



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.

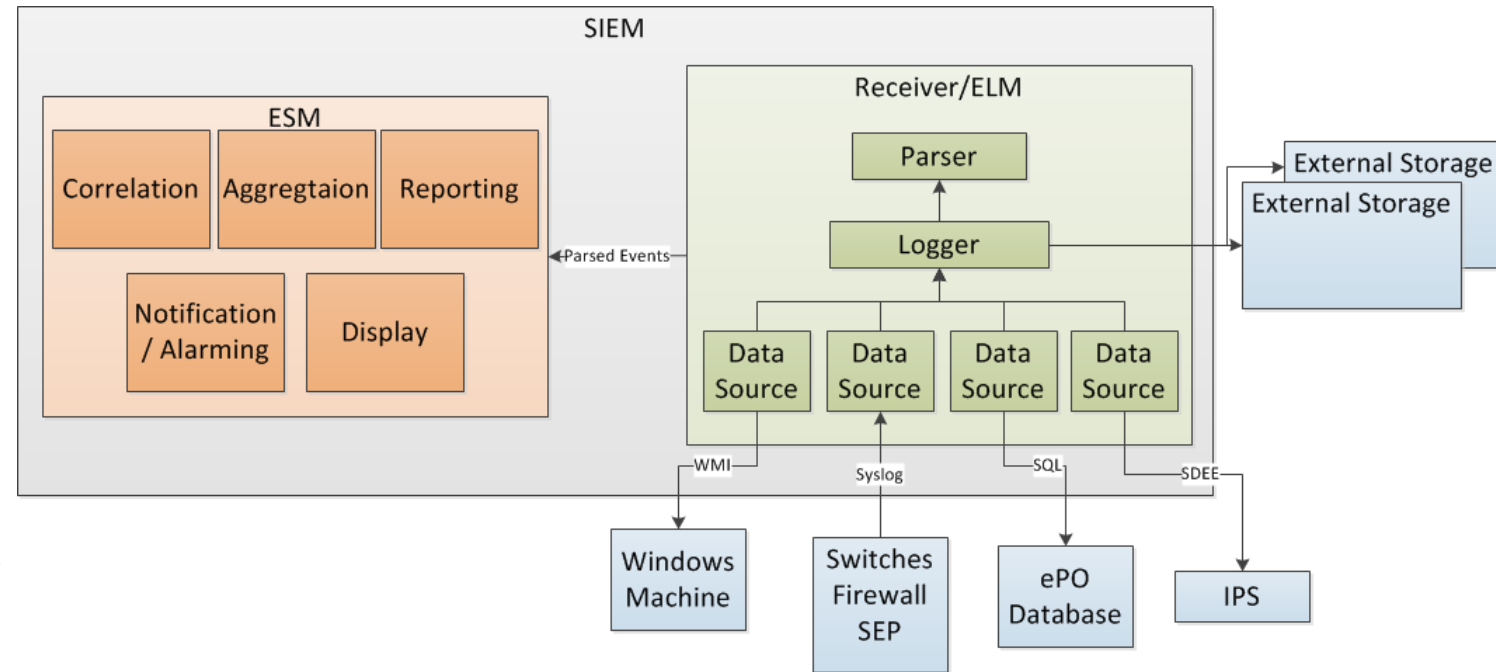
- Common SIEM Datasources on an AIM SCS System
 - Network Switches and Devices
 - Servers and Workstations (Running Windows, Linux, etc.)
 - Cyber Security Devices and Software Applications (NIDS, Firewalls (HW and SW), Endpoint Protection, etc.)
 - Encoders
 - Other SIEMs

■ Datasources provide data to the SIEM by

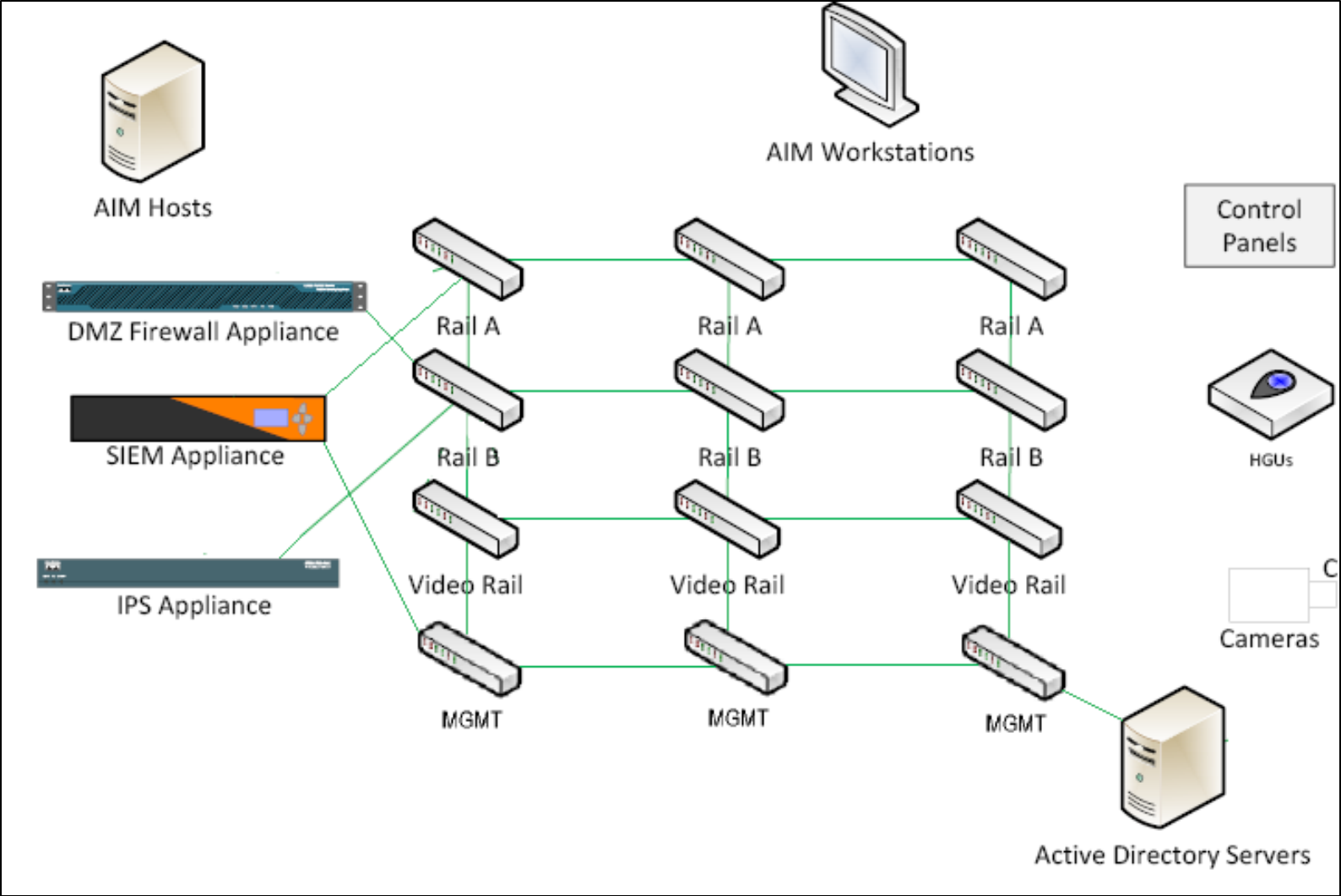
- RFC 5424 Syslog
- WMI (Windows Servers and Workstations)
- Databases (Trellix ePO, Trellix IPS)

■ 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



Properties

Policy Editor

Retrieve Events

ESM 11.3.2 20200730

User time: 07/16/2021 14:24

16

?

SIEM_Admin

Configuration

Normalized Dashboard

Add Tab

Physical Display

Physical Display

Local ESM

Local ESM

Local Receiver-ELM

Mcafee_ePO

(Mcafee_ePO)

Mcafee_ePO_Endpoint Security Firewa

Mcafee_ePO_Endpoint Security Platfor

Mcafee_ePO_Endpoint Security Threat

Mcafee_ePO_Endpoint Security Web C

Mcafee_ePO_ePO Audit Log (ePO)

Mcafee_ePO_ePolicy Orchestrator Age

Mcafee_ePO_Host Data Loss Preventi

NIDS

Alarms

SIEM Critical Status

Rogue System(s) Detected

SIEM Critical Status

Rogue System(s) Detected

Rogue System(s) Detected

Local ESM - Mcafee_ePO - (Mcafee_ePO)

Triggered Alarms

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		

Details

Triggering Event

Actions

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

Alarm Details

Filters

Signature ID

or Aa

Destination IP

or

Normalized ID

or

Source IP

or

Destination U...

or Aa

Source User

or Aa

Enter a Field or Filter Set

Data Sources

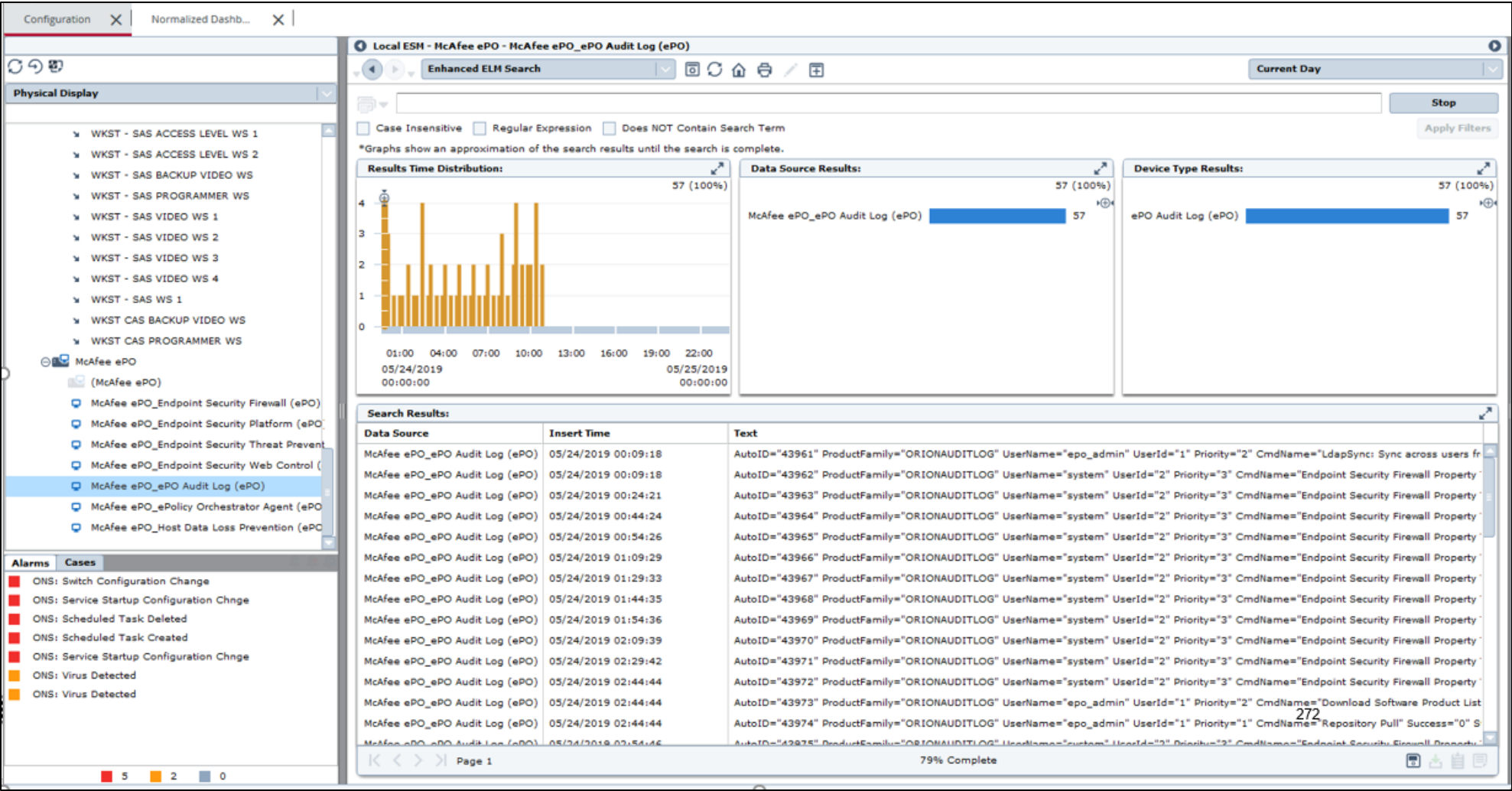
Unacknowledged Alarms

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

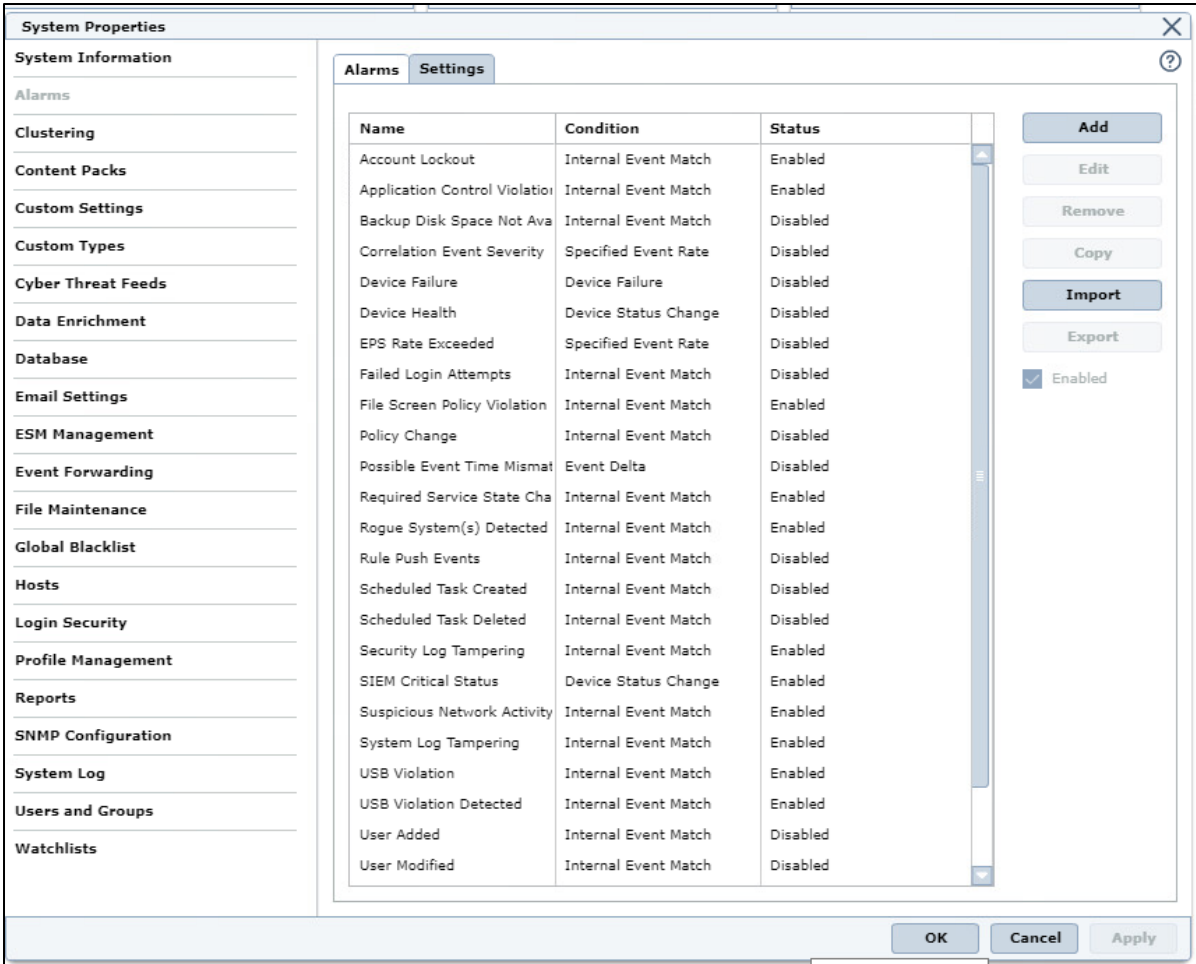
- Add Datasources to the SIEM
 - Syslog Datasources need to be configured to forward logs to SIEM.
 - WMI and Database Datasources need to have an account created with the service account credentials
- Configure Rule sets
 - Mirion SIS has a standard ruleset which is imported
 - Create custom rules for 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"/>

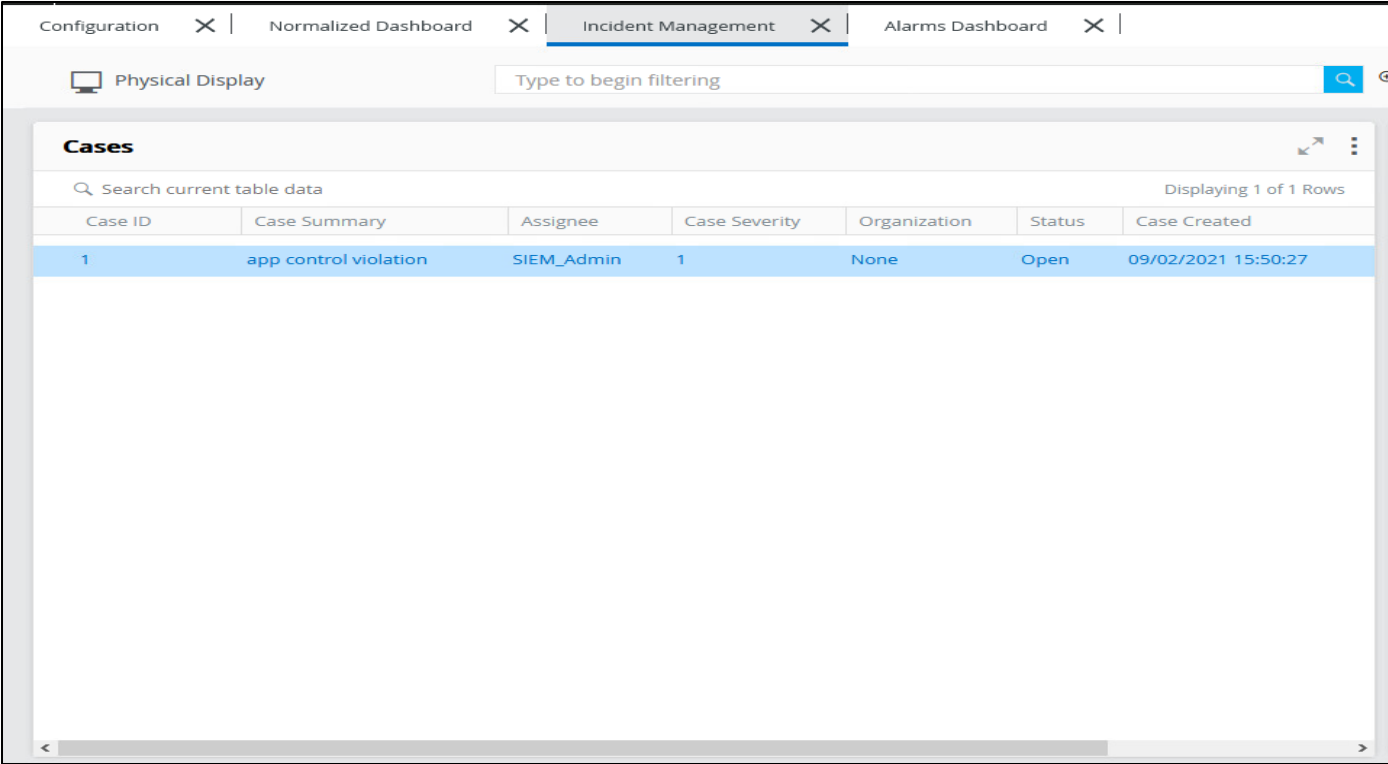
Searching the ELM
Logs (Enterprise Log
Manager)



- 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



- 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)



The screenshot shows a web application interface for Incident Management. At the top, there are tabs for Configuration, Normalized Dashboard, Incident Management (selected), and Alarms Dashboard. Below the tabs is a search bar with the placeholder text 'Type to begin filtering'. The main content area is titled 'Cases' and contains a table with the following 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

The table is titled 'Cases' and has a search bar above it. The table has 7 columns: Case ID, Case Summary, Assignee, Case Severity, Organization, Status, and Case Created. There is one row of data. The table is displaying 1 of 1 rows.

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

System Properties

System Information

Alarms

Clustering

Content Packs

Custom Settings

Custom Types

Cyber Threat Feeds

Data Enrichment

Database

Email Settings

ESM Management

Event Forwarding

File Maintenance

Global Blacklist

Hosts

Login Security

Profile Management

Reports

SNMP Configuration

System Log

Users and Groups

Watchlists

Reports:

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

Add

Edit

Remove

Run Now

Share

Import

Export

☒ Enabled

Disable

Conditions

Recipients

View

Files

Disable reporting. Reports are currently enabled.

Manage report conditions

Manage email addresses for report recipients

View currently running reports with the option to cancel them

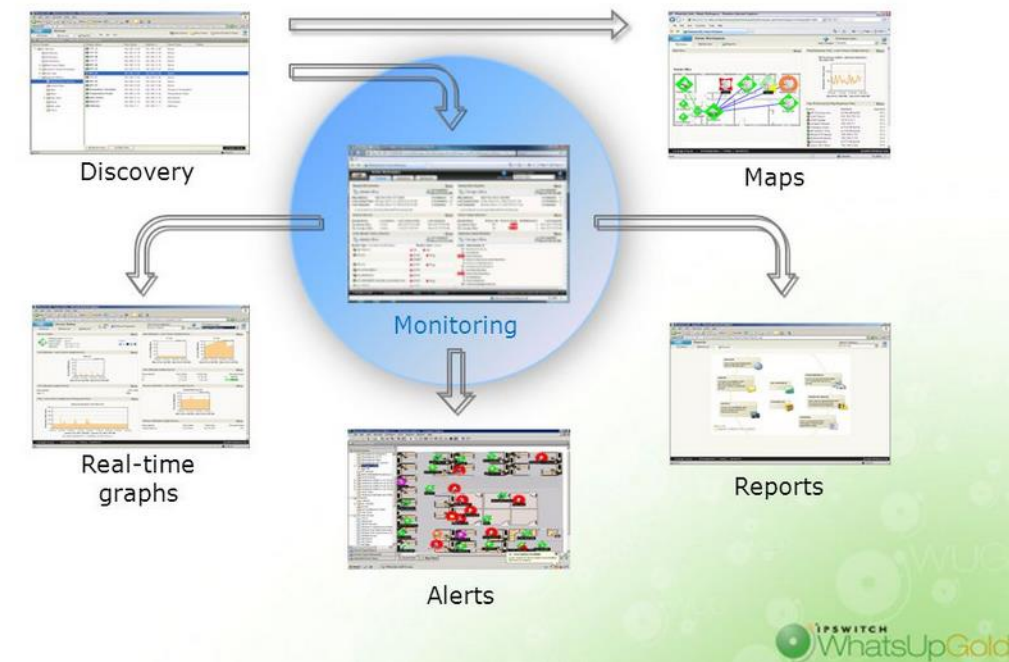
View generated report files

NMS Configuration and Administration



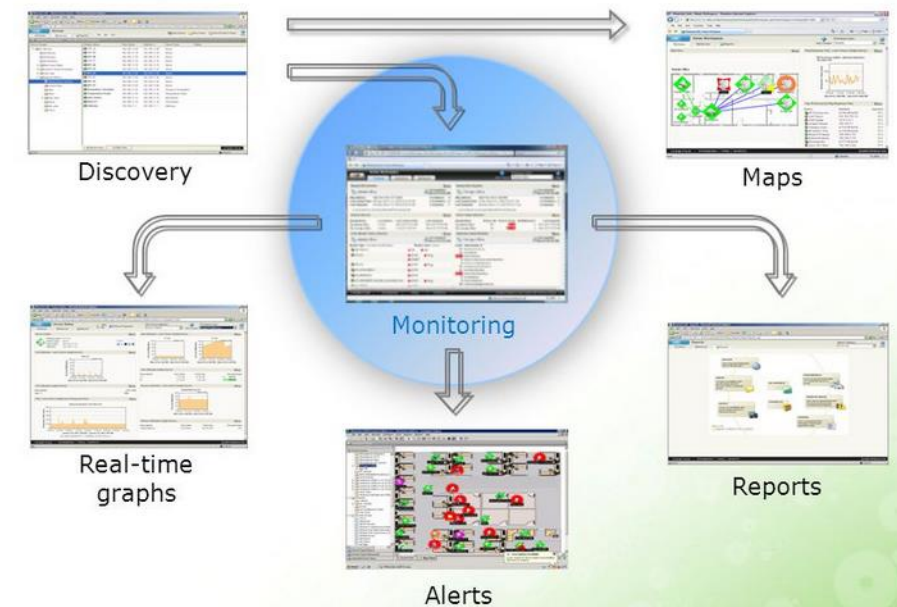
- The Network Management System (NMS) is a comprehensive network monitoring and management tool for optimizing and maintaining network infrastructure on a system.
 - Mirion SIS uses WhatsUp Gold as the NMS solution on AIM SCS systems.
- Using SNMP (Simple Network Management Protocol) and MIB (Management 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 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

Enable

Disable

Setup Critical

<input type="checkbox"/>	Monitor	Argument	Com
<input checked="" type="checkbox"/>	Interface	15	MGMT
<input type="checkbox"/>	Interface	5	RAILA
<input type="checkbox"/>	Interface	8	RAILB
<input type="checkbox"/>	Interface	3	RAILV
<input type="checkbox"/>	Ping		
<input type="checkbox"/>	SNMP		
▼ Type: Passive Monitor			
<input type="checkbox"/>	Domain Time Sync Fail		
<input type="checkbox"/>	Domain Time Sync Out of Bo...		

Active Monitor Properties

Apply this Action Policy

Interface Action Policy

State Change	Action to perform
Up	Interface Up Alarm
Down	Interface Down Alarm

Back

Next

Finish

Cancel

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

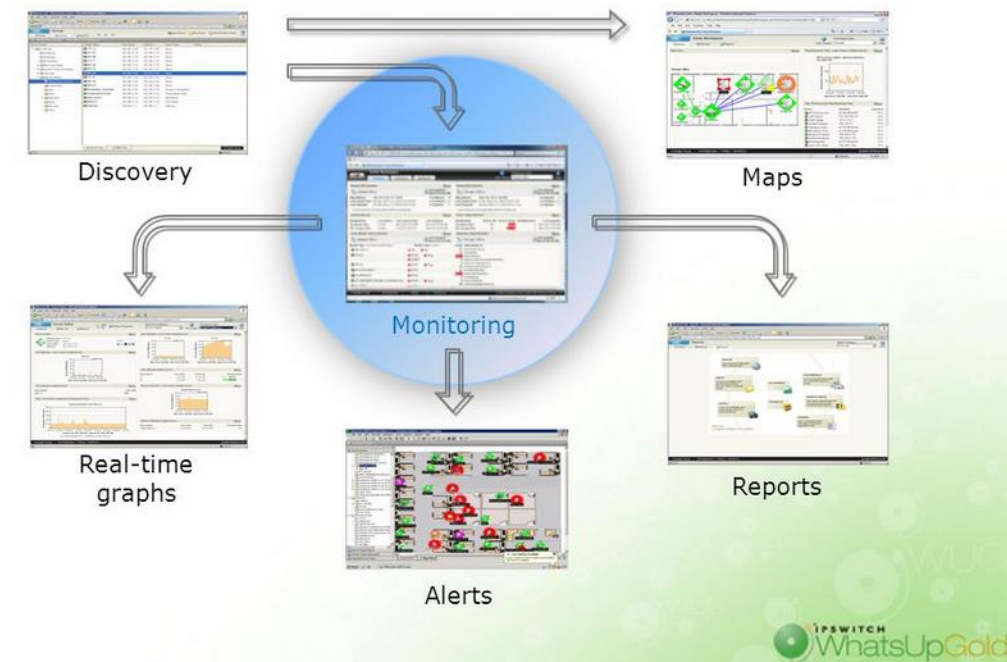
What performance indicators are relevant for this machine?

▼ 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:

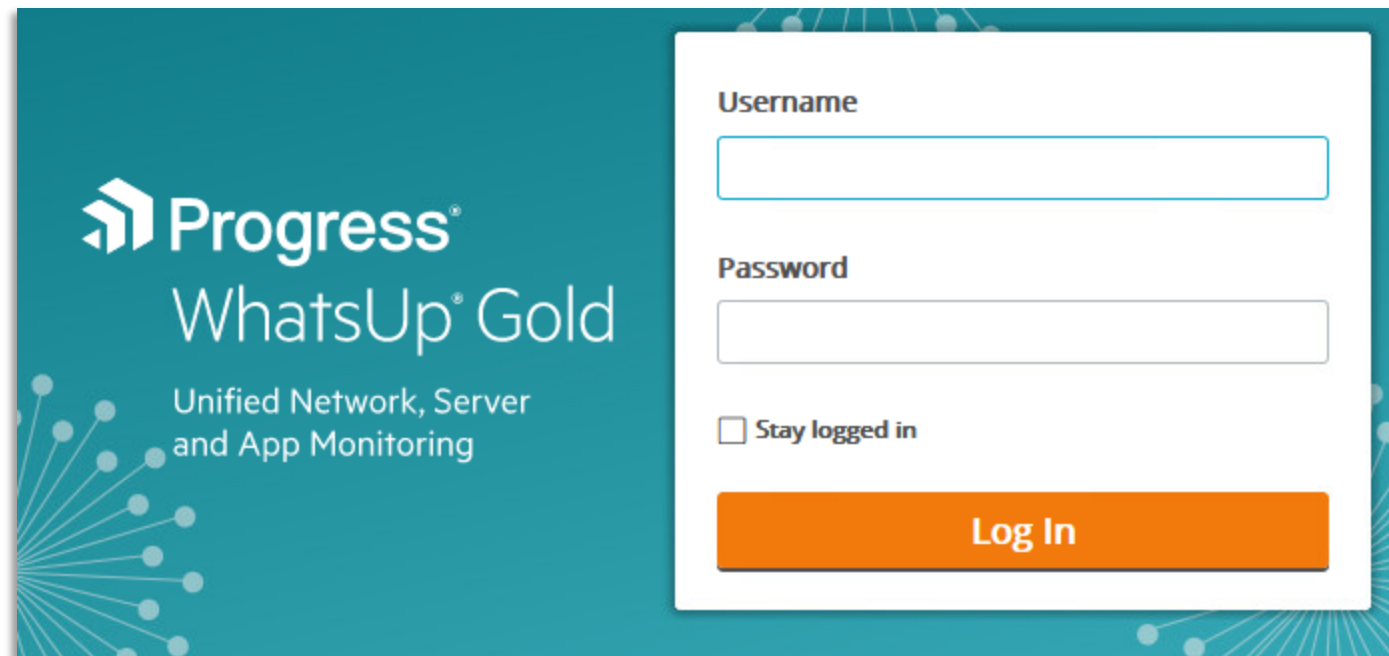
- Network Discovery
 - Discover network attached devices using a Discovery Scan via SNMP credentials
- Device Configuration
 - Once a device is discovered, the properties of the device are configured
 - Active, Passive, and Performance monitors are configured
 - Ensuring correct arguments are assigned 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



The image shows the login page for Progress WhatsUp Gold. The background is a teal color with a network diagram of nodes and lines. On the left, the Progress logo is above the text 'WhatsUp® Gold' and 'Unified Network, Server and App Monitoring'. On the right, there is a white login box containing a 'Username' field, a 'Password' field, a 'Stay logged in' checkbox, and an orange 'Log In' button.

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

Username

Password

☐ Stay logged in

Log In

WhatsUp Gold NMS Administration - Website

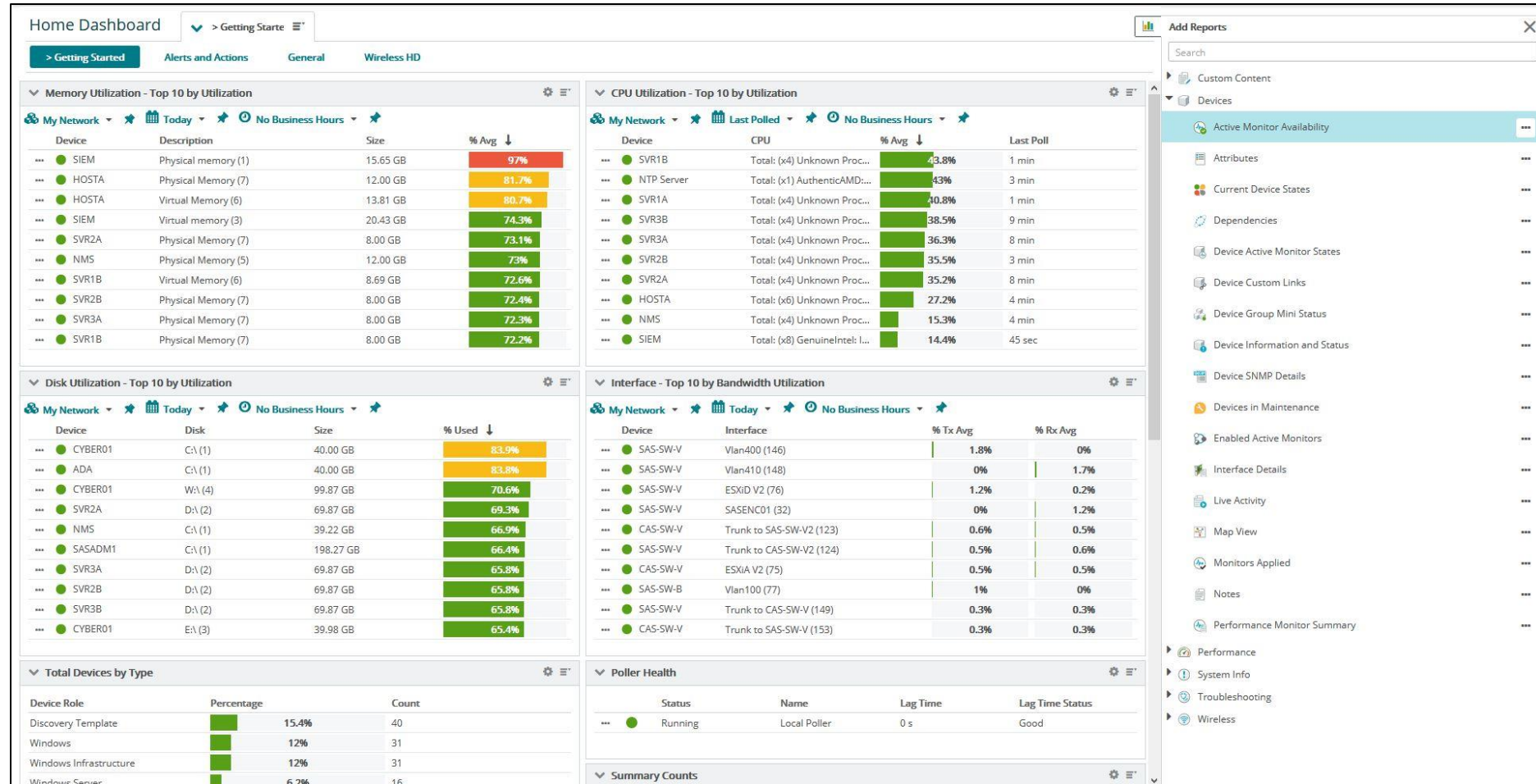
Devices tab – Detail view

WhatsUp Gold						
DISCOVER MY NETWORK ANALYZE SETTINGS						
Groups	Groups	My Network (47 Devices)				
	<input checked="" type="checkbox"/> Include devices in sub-groups					
	My Network (47)					
	AIM Hosts (2)					
	AIM Video Workstations (4)					
	AIM Workstations (4)					
	Cyber (10)					
	DMZ (3)					
	Domain Controllers (2)					
	Log Sources (0)					
Monitor Legend	Printers (1)					
	Qognify (5)					
	Switches (8)					
		<input type="checkbox"/> Display Name	Device Role	Operating System	Status	Brand
		<input type="checkbox"/> SASVIDEO2	Windows Desktop	Windows 10	Ping - Down At Least 20 Minutes	VMware, Inc.
		<input type="checkbox"/> SASGUI2	Windows Desktop	Windows 10	Ping - Down At Least 20 Minutes	VMware, Inc.
		<input type="checkbox"/> sasvideo1	Windows Desktop	Windows 10	Ping - Down At Least 20 Minutes	Dell Inc.
		<input type="checkbox"/> sasgui1	Windows Desktop	Windows 10	Ping - Down At Least 20 Minutes	Dell Inc.
		<input type="checkbox"/> CASVIDEO2	Windows Desktop	Windows 10	Up	VMware, Inc.
		<input type="checkbox"/> CASGUI2	Windows Desktop	Windows 10	RAILA - Down At Least 20 Minutes, RAILB - Down At Least 20 Minutes	VMware, Inc.
		<input type="checkbox"/> casvideo1	Windows Desktop	Windows 10	Ping - Down At Least 20 Minutes	Intel Corporation
		<input type="checkbox"/> NMS	Windows Server	Windows	Up	VMware, Inc.
		<input type="checkbox"/> CYBER02	Windows Server	Windows	Up	VMware, Inc.
		<input type="checkbox"/> CYBER01	Windows Server	Windows	Up	VMware, Inc.
		<input type="checkbox"/> CLIP02	Windows Server	Windows Server	Ping - Down At Least 20 Minutes, SNMP - Down At Least 20 Minutes, MGMT ...	VMware, Inc.
		<input type="checkbox"/> iebsts	Windows Server	Windows	Ping - Down At Least 20 Minutes	VMware, Inc.

WhatsUp Gold NMS Administration - Website

Home screen is configurable

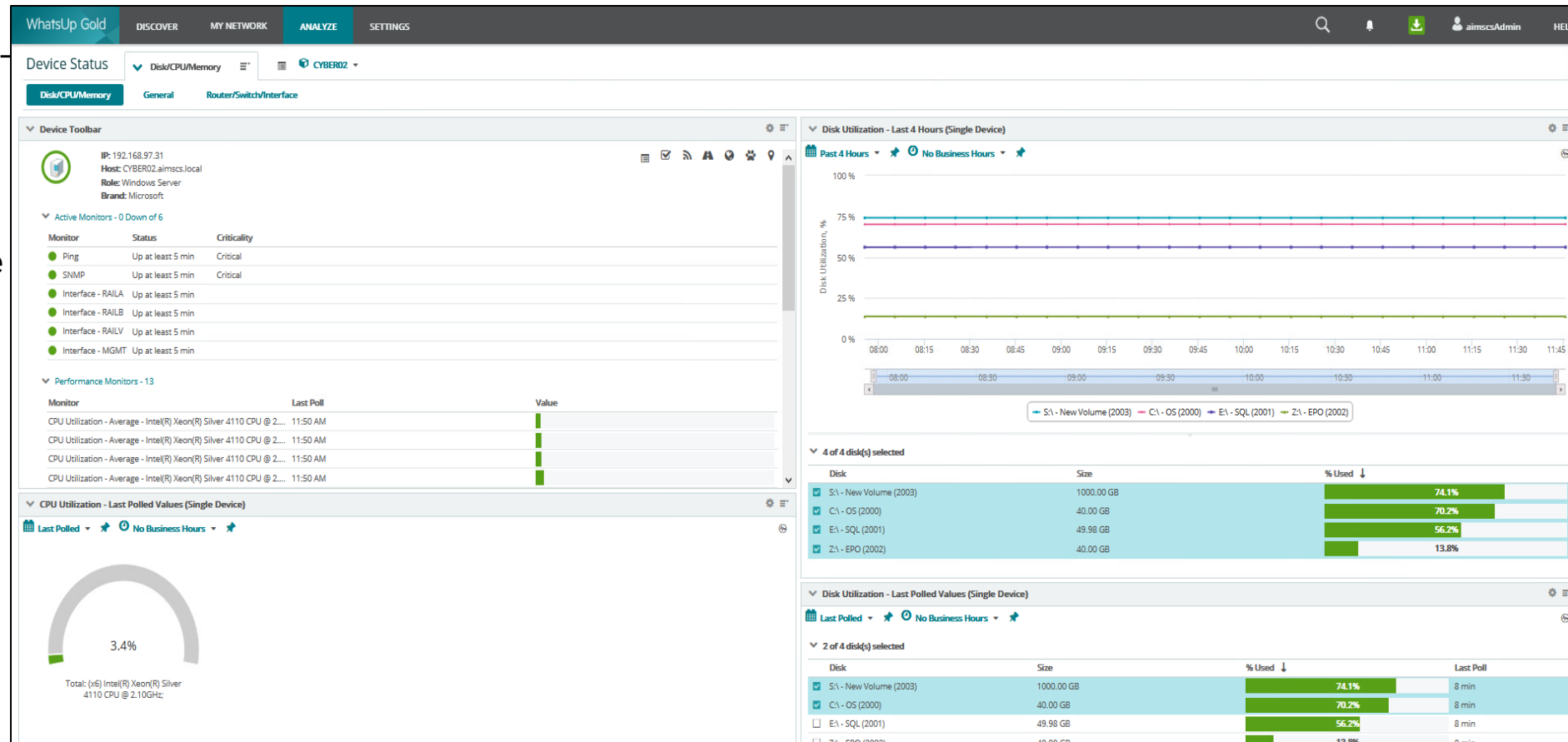
- Drag and drop displays
- Configure size, etc.



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



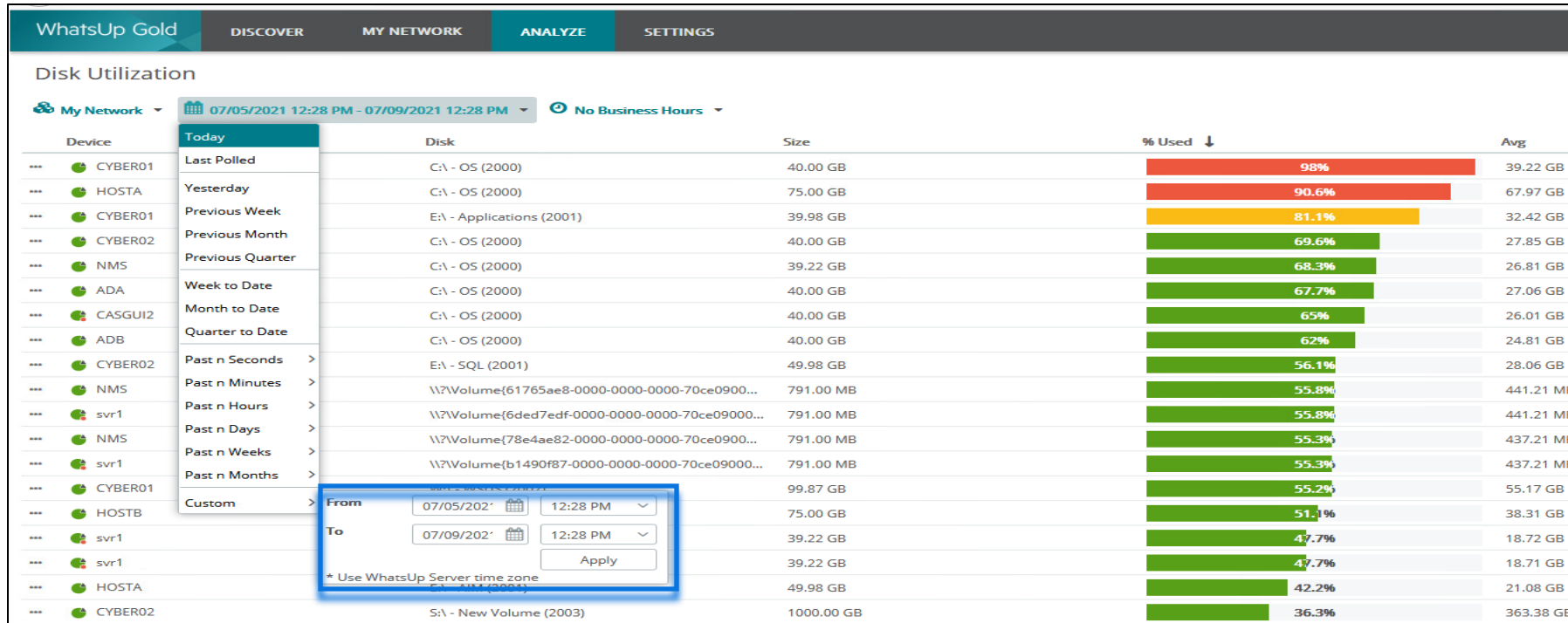
WhatsUp Gold NMS Administration - Website

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




WhatsUp Gold NMS Administration - Device Properties

Device properties

- Name: no spaces or special characters
- Polling type: Host Name vs Network Address

Device Properties

HOSTA


Keep Details Current
☒

Display Name | [Edit](#)
HOSTA

Host Name | [Edit](#)
HOSTA.aimsco.local

IP Address | [Configure Network Interfaces](#)
192.168.97.12

SNMP OID | [Edit Custom](#)
1.3.6.1.4.1.311.1.1.3.1.2

OS | [Edit](#)
Windows Server 2019

Brand | [Edit](#)
VMware, Inc.

Role | [Edit](#)
Windows Server

Device Status Up

Up At Least 5 Minutes

Notes | [Edit](#)
This device was scanned by discovery on 11/2/2020 9:50:00 AM.

Monitors (13)

Polling

Actions

Credentials (2)

Groups (1)

Attributes (17)

Roles (5)

Inventory

Refresh timeline

Links (0)

Tasks (0)


+ -

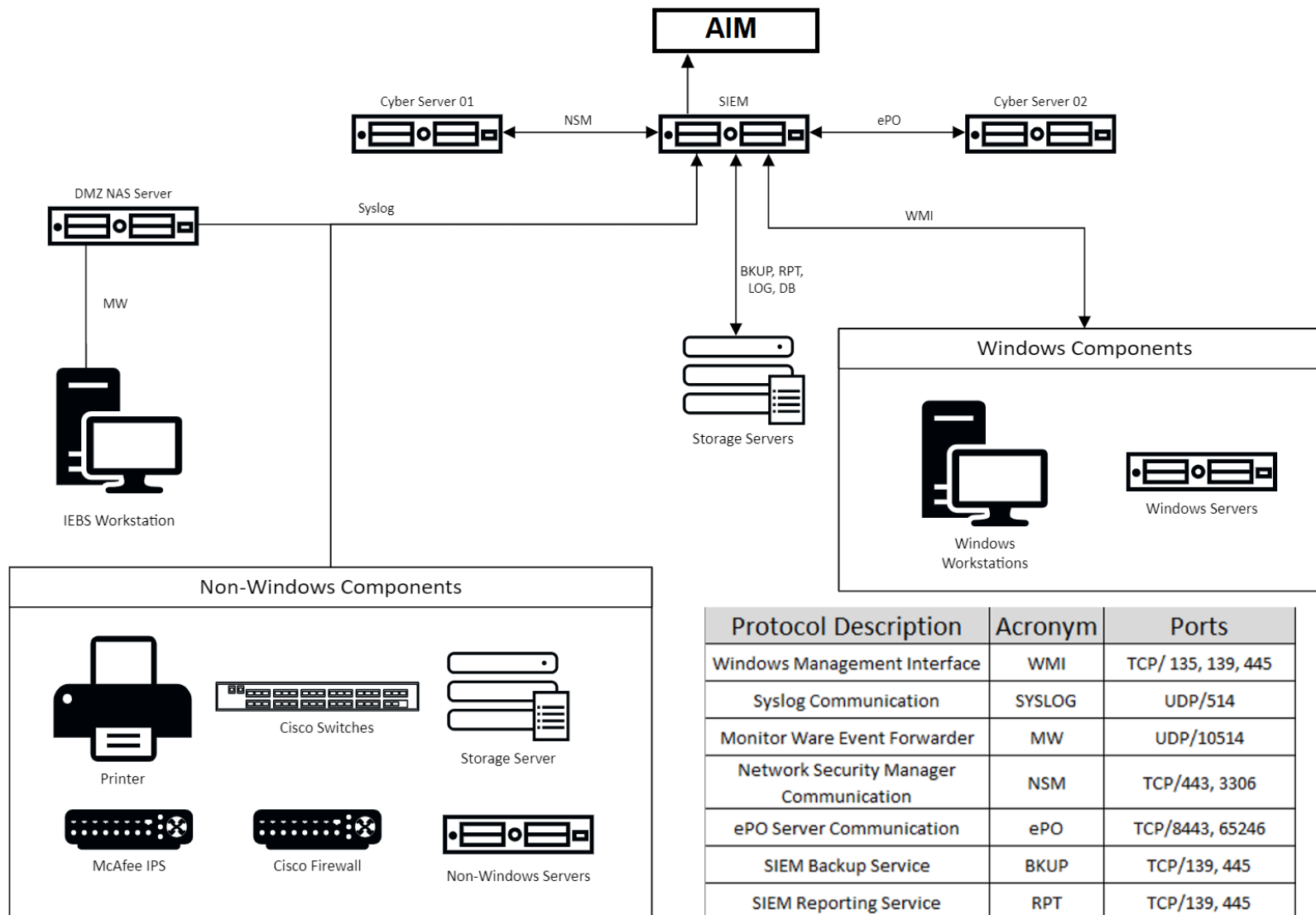
[Enable](#) [Disable](#) [Setup Critical \(Enabled\)](#) ☐ Hide disabled monitors

Go to library...

<input type="checkbox"/> Monitor	Argument	Comment	Status	Enabled	Library	Critical	Polling Interval
▼ Type: Active Monitor							
<input type="checkbox"/> Interface	3	MGMT	Up at least 5 min	Yes	Yes	No	60 seconds (Default)
<input type="checkbox"/> Interface	8	RAILA	Up at least 5 min	Yes	Yes	No	60 seconds (Default)
<input type="checkbox"/> Interface	9	RAILB	Up at least 5 min	Yes	Yes	No	60 seconds (Default)
<input type="checkbox"/> Interface	6	RAILV	Up at least 5 min	Yes	Yes	No	60 seconds (Default)
<input type="checkbox"/> Ping			Up at least 5 min	Yes	Yes	Yes (1)	60 seconds (Default)
<input type="checkbox"/> SNMP			Up at least 5 min	Yes	Yes	Yes (2)	60 seconds (Default)
▼ Type: Passive Monitor							
<input type="checkbox"/> Domain Time Sync Fail				Yes	Yes		
<input type="checkbox"/> Domain Time Sync Out ...				Yes	Yes		
▼ 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 Availa...				Yes	Yes		10 Minutes
<input type="checkbox"/> VMware Datastore IOPS				No	No		

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](#)

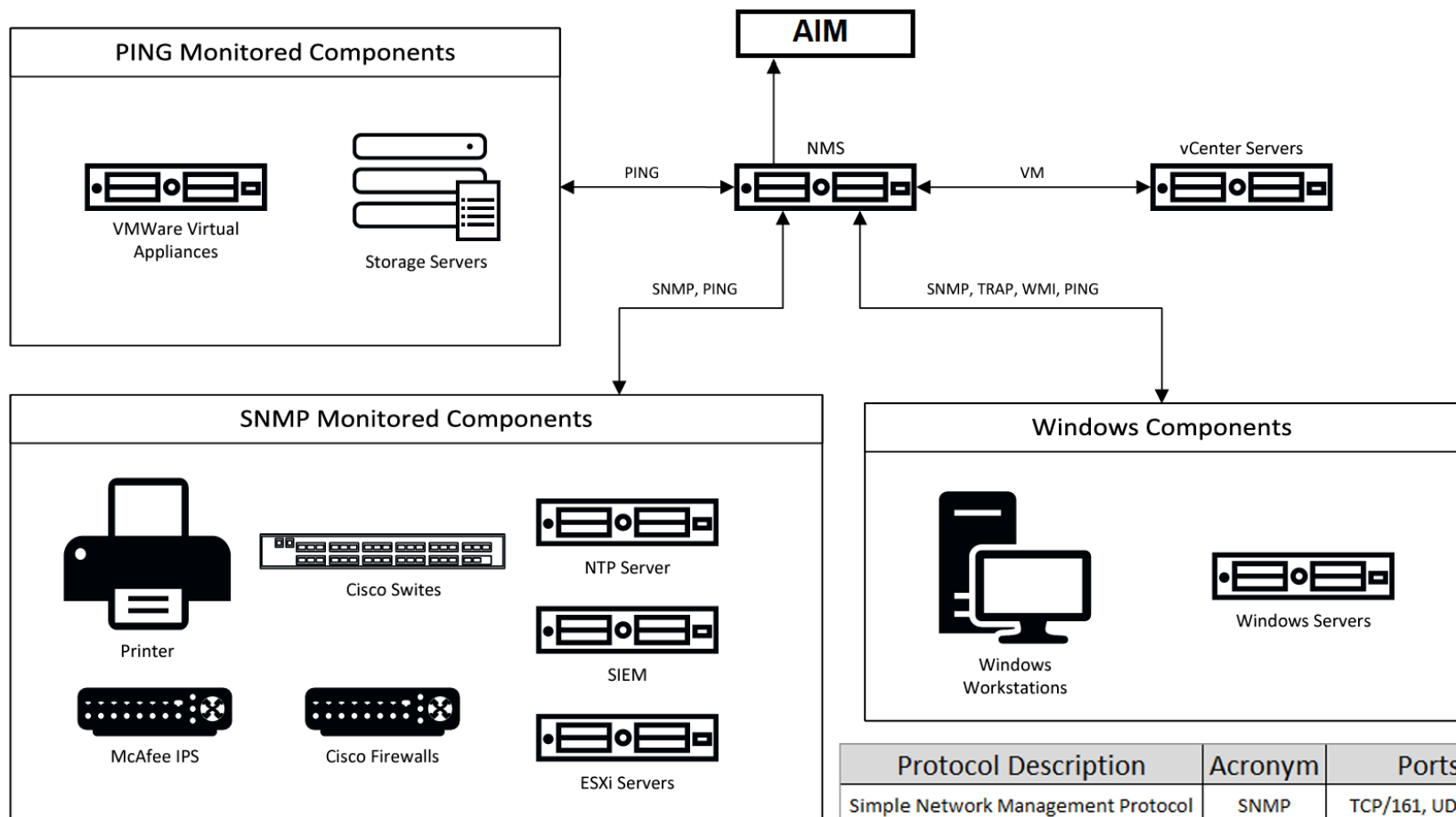
☐ Send to Remedy: [Configure](#)

☐ Assign Tag with ePO: [Configure](#)

☐ Blacklist: [Configure](#)

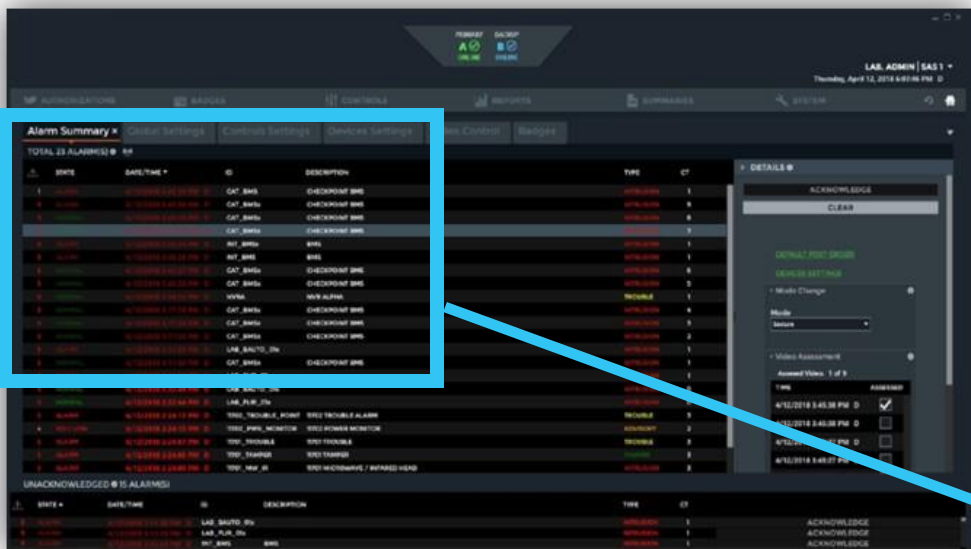
☐ Custom alarm summary: [Configure](#)

[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

AUTHORIZATIONS

BADGES

CONTROLS

Alarm Summary x

Devices Settings

Global Settings

TOTAL 31 ALARM(S)

	STATE	DATE/TIME	D	ID	DESCRIPTION
4	ALARM	5/24/2019 12:39:40 PM	D	SIEM	USB violation on AD-B
4	ALARM	5/24/2019 12:25:39 PM	D	SIEM	Scheduled task modified on MTS-SAS-OP2
4	ALARM	5/24/2019 12:25:19 PM	D	SIEM	USB violation on AD-A
4	ALARM	5/24/2019 12:12:59 PM	D	SIEM	Scheduled task modified on MTS-SAS-OP2
4	ALARM	5/24/2019 12:02:39 PM	D	SIEM	Scheduled task modified on MTS-SAS-OP2
4	ALARM	5/24/2019 11:59:39 AM	D	SIEM	Scheduled task modified on AIM Host Server B
4	ALARM	5/24/2019 11:41:19 AM	D	SIEM	IP address spoofing detected by DMZ Firewall
4	ALARM	5/24/2019 11:38:19 AM	D	SIEM	Antivirus Client was disabled on IEBS-WS1
4	ALARM	5/24/2019 10:57:19 AM	D	SIEM	IP address spoofing detected by DMZ Firewall
4	ALARM	5/24/2019 10:15:39 AM	D	SIEM	Scheduled task modified on MTS-CAS-OP2
4	ALARM	5/24/2019 10:02:19 AM	D	SIEM	Multiple application control violations on cas-op2.aimscs.local
4	ALARM	5/24/2019 9:48:38 AM	D	SIEM	Scheduled task modified on MTS-SAS-OP2
5	ALARM	5/23/2019 4:06:57 PM	D	U3-CAS-PRT.SNMP	SNMP on U3-CAS-PRT is down
4	ALARM	5/22/2019 4:07:21 PM	D	SIEM	IP address spoofing detected by DMZ Firewall

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?

