Real–TimeNonStop Security

Security Monitoring of NonStop Systems

Steve Tcherchian – 2018 Mai

Agenda

- Introduction
- The Problem and Requirements
- The Solution
- Navy Federal Benefits
- Use Cases
- Questions

NAVY FEDERAL Information Services

The Problem

- Inadequate real--time monitoring of suspicious activity.
- Multiple security products.
- Intimate knowledge required to extract value.
- Limited view of security data
- Manual processes are not practical.
- Limited visibility and correlation of data between security solutions.
- Inadequate historical view of trending security events.

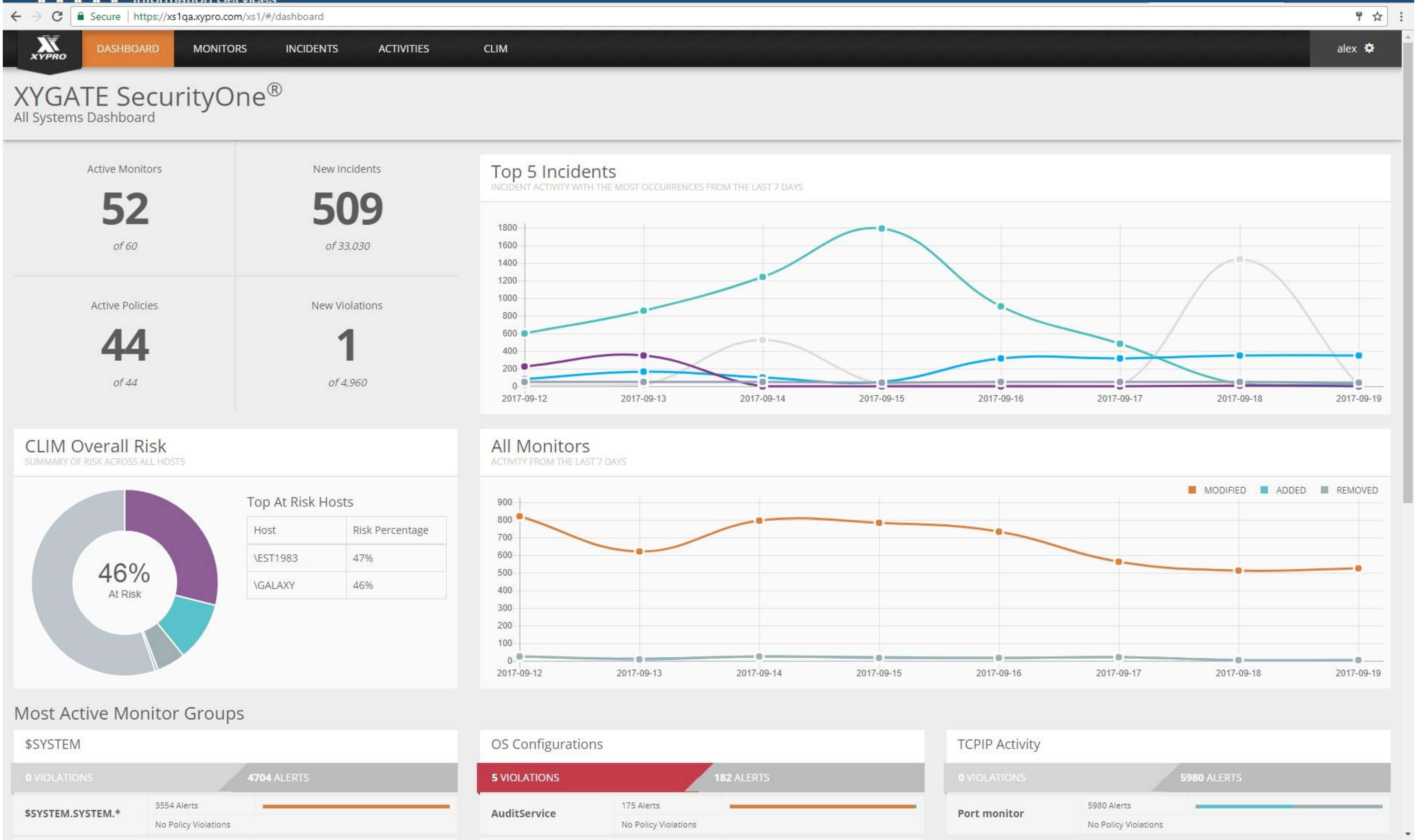
The Ask for a Unified View

- A single console solution for monitoring.
- A single point of access for reporting.
- A single solution for alerting, via text, email or voice.
- Standard messaging.
- Proactive monitoring.
- Historical and trending view of data.
- Quick deployment.

XYGATE SecurityOne

- A single view of NonStop Security.
- A single access point for automated and on demand reporting.
- Customer configurable thresholds and alerting.
- Rules based securityanalysis and reporting.
- Compliance madesimple.

XYGATE SecurityOne



XYGATE SecurityOne®

All Systems Dashboard

Active Monitors	New Incidents
52	**509**
of 60	*of 33,030*

Active Policies	New Violations
44	**1**
of 44	*of 4,960*

Top 5 Incidents

INCIDENT ACTIVITY WITH THE MOST OCCURRENCES FROM THE LAST 7 DAYS

CLIM Overall Risk

SUMMARY OF RISK ACROSS ALL HOSTS

Top At Risk Hosts

Host	Risk Percentage
\EST1983	47%
\GALAXY	46%

All Monitors

ACTIVITY FROM THE LAST 7 DAYS

Most Active Monitor Groups

$SYSTEM

0 VIOLATIONS | 4704 ALERTS

$SYSTEM.SYSTEM.*	3554 Alerts No Policy Violations

OS Configurations

5 VIOLATIONS | 182 ALERTS

AuditService	175 Alerts No Policy Violations

TCPIP Activity

0 VIOLATIONS | 5980 ALERTS

Port monitor	5980 Alerts No Policy Violations

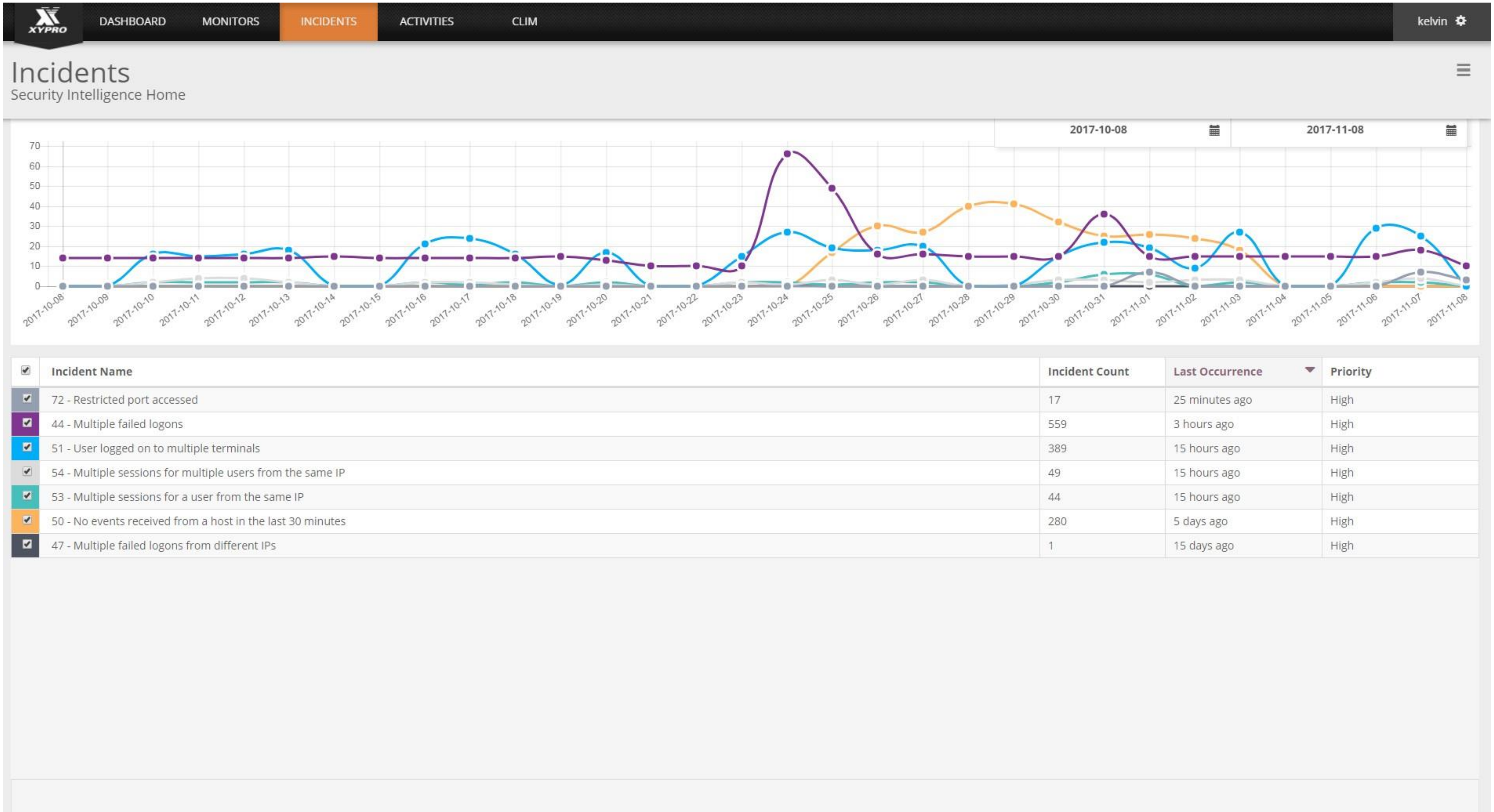
Leverage Existing Technology

- Off–box monitoring of Nonstop.
- Windows server based, but platform agnostic.
- Web based interface with nothing to install on workstations.
- Can combine existing XYPRO solutions to provide a security management console for NonStop.
  - XAC XSM XCM tools installed on same server for single solution point.
- Scalable for disaster recovery/business continuity.
- Easy uptake for Non--NonStop Users.

Benefits to Navy Federal

- Revealed the unknown unknowns and ‘suspicious’ activity.
- Contextualized security incidents.
- Reduction in time to detect and respond to security events.
- Greater ability to do more in less time & limited staff.
- Unified view of the entire NonStop ecosystem.
- Summary/Detail view represents data we need to see without inundating us with what we don’t.
- Utilize information in a proactive and modern way.

Unknown Unknowns



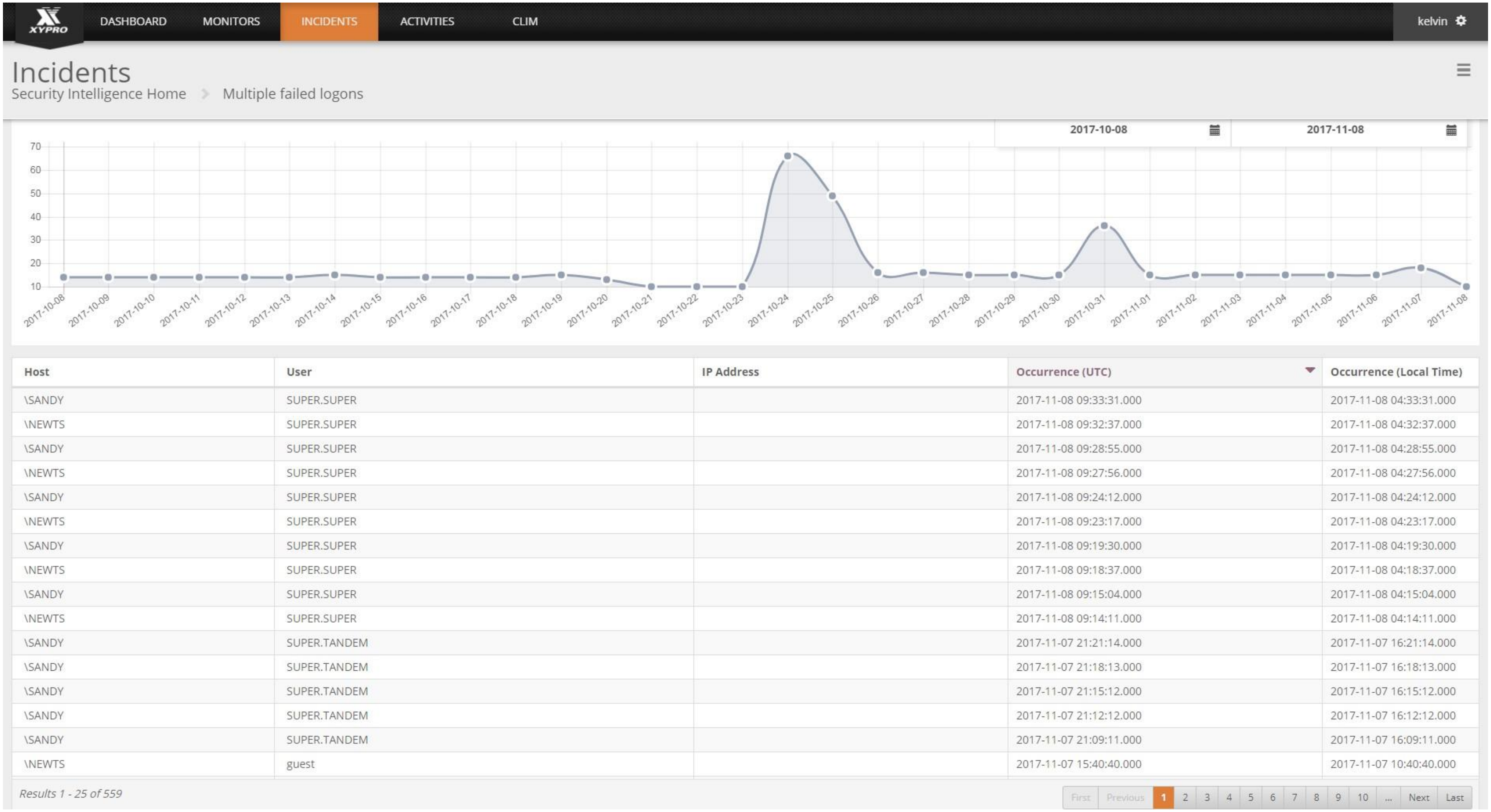
Incidents

Security Intelligence Home

2017-10-08 — 2017-11-08

☑	Incident Name	Incident Count	Last Occurrence	Priority
☑	72 - Restricted port accessed	17	25 minutes ago	High
☑	44 - Multiple failed logons	559	3 hours ago	High
☑	51 - User logged on to multiple terminals	389	15 hours ago	High
☑	54 - Multiple sessions for multiple users from the same IP	49	15 hours ago	High
☑	53 - Multiple sessions for a user from the same IP	44	15 hours ago	High
☑	50 - No events received from a host in the last 30 minutes	280	5 days ago	High
☑	47 - Multiple failed logons from different IPs	1	15 days ago	High

Incident Detail



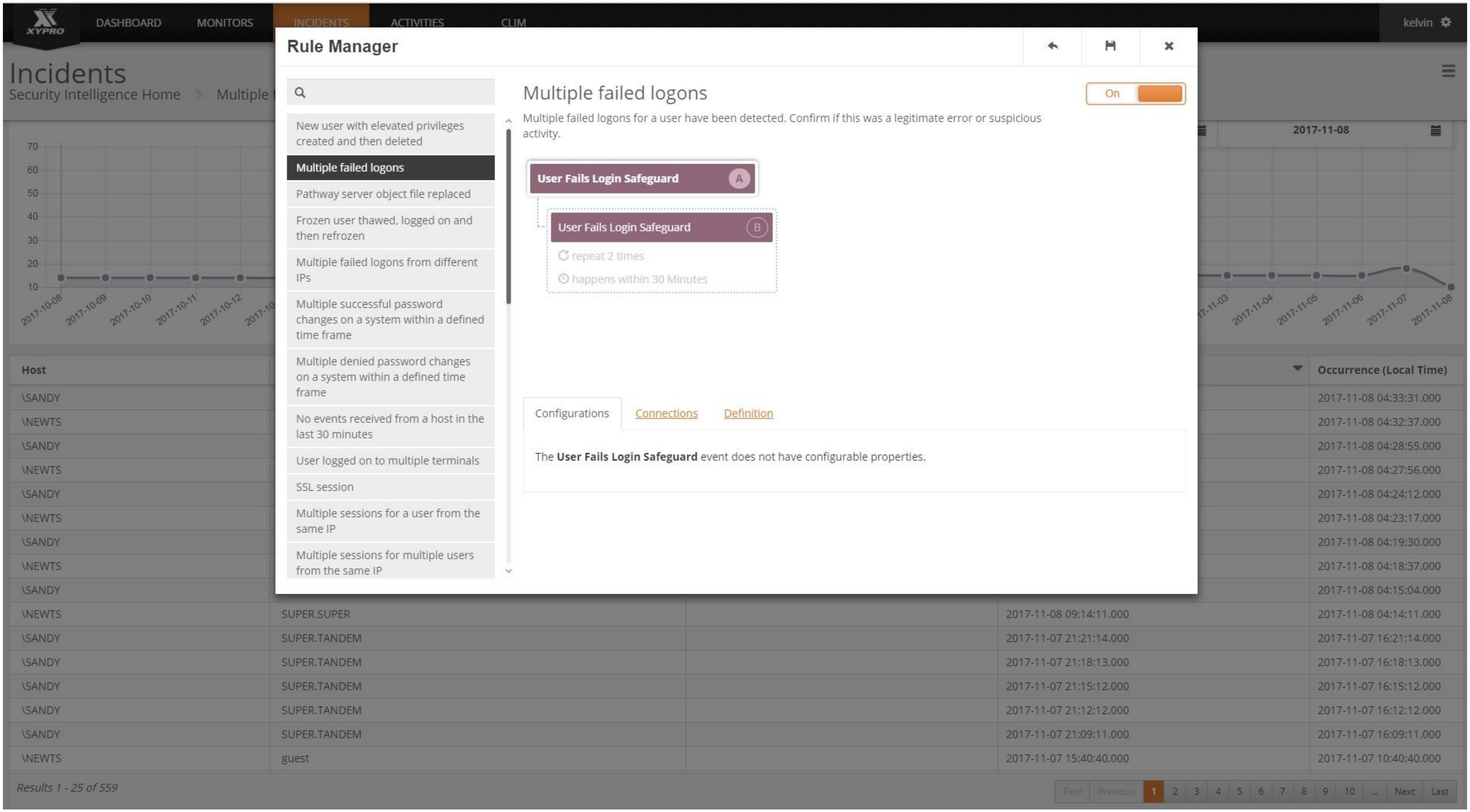
Incidents

Security Intelligence Home > Multiple failed logons

Host	User	IP Address	Occurrence (UTC)	Occurrence (Local Time)
\SANDY	SUPER.SUPER		2017-11-08 09:33:31.000	2017-11-08 04:33:31.000
\NEWTS	SUPER.SUPER		2017-11-08 09:32:37.000	2017-11-08 04:32:37.000
\SANDY	SUPER.SUPER		2017-11-08 09:28:55.000	2017-11-08 04:28:55.000
\NEWTS	SUPER.SUPER		2017-11-08 09:27:56.000	2017-11-08 04:27:56.000
\SANDY	SUPER.SUPER		2017-11-08 09:24:12.000	2017-11-08 04:24:12.000
\NEWTS	SUPER.SUPER		2017-11-08 09:23:17.000	2017-11-08 04:23:17.000
\SANDY	SUPER.SUPER		2017-11-08 09:19:30.000	2017-11-08 04:19:30.000
\NEWTS	SUPER.SUPER		2017-11-08 09:18:37.000	2017-11-08 04:18:37.000
\SANDY	SUPER.SUPER		2017-11-08 09:15:04.000	2017-11-08 04:15:04.000
\NEWTS	SUPER.SUPER		2017-11-08 09:14:11.000	2017-11-08 04:14:11.000
\SANDY	SUPER.TANDEM		2017-11-07 21:21:14.000	2017-11-07 16:21:14.000
\SANDY	SUPER.TANDEM		2017-11-07 21:18:13.000	2017-11-07 16:18:13.000
\SANDY	SUPER.TANDEM		2017-11-07 21:15:12.000	2017-11-07 16:15:12.000
\SANDY	SUPER.TANDEM		2017-11-07 21:12:12.000	2017-11-07 16:12:12.000
\SANDY	SUPER.TANDEM		2017-11-07 21:09:11.000	2017-11-07 16:09:11.000
\NEWTS	guest		2017-11-07 15:40:40.000	2017-11-07 10:40:40.000

Results 1 - 25 of 559

Rule Manager



Incidents

Security Intelligence Home > Multiple f

Rule Manager

- New user with elevated privileges created and then deleted
- **Multiple failed logons**
- Pathway server object file replaced
- Frozen user thawed, logged on and then refrozen
- Multiple failed logons from different IPs
- Multiple successful password changes on a system within a defined time frame
- Multiple denied password changes on a system within a defined time frame
- No events received from a host in the last 30 minutes
- User logged on to multiple terminals
- SSL session
- Multiple sessions for a user from the same IP
- Multiple sessions for multiple users from the same IP

Multiple failed logons

On

Multiple failed logons for a user have been detected. Confirm if this was a legitimate error or suspicious activity.

User Fails Login Safeguard A
User Fails Login Safeguard B
repeat 2 times
happens within 30 Minutes

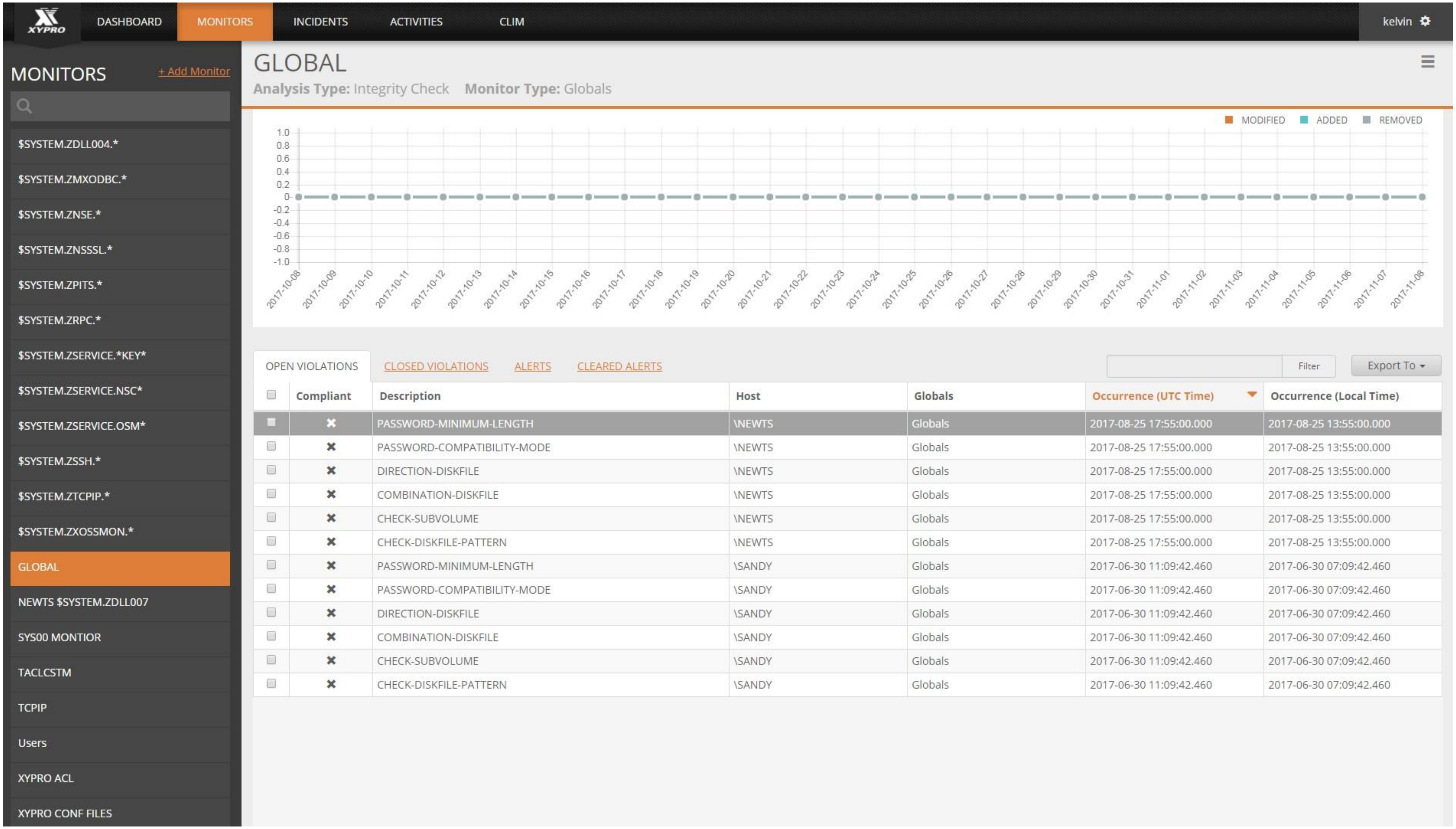
Configurations | Connections | Definition

The **User Fails Login Safeguard** event does not have configurable properties.

Host				Occurrence (Local Time)
\SANDY				2017-11-08 04:33:31.000
\NEWTS				2017-11-08 04:32:37.000
\SANDY				2017-11-08 04:28:55.000
\NEWTS				2017-11-08 04:27:56.000
\SANDY				2017-11-08 04:24:12.000
\NEWTS				2017-11-08 04:23:17.000
\SANDY				2017-11-08 04:19:30.000
\NEWTS				2017-11-08 04:18:37.000
\SANDY				2017-11-08 04:15:04.000
\NEWTS	SUPER.SUPER		2017-11-08 09:14:11.000	2017-11-08 04:14:11.000
\SANDY	SUPER.TANDEM		2017-11-07 21:21:14.000	2017-11-07 16:21:14.000
\SANDY	SUPER.TANDEM		2017-11-07 21:18:13.000	2017-11-07 16:18:13.000
\SANDY	SUPER.TANDEM		2017-11-07 21:15:12.000	2017-11-07 16:15:12.000
\SANDY	SUPER.TANDEM		2017-11-07 21:12:12.000	2017-11-07 16:12:12.000
\SANDY	SUPER.TANDEM		2017-11-07 21:09:11.000	2017-11-07 16:09:11.000
\NEWTS	guest		2017-11-07 15:40:40.000	2017-11-07 10:40:40.000

Results 1 - 25 of 559

The Navy Federal Experience

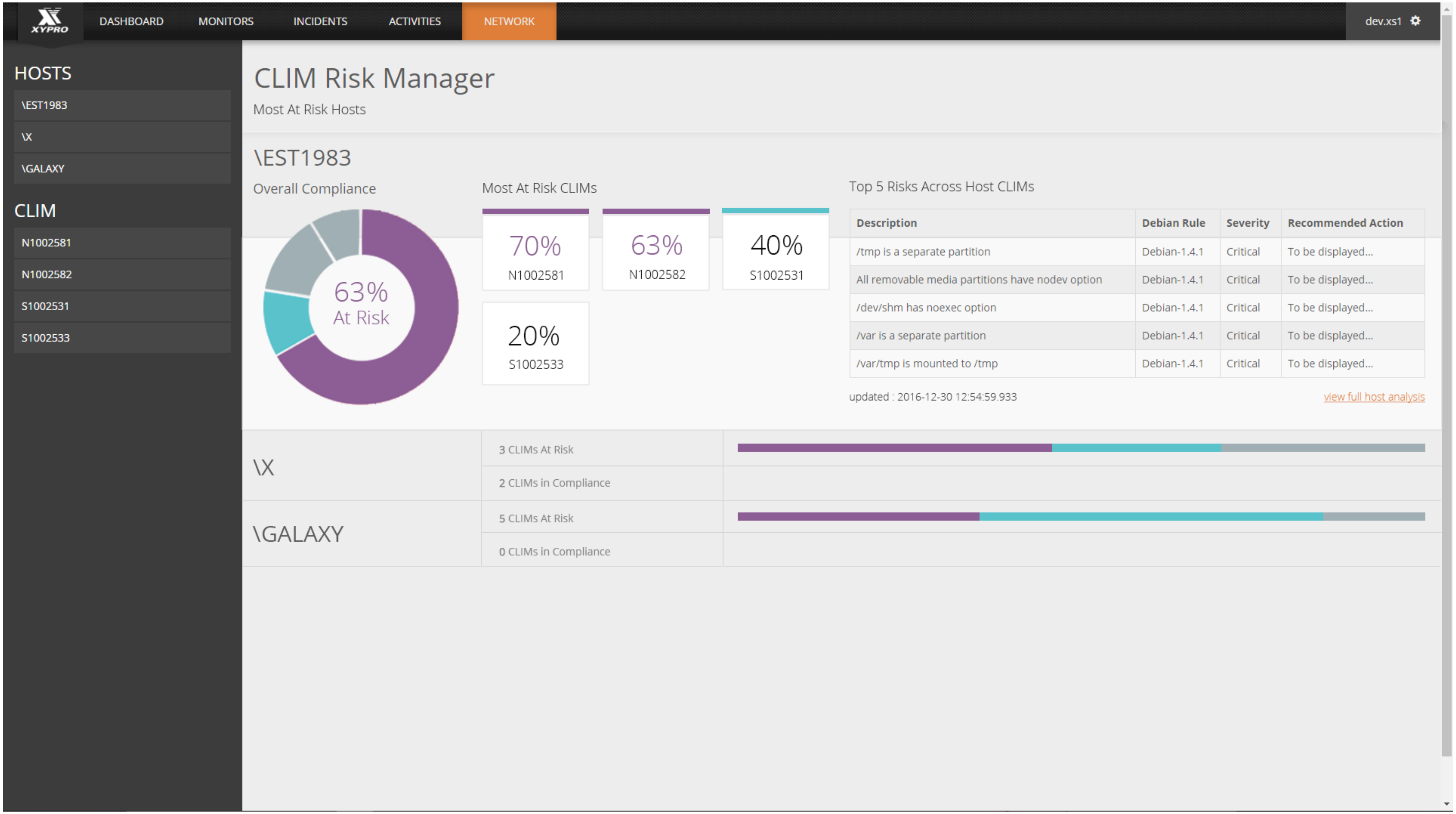


GLOBAL

Analysis Type: Integrity Check **Monitor Type:** Globals

☐	Compliant	Description	Host	Globals	Occurrence (UTC Time)	Occurrence (Local Time)
☐	✖	PASSWORD-MINIMUM-LENGTH	\NEWTS	Globals	2017-08-25 17:55:00.000	2017-08-25 13:55:00.000
☐	✖	PASSWORD-COMPATIBILITY-MODE	\NEWTS	Globals	2017-08-25 17:55:00.000	2017-08-25 13:55:00.000
☐	✖	DIRECTION-DISKFILE	\NEWTS	Globals	2017-08-25 17:55:00.000	2017-08-25 13:55:00.000
☐	✖	COMBINATION-DISKFILE	\NEWTS	Globals	2017-08-25 17:55:00.000	2017-08-25 13:55:00.000
☐	✖	CHECK-SUBVOLUME	\NEWTS	Globals	2017-08-25 17:55:00.000	2017-08-25 13:55:00.000
☐	✖	CHECK-DISKFILE-PATTERN	\NEWTS	Globals	2017-08-25 17:55:00.000	2017-08-25 13:55:00.000
☐	✖	PASSWORD-MINIMUM-LENGTH	\SANDY	Globals	2017-06-30 11:09:42.460	2017-06-30 07:09:42.460
☐	✖	PASSWORD-COMPATIBILITY-MODE	\SANDY	Globals	2017-06-30 11:09:42.460	2017-06-30 07:09:42.460
☐	✖	DIRECTION-DISKFILE	\SANDY	Globals	2017-06-30 11:09:42.460	2017-06-30 07:09:42.460
☐	✖	COMBINATION-DISKFILE	\SANDY	Globals	2017-06-30 11:09:42.460	2017-06-30 07:09:42.460
☐	✖	CHECK-SUBVOLUME	\SANDY	Globals	2017-06-30 11:09:42.460	2017-06-30 07:09:42.460
☐	✖	CHECK-DISKFILE-PATTERN	\SANDY	Globals	2017-06-30 11:09:42.460	2017-06-30 07:09:42.460

CLIM Monitoring



CLIM Risk Manager

Most At Risk Hosts

\EST1983

Overall Compliance

Most At Risk CLIMs

70%	N1002581
63%	N1002582
40%	S1002531
20%	S1002533

Top 5 Risks Across Host CLIMs

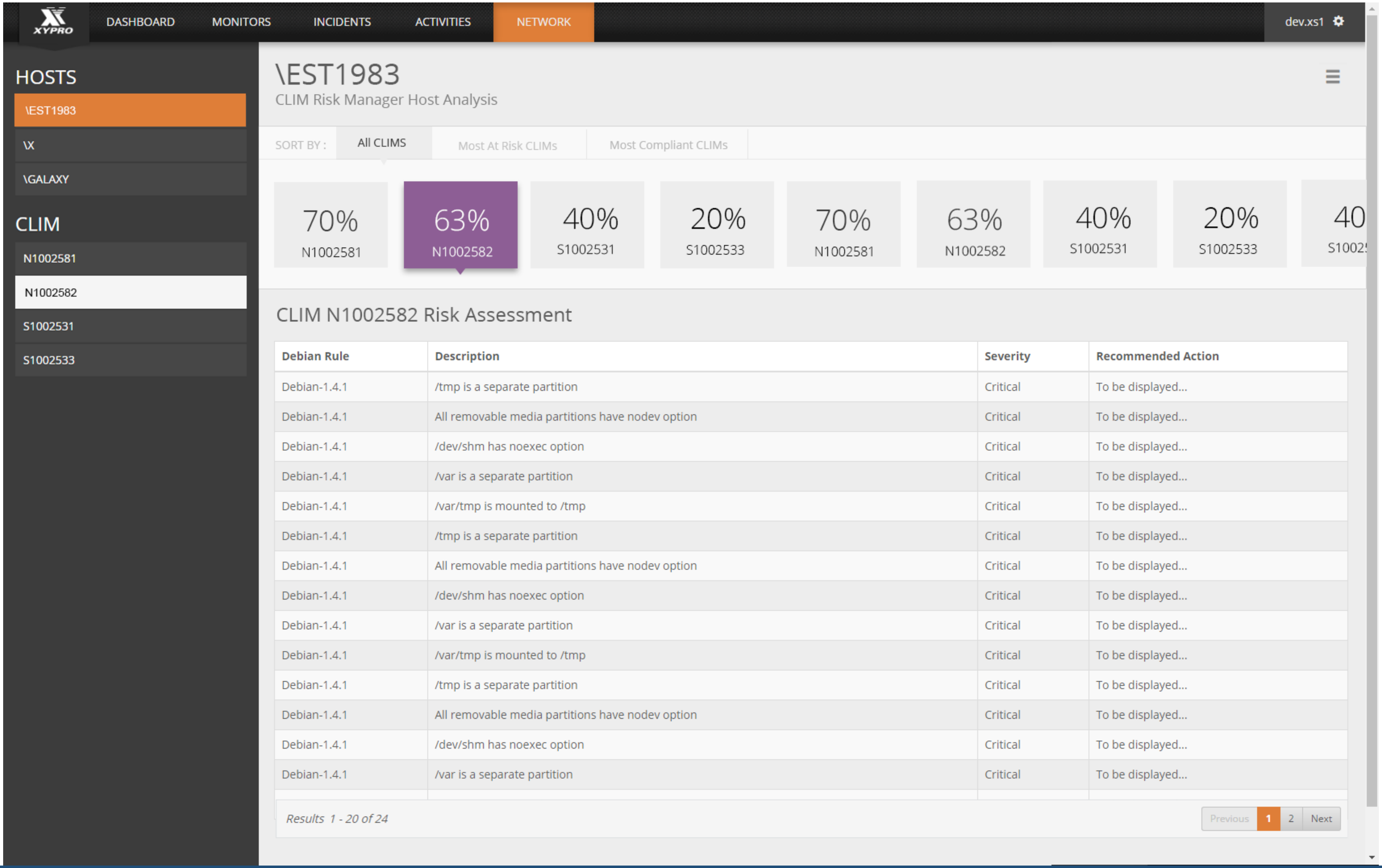
Description	Debian Rule	Severity	Recommended Action
/tmp is a separate partition	Debian-1.4.1	Critical	To be displayed...
All removable media partitions have nodev option	Debian-1.4.1	Critical	To be displayed...
/dev/shm has noexec option	Debian-1.4.1	Critical	To be displayed...
/var is a separate partition	Debian-1.4.1	Critical	To be displayed...
/var/tmp is mounted to /tmp	Debian-1.4.1	Critical	To be displayed...

updated : 2016-12-30 12:54:59.933

view full host analysis

\X	3 CLIMs At Risk 2 CLIMs in Compliance
\GALAXY	5 CLIMs At Risk 0 CLIMs in Compliance

CLIM Monitoring



\EST1983

CLIM Risk Manager Host Analysis

CLIM N1002582 Risk Assessment

Debian Rule	Description	Severity	Recommended Action
Debian-1.4.1	/tmp is a separate partition	Critical	To be displayed...
Debian-1.4.1	All removable media partitions have nodev option	Critical	To be displayed...
Debian-1.4.1	/dev/shm has noexec option	Critical	To be displayed...
Debian-1.4.1	/var is a separate partition	Critical	To be displayed...
Debian-1.4.1	/var/tmp is mounted to /tmp	Critical	To be displayed...
Debian-1.4.1	/tmp is a separate partition	Critical	To be displayed...
Debian-1.4.1	All removable media partitions have nodev option	Critical	To be displayed...
Debian-1.4.1	/dev/shm has noexec option	Critical	To be displayed...
Debian-1.4.1	/var is a separate partition	Critical	To be displayed...
Debian-1.4.1	/var/tmp is mounted to /tmp	Critical	To be displayed...
Debian-1.4.1	/tmp is a separate partition	Critical	To be displayed...
Debian-1.4.1	All removable media partitions have nodev option	Critical	To be displayed...
Debian-1.4.1	/dev/shm has noexec option	Critical	To be displayed...
Debian-1.4.1	/var is a separate partition	Critical	To be displayed...

Results 1 - 20 of 24

The Navy Federal Experience

- Detection of suspicious activity in our environment with actionable feedback
- CLIM monitoring to identify risks and weakness
- User activity monitoring including network info, meaningful context.
- Password Violations.
- Violations from Multiple IP Addresses.
- Compliance Alerting, are we out of compliance?

Our Experience at Navy Federal

- Familiar interface for non--NonStop Security Managers.
- GUI driven management of users/ACLs/objects.
- Rules for alerting configurable for installation.
- Historical Trending of events.
- Reporting to data warehouse or SIEM Server.
- Single view of NonStop security events across all systems.

QUESTIONS?