performance information from the WUG database and send an alarm to AIM.

Discover - Map - Monitor - Alert - Report



- Active Monitors
 - These monitors include hardware status (Boolean).
 - Switch Port Interfaces
 - Hard Drives
 - Fans
 - NIC → Ping and SNMP
 - Power Supplies
- Passive Monitors
 - These monitors include software status (Boolean)
 - Time Synchronization
 - OS Services
- Performance Monitors
 - These monitors include hardware status (Numeric)
 - CPU Utilization (frequency)
 - Memory Utilization (percentage)
 - Disk Utilization (percentage)
 - NIC Bandwidth (percentage)

Discover - Map - Monitor - Alert - Report



WhatsUp NMS Gold Configuration - Monitors

Active Monitors

- SNMP OID that WUG actively polls on a configurable basis
- Active monitor polls a MIB, and expects a certain value back
 - As defined in Monitor Library in Admin Console
- If polling returns a value other than the expected value, or no value at all, monitor is “Down”

WhatsUp Gold Configuration NMS - Monitors

Active Monitors

Example active monitors

The image shows a screenshot of the 'Active Monitor Properties' dialog box overlaid on the 'Active Monitors' configuration table. A blue arrow points from the 'Edit' icon in the table's toolbar to the dialog box.

Active Monitor Properties Dialog:

- Apply this Action Policy: Interface Action Policy
- State Change: Up, Action to perform: Interface Up Alarm
- State Change: Down, Action to perform: Interface Down Alarm
- Buttons: Back, Next, Finish, Cancel

Active Monitors Table:

Monitor	Argument	Com	Up at least 5 min	Yes	Yes	No	130 seconds (Default)
<input checked="" type="checkbox"/> Interface	15	MGMT	Up at least 5 min	Yes	Yes	No	130 seconds (Default)
<input type="checkbox"/> Interface	5	RAILA	Up at least 5 min	Yes	Yes	No	130 seconds (Default)
<input type="checkbox"/> Interface	8	RAILB	Up at least 5 min	Yes	Yes	No	130 seconds (Default)
<input type="checkbox"/> Interface	3	RAILV	Up at least 5 min	Yes	Yes	No	130 seconds (Default)
<input type="checkbox"/> Ping			Up at least 5 min	Yes	Yes	Yes (1)	130 seconds (Default)
<input type="checkbox"/> SNMP			Up at least 5 min	Yes	Yes	Yes (2)	130 seconds (Default)
Type: Passive Monitor							
<input type="checkbox"/> Domain Time Sync Fail				Yes	Yes		
<input type="checkbox"/> Domain Time Sync Out of Bo...				Yes	Yes		

WhatsUp Gold Configuration NMS - Monitors

Passive Monitors

- SNMP OID that WUG passively listens for via SNMP trap
- Originator of trap must be configured to send the trap to WUG
- In AIM, most monitoring is active
- Passive monitors limited to
 - Domain Time II time sync failures
 - Monitored Applications or services

WhatsUp Gold Configuration NMS - Monitors

Performance Monitors

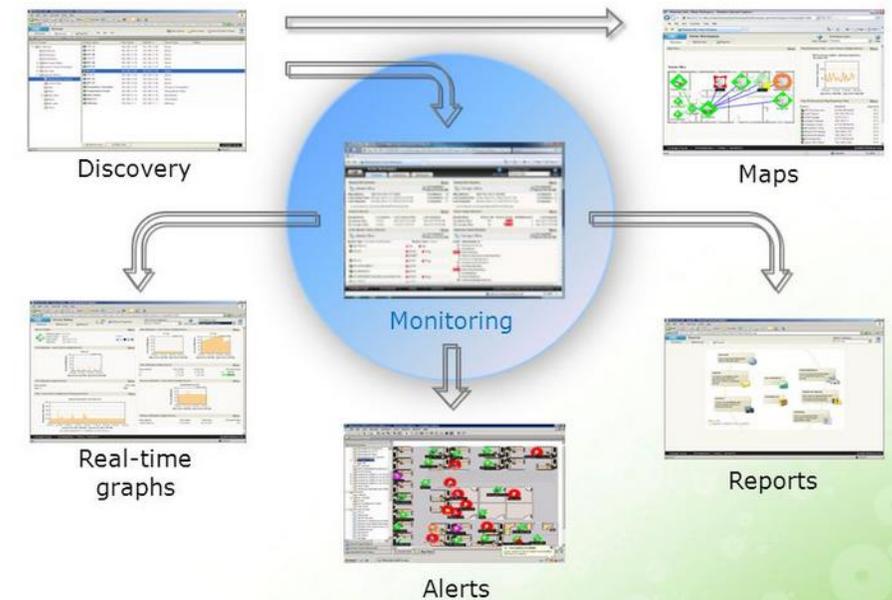
What performance indicators are relevant for this machine?

▼ Type: Performance Monitor				
<input type="checkbox"/>	 CPU Utilization	Yes	Yes	10 Minutes
<input type="checkbox"/>	 Disk Utilization	Yes	Yes	10 Minutes
<input type="checkbox"/>	 Memory Utilization	Yes	Yes	10 Minutes
<input type="checkbox"/>	 Ping Latency and Availability	Yes	Yes	10 Minutes
<input type="checkbox"/>	 VMware Datastore IOPS	No	No	

Initial conditions assume a WhatsUp Gold instance is installed and ready to configure:

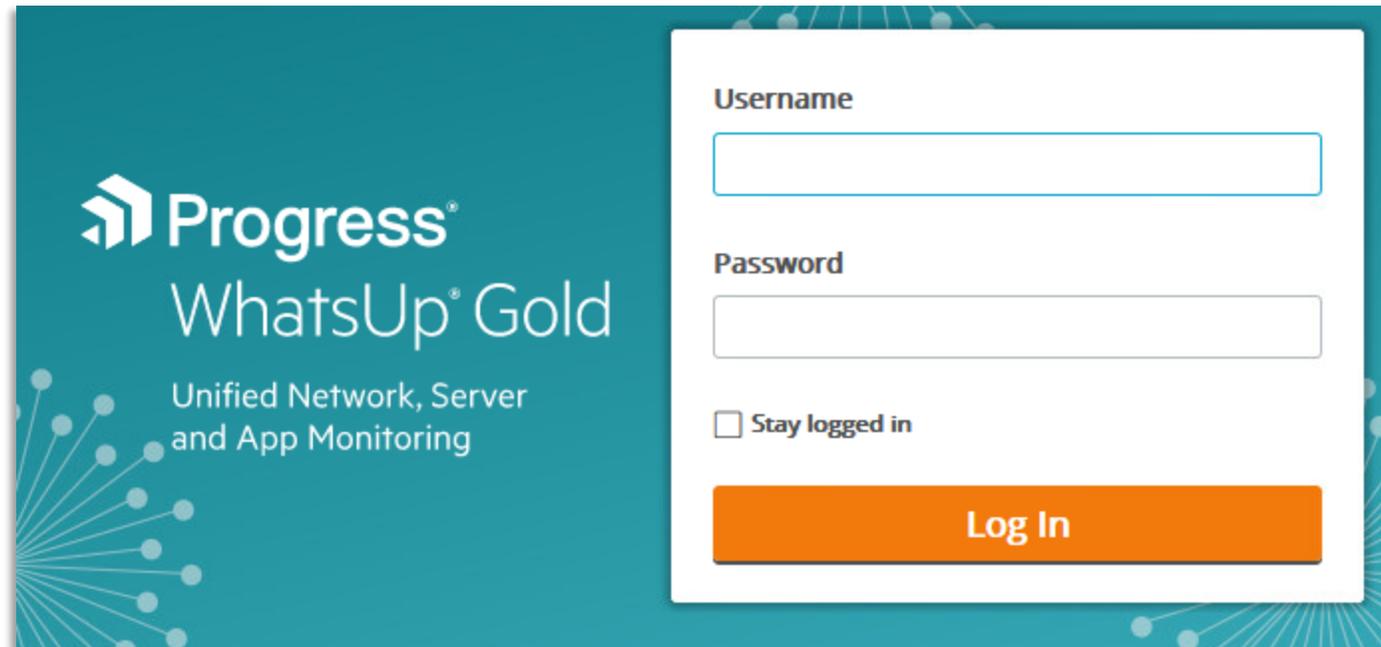
- Network Discovery
 - Discover network attached devices using a Discovery Scan via SNMP credentials
- Device Configuration
 - Once a device is discovered, the properties of the device are configured
 - Active, Passive, and Performance monitors are configured
 - Ensuring correct arguments are assigned to the Active monitors
 - Setting Polling frequency for device (30s, 60s, 120s)
- Configure Actions / Alarming
 - Configure Actions
 - Assigning Action Policies to each of the Active monitors (Interface, Ping, Monitor policies) → CreateAIMAlarm.exe
 - Configuring action on SNMP trap messages for Passive monitors → CreateAIMAlarm.exe
 - Configuring scheduled task to pull performance data from the database for the passive monitors → WUGNotify.ps1.

Discover - Map - Monitor - Alert - Report



WhatsUp Gold NMS Administration - Website

Log In with domain administrator credentials



Progress®
WhatsUp® Gold
Unified Network, Server
and App Monitoring

Username

Password

Stay logged in

Log In

WhatsUp Gold NMS Administration - Website

Devices tab – Detail view

Display Name	Device Role	Operating System	Status	Brand
SASVIDEO2	Windows Desktop	Windows 10	Ping - Down At Least 20 Minutes	VMware, Inc.
SASGUI2	Windows Desktop	Windows 10	Ping - Down At Least 20 Minutes	VMware, Inc.
sasvideo1	Windows Desktop	Windows 10	Ping - Down At Least 20 Minutes	Dell Inc.
sasgui1	Windows Desktop	Windows 10	Ping - Down At Least 20 Minutes	Dell Inc.
CASVIDEO2	Windows Desktop	Windows 10	Up	VMware, Inc.
CASGUI2	Windows Desktop	Windows 10	RAILA - Down At Least 20 Minutes, RAILB - Down At Least 20 Minutes	VMware, Inc.
casvideo1	Windows Desktop	Windows 10	Ping - Down At Least 20 Minutes	Intel Corporation
NMS	Windows Server	Windows	Up	VMware, Inc.
CYBER02	Windows Server	Windows	Up	VMware, Inc.
CYBER01	Windows Server	Windows	Up	VMware, Inc.
CLIP02	Windows Server	Windows Server	Ping - Down At Least 20 Minutes, SNMP - Down At Least 20 Minutes, MGMT ...	VMware, Inc.
iebsts	Windows Server	Windows	Ping - Down At Least 20 Minutes	VMware, Inc.

WhatsUp Gold NMS Administration - Website

Home screen is configurable

- Drag and drop displays
- Configure size, etc.

The screenshot displays the 'Home Dashboard' of the WhatsUp Gold NMS website. The dashboard is organized into several sections:

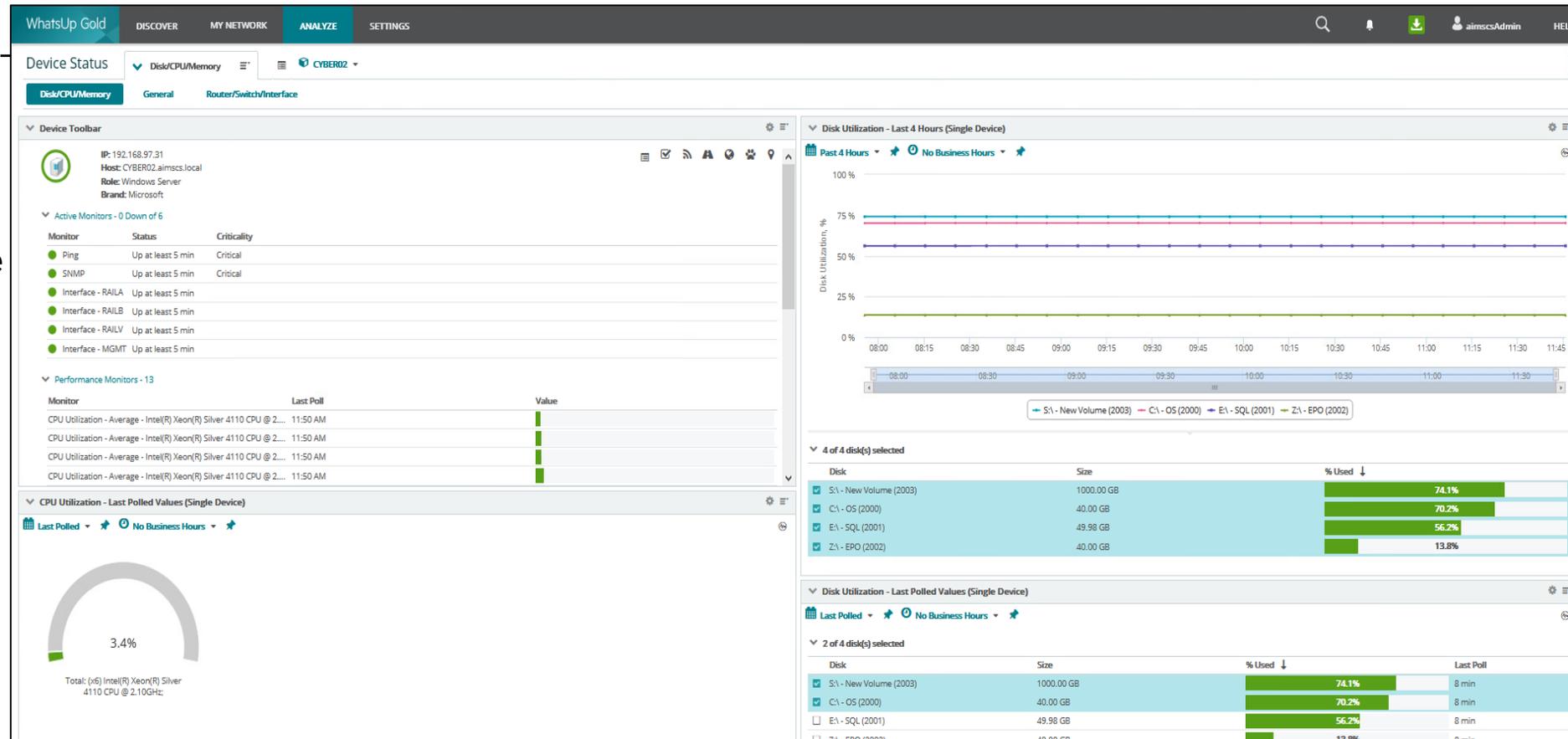
- Memory Utilization - Top 10 by Utilization:** A table showing memory usage for various devices. The top entries are SIEM (97%), HOSTA (81.7%), and HOSTA (80.7%).
- CPU Utilization - Top 10 by Utilization:** A table showing CPU usage for various devices. The top entries are SVR1B (43.8%), NTP Server (43%), and SVR1A (40.8%).
- Disk Utilization - Top 10 by Utilization:** A table showing disk usage for various devices. The top entries are CYBER01 (83.9%), ADA (83.8%), and CYBER01 (70.6%).
- Interface - Top 10 by Bandwidth Utilization:** A table showing bandwidth usage for various interfaces. The top entries are SAS-SW-V (Vlan400) (1.8% Tx, 0% Rx) and SAS-SW-V (Vlan410) (0% Tx, 1.7% Rx).
- Total Devices by Type:** A table showing the distribution of device roles. The top entries are Discovery Template (15.4%, 40), Windows (12%, 31), and Windows Infrastructure (12%, 31).
- Poller Health:** A table showing the status of the local poller, which is currently 'Running' with a 'Lag Time' of 0 s and a 'Lag Time Status' of 'Good'.
- Summary Counts:** A section for overall system counts.

The dashboard also includes a navigation menu on the right side with options like 'Add Reports', 'Custom Content', 'Devices', 'Active Monitor Availability', 'Attributes', 'Current Device States', 'Dependencies', 'Device Active Monitor States', 'Device Custom Links', 'Device Group Mini Status', 'Device Information and Status', 'Device SNMP Details', 'Devices in Maintenance', 'Enabled Active Monitors', 'Interface Details', 'Live Activity', 'Map View', 'Monitors Applied', 'Notes', 'Performance Monitor Summary', 'Performance', 'System Info', 'Troubleshooting', and 'Wireless'.

WhatsUp Gold NMS Administration - Website

Device status

- Disk/CPU/Memory Tab – vital usage statistics
- General Tab – last alarms/alerts, etc.
- Router/Switch/Interface Tab – bandwidth and interfaces statistics



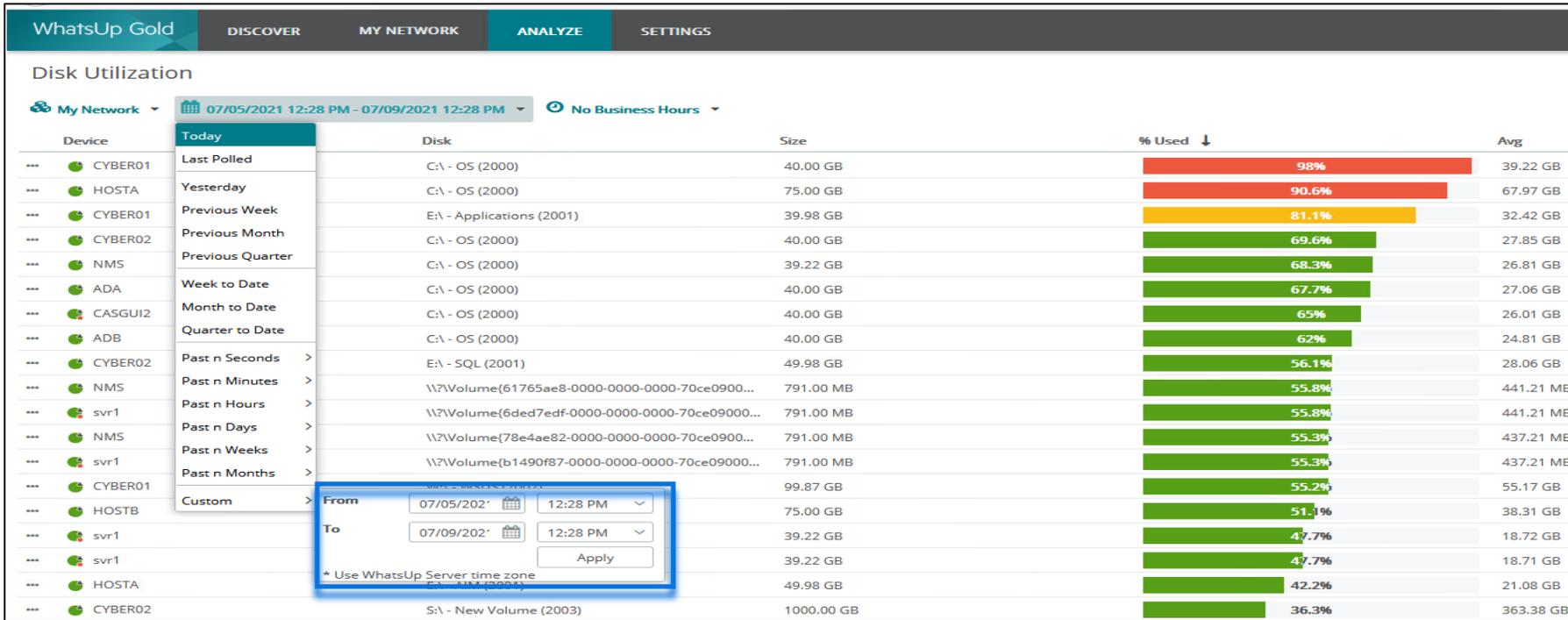
WhatsUp Gold NMS Administration - Website

Analyze

WUG Performance searches give normalized historical data on components over a period of time

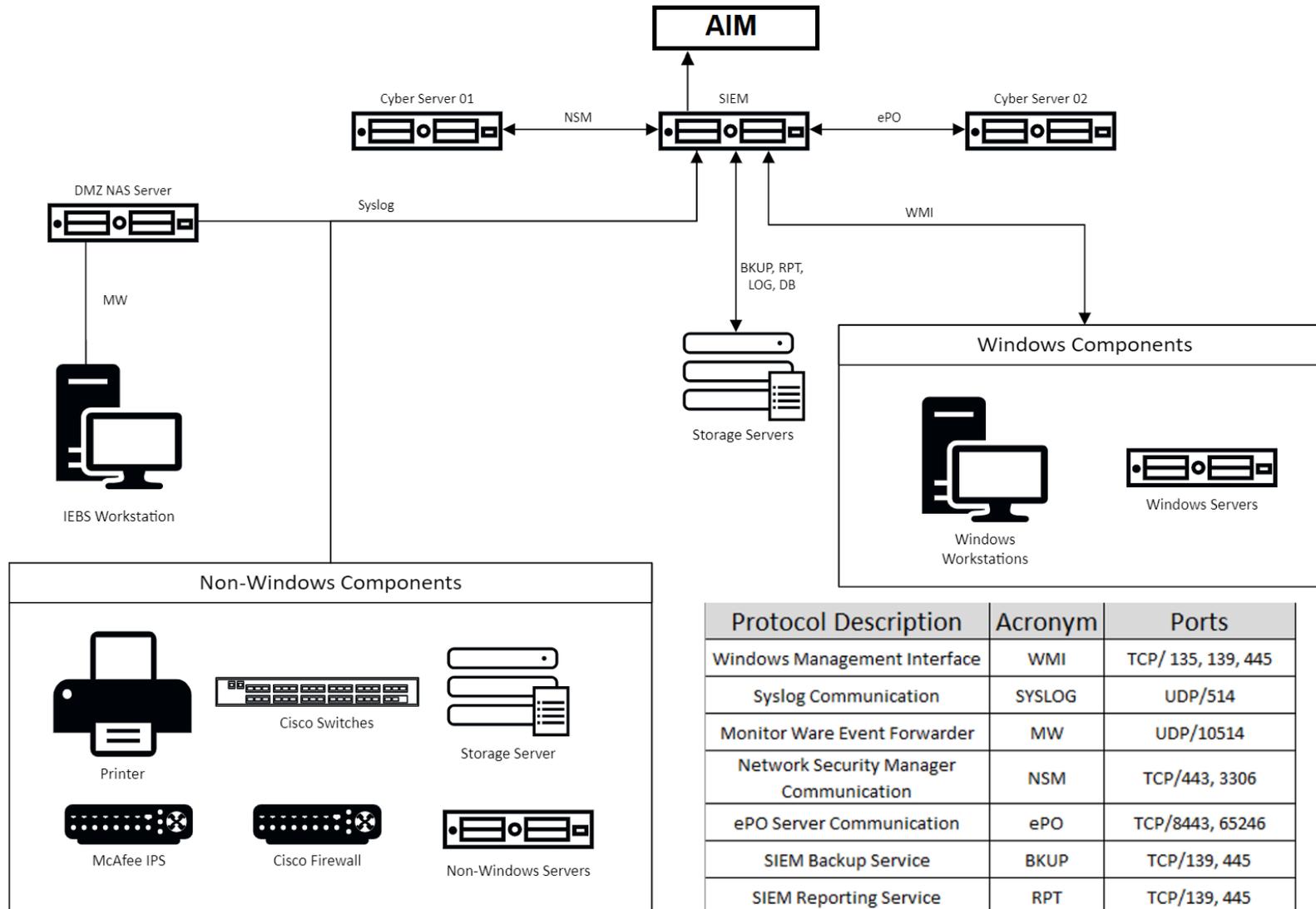
- Bandwidth utilization over last 24 hours
- Processor utilization over last 2 weeks

WUG is set to purge data after 60 days to prevent database growth



SIEM and NMS Dataflow





Protocol Description	Acronym	Ports
Windows Management Interface	WMI	TCP/ 135, 139, 445
Syslog Communication	SYSLOG	UDP/514
Monitor Ware Event Forwarder	MW	UDP/10514
Network Security Manager Communication	NSM	TCP/443, 3306
ePO Server Communication	ePO	TCP/8443, 65246
SIEM Backup Service	BKUP	TCP/139, 445
SIEM Reporting Service	RPT	TCP/139, 445
SIEM Log Storage Service	LOG	TCP/111
SIEM DB Storage Service	DB	TCP/111

- Alarming to AIM works by configuring an Alarm action for the SIEM Alarm to forward to AIM.
 - When an alarm is generated, the SIEM sends a Syslog Message to both Hosts.
 - The Primary Host parses the syslog and processes an AIM Alarm in the UI.
- Configure Alarming to AIM
 - Alarm Settings -> Actions -> Send Message -> Configure.

Alarm Settings

Summary | Condition | Devices | **Actions** | Escalation

Log event

Auto-acknowledge Alarm

Visual Alert: [Configure](#)

Create Case: [Configure](#)

Update Watchlist: [Configure](#)

Send Message: [Configure](#)

SYSLOG@192.168.2.12;514;User;... [Remove](#)

SYSLOG@192.168.2.13;514;User;... [Remove](#)

[Add recipient](#)

Generate Reports: [Configure](#)

Execute remote command: [Configure](#)

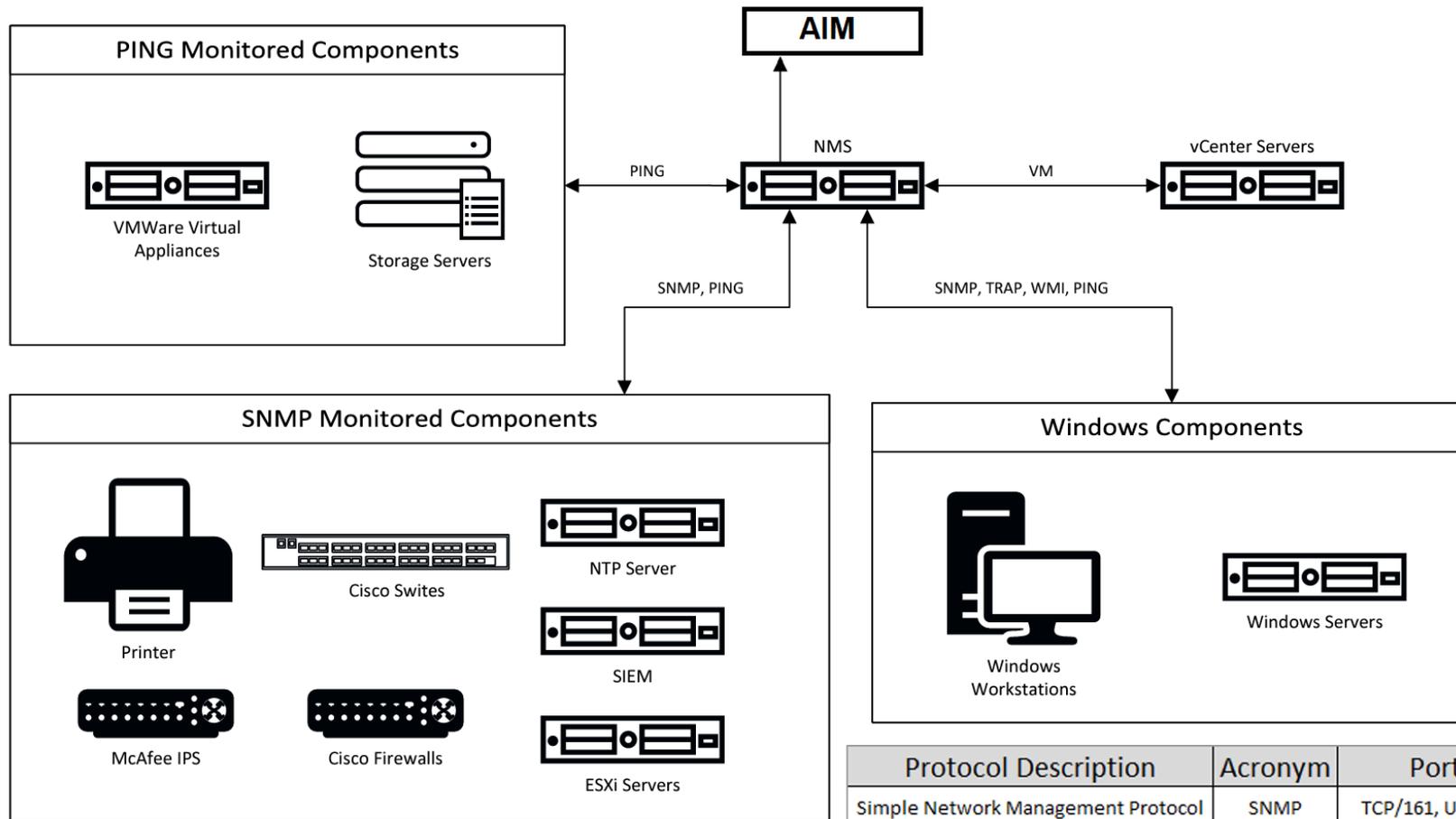
Send to Remedy: [Configure](#)

Assign Tag with ePO: [Configure](#)

Blacklist: [Configure](#)

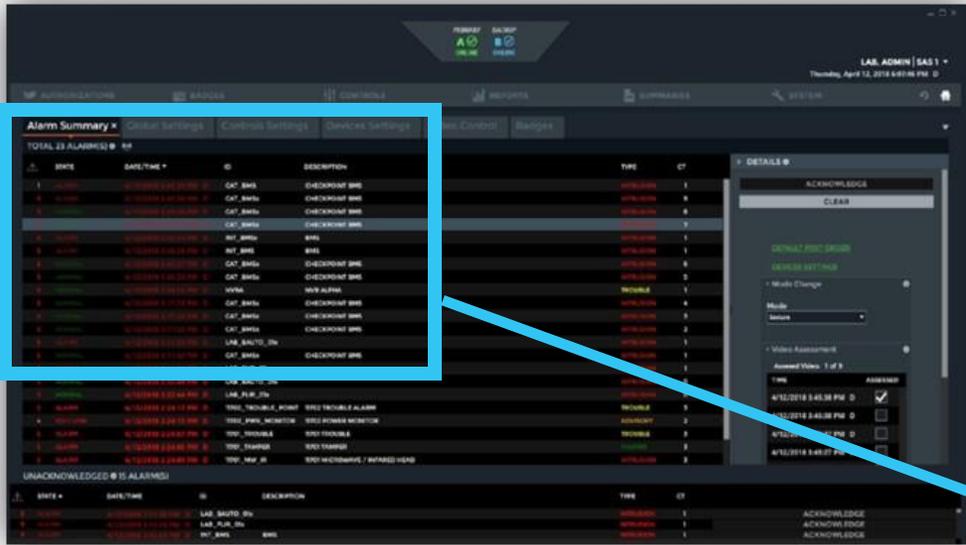
Custom alarm summary [Configure](#)

[Cancel](#) [< Back](#) [Next >](#) [Finish](#)

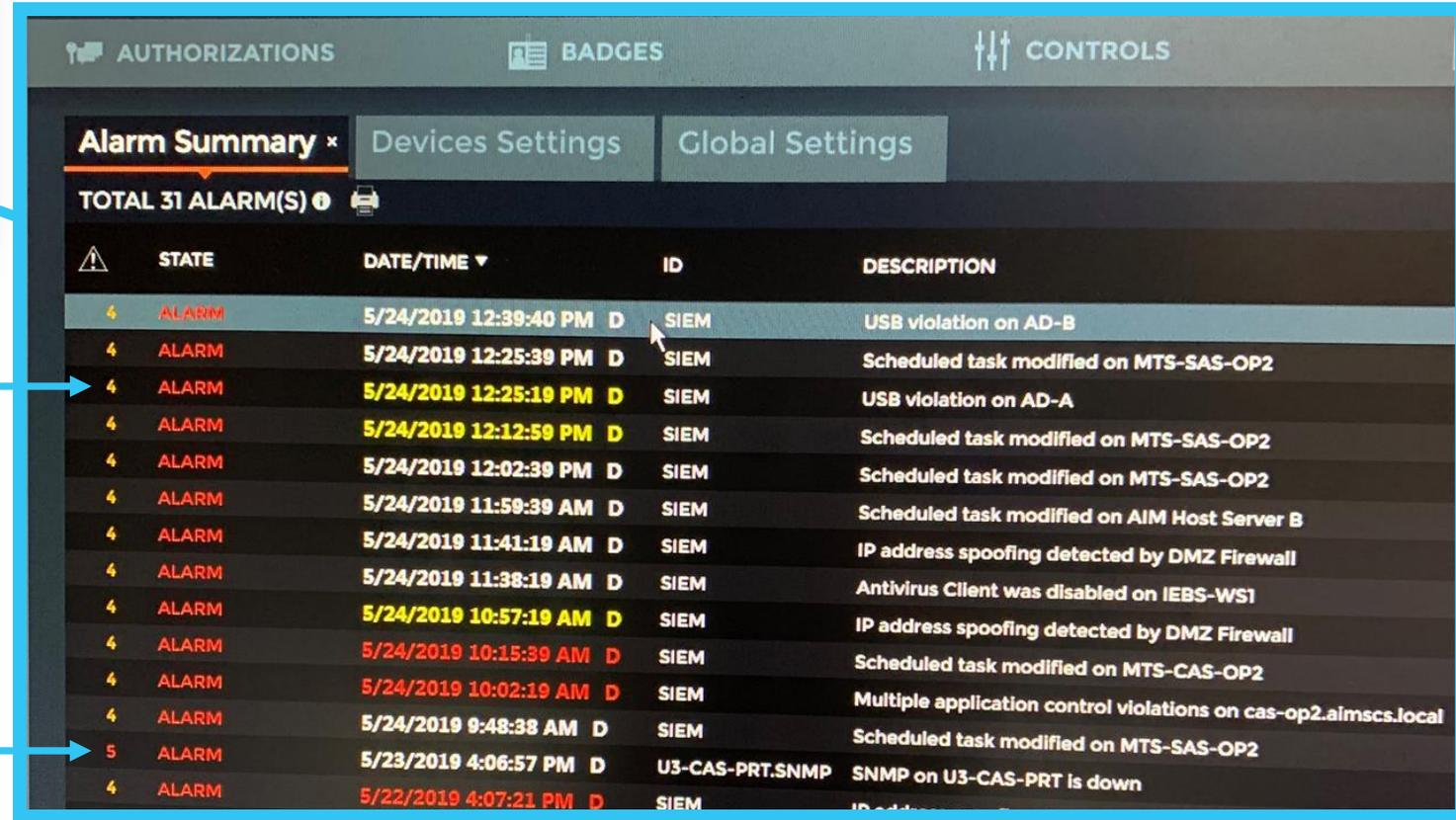


Protocol Description	Acronym	Ports
Simple Network Management Protocol	SNMP	TCP/161, UDP/161
SNMP Traps	TRAP	UDP/162
Windows Management Interface	WMI	TCP/135
vSphere Monitoring	VM	TCP/80, 443
PING Monitor	PING	ICMP

- Alarming to AIM works by a custom executable created by Mirion SIS 'CreateAIMAlarm.exe'
 - When an alarm is generated, WUG passes parameters to CreateAIMAlarm.exe, which then parses through a custom XML file to provide the appropriate alarm message and formatting for the alarm state.
 - The Alarm is then transmitted as a message to AIM.
 - AIM receives the message and then produces the Alarm in the Alarm List on the UI.
- Configure Alarming
 - Active and Passive monitors directly call CreateAIMAlarm.exe
 - Performance Monitors call WUGNotify.ps1 via Scheduled Task
 - Parses WUG Database
 - Writes any new alarm states which have been generated (WUGsize.txt)
 - Calls CreateAIMAlarm.exe to send new alarms to AIM



SIEM Alarm



WUG NMS Alarm

Final Exam

- How does WhatsUp Gold obtain status information from system components?
- Where do you go to access the WhatsUp Gold interface?
- How are WhatsUp Gold alarms sent to AIM?
- What are the main functions of the SIEM?
- What is the difference between the ELM and the ESM?
- What are some of the alarms already defined in the system?
- Where do you go to start investigation of alarms?

Who is ready for their next NRC Cyber Inspection?



MIRION
TECHNOLOGIES

Questions?

