IT NATION™ SECURE

hosted by CONNECTWISE

Cybersecurity

Simply SIEM

IT NATION™ SECURE

Rob DeBok (DeeeeeBok)

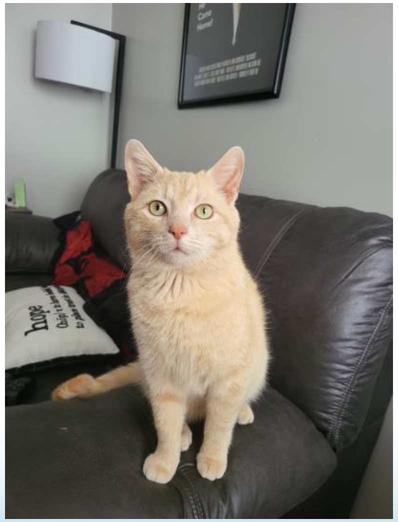
Software Training Consultant

- 9 years with ConnectWise
- Love cats
- Upcycle/repurpose
- Love helping partners

Bryan Pasquale

Security Solutions Architect

- 11 years experience in cybersecurity
- Former SIEM engineer
- GCIA, GSEC, Security+
- Also owns a cat



Agenda

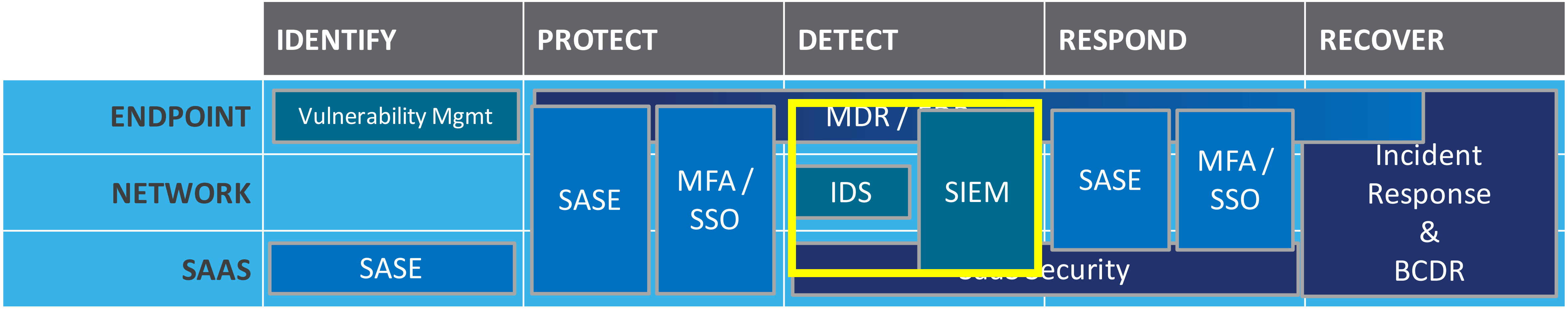
- What is security information and event management (SIEM)?
- Security Operations Center (SOC) for Co-managed SIEM
- SIEM Components
- Communities, indicators, alerts, and notifications

Simply SIEM

What is a SIEM?

IT NATION™ SECURE

ConnectWise Cybersecurity Ecosystem



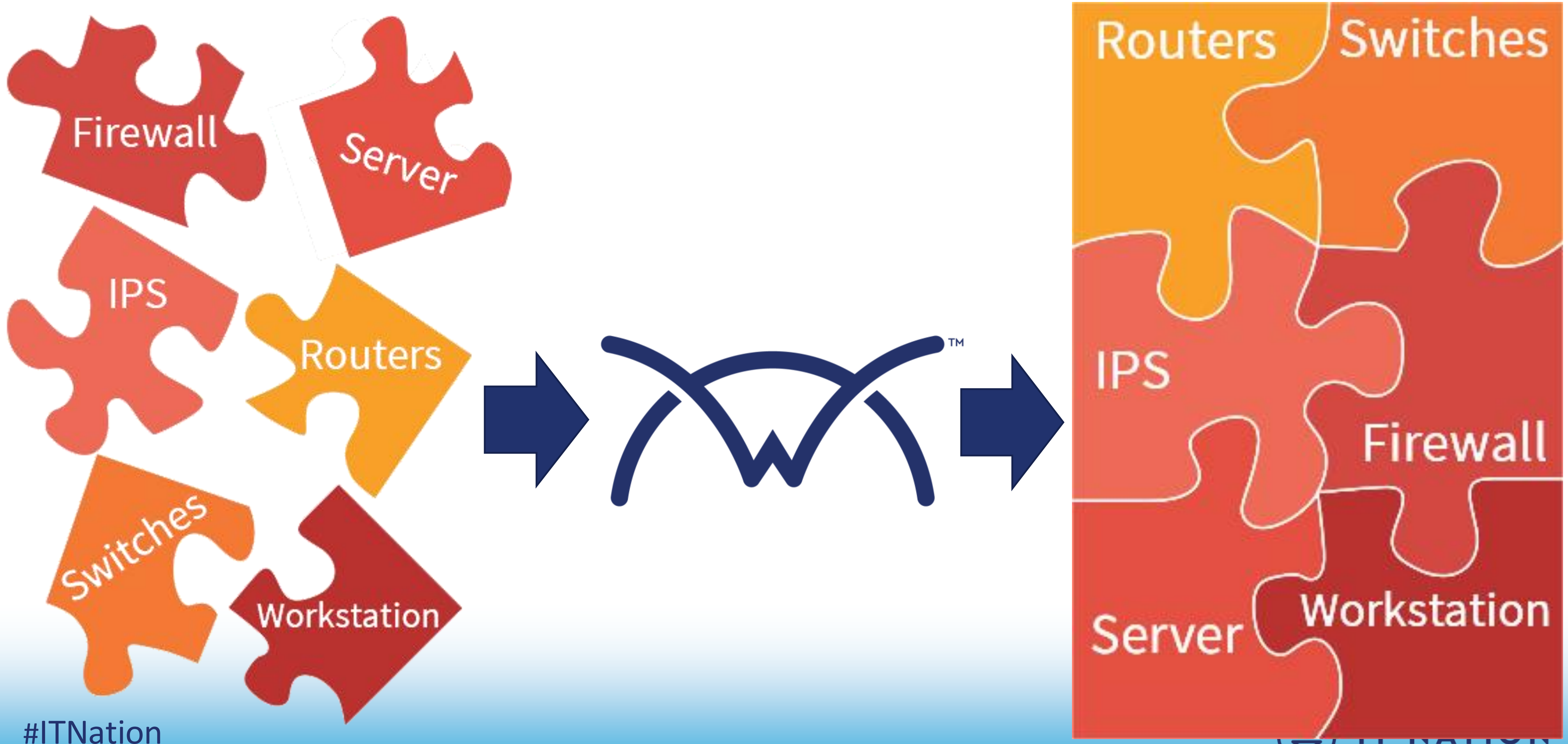
■ ConnectWise Products

■ ConnectWise Integrated Expert Services

■ Third-Party, Strategic Resold Products

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
FRAMEWORK

What is a SIEM?



What is a SIEM, and why do I need it?

Security information and event management

- A SIEM works by collecting log and event data generated by an organization's systems, devices, and applications and brings them into the centralized platform for analysis and reporting.
- When the SIEM identifies a threat through a set of predetermined rules, an alert is generated for human review.

- Auditing and compliance requirements
- Full visibility of everything happening within the network
- Dramatically decreases the time it takes to identify threats
- Detailed forensic analysis in the event of major security breaches

What sets ConnectWise SIEM apart

Predictable Subscription Model

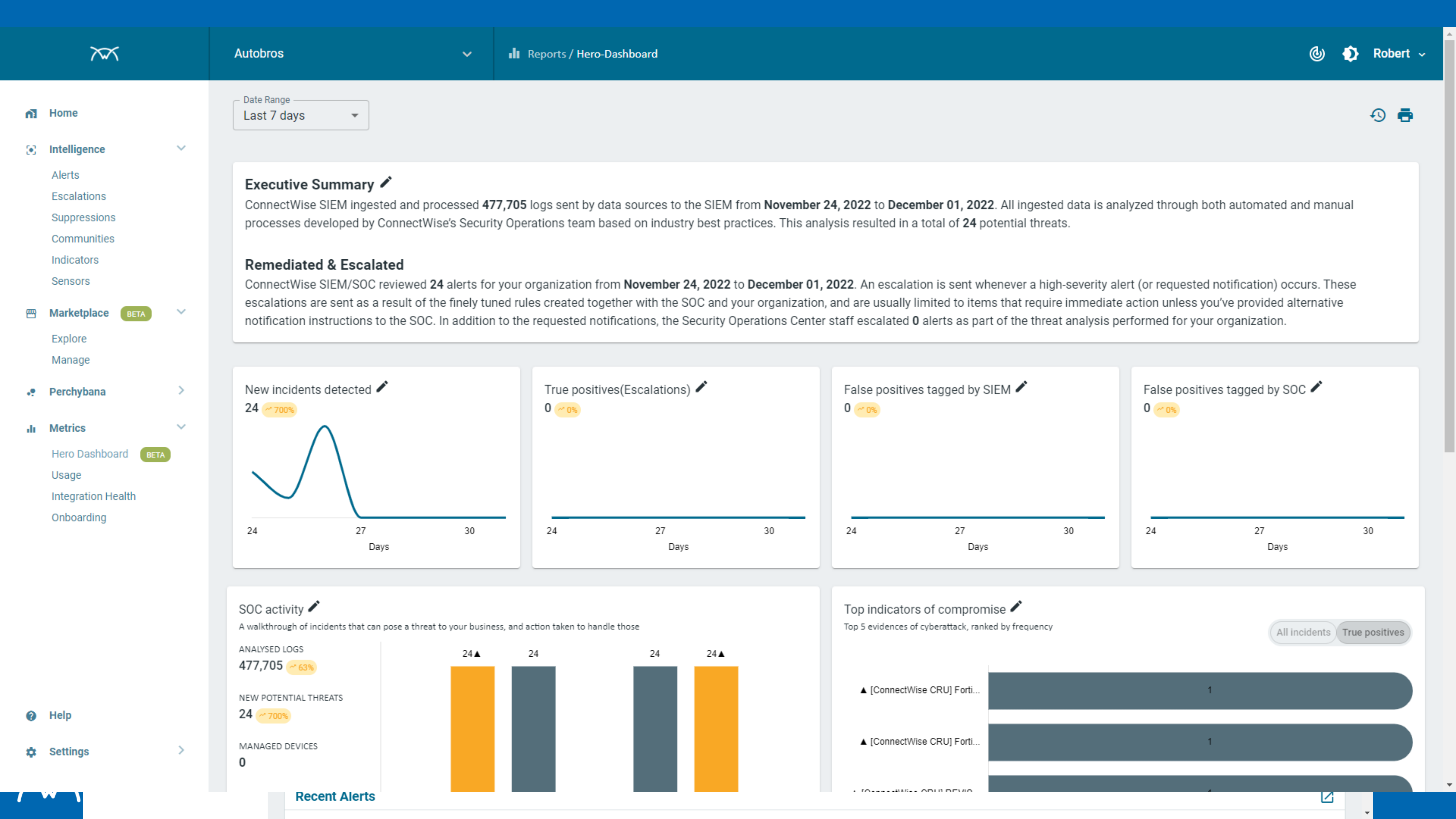
- Easy user-based, with option on SLO and data retention
    - No need to count devices or worry about ingestion rates
- Includes virtual IDS appliances

It’s an MSP Platform

- Multi-tenant
    - Each customer can have their own alerts and dashboards
- Templated dashboarding and alerts

Backed by ConnectWise SOC Services

- Certified threat analysts do the heavy lifting for users
    - Act alone or with your analysts (co-managed)
    - White-labeled, we will never reach out to your customer directly
- Our SOC tunes out all the noise, allowing you to focus on your customer and the real threats



Date Range
Last 7 days

Executive Summary

ConnectWise SIEM ingested and processed **477,705** logs sent by data sources to the SIEM from **November 24, 2022** to **December 01, 2022**. All ingested data is analyzed through both automated and manual processes developed by ConnectWise's Security Operations team based on industry best practices. This analysis resulted in a total of **24** potential threats.

Remediated & Escalated

ConnectWise SIEM/SOC reviewed **24** alerts for your organization from **November 24, 2022** to **December 01, 2022**. An escalation is sent whenever a high-severity alert (or requested notification) occurs. These escalations are sent as a result of the finely tuned rules created together with the SOC and your organization, and are usually limited to items that require immediate action unless you've provided alternative notification instructions to the SOC. In addition to the requested notifications, the Security Operations Center staff escalated **0** alerts as part of the threat analysis performed for your organization.

New incidents detected
24 700%

True positives(Escalations)
0 0%

False positives tagged by SIEM
0 0%

False positives tagged by SOC
0 0%

SOC activity

A walkthrough of incidents that can pose a threat to your business, and action taken to handle those

ANALYSED LOGS
477,705 63%

NEW POTENTIAL THREATS
24 700%

MANAGED DEVICES
0

Top indicators of compromise

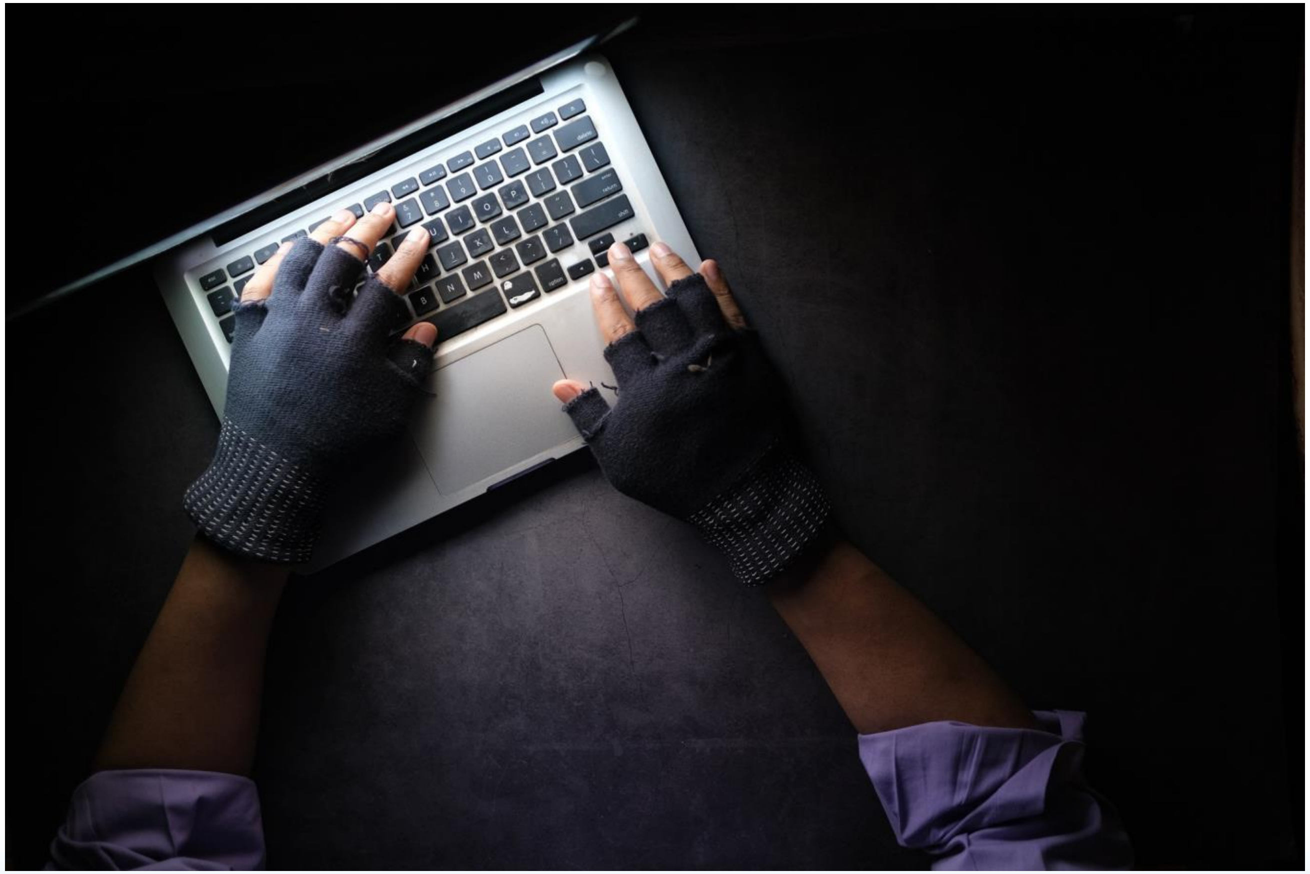
Top 5 evidences of cyberattack, ranked by frequency

Recent Alerts

Why SIEM?

Use case:
A breach occurs and during forensics, all logs are requested to determine impact. The attackers made sure to delete and/or encrypt logs on devices to cover their tracks. This could increase fines and the worst would have to be assumed when determining impact to report.

Solution:
SIEM records all of this data and holds it in the cloud for full forensics after an event. This information is used to determine precise impact to everyone and everything, so the worst is not just assumed in the aftermath. This reduces total damages from the incident in many ways.



Simply SIEM

Co-managed SIEM

IT NATION™ SECURE

And another thing!

When co-managed by ConnectWise SOC (security operations center), response to initial events can significantly reduce the impact attackers have. Even thwarting efforts to get their payloads deployed!

What is a SOC?

A team dedicated to:

- Security monitoring
- Threat intelligence
- Incident response
- Vulnerability management
- Compliance

ConnectWise SOC

- Accelerate your practice
- Avoid expensive costs
- 24/7/365 monitoring and response

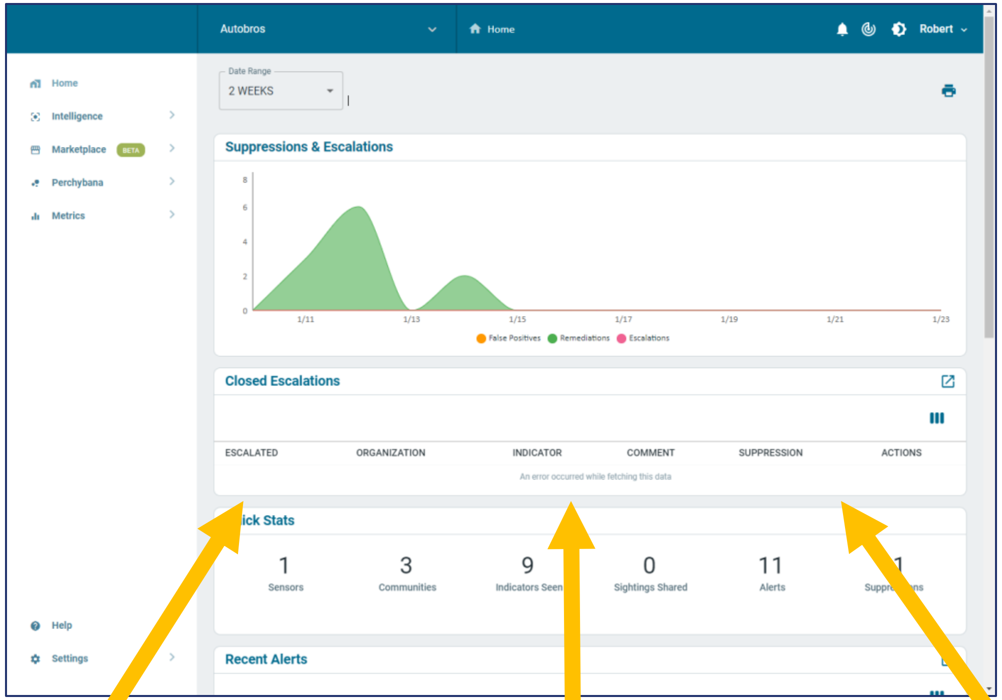
Simply SIEM

SIEM Components

IT NATION™ SECURE

Components for the SIEM

- SIEM app (web)
- Sensors
- Log shipper
- Integrations



Date Range
2 WEEKS

Suppressions & Escalations

Closed Escalations

ESCALATED	ORGANIZATION	INDICATOR	COMMENT	SUPPRESSION	ACTIONS

An error occurred while fetching this data

ick Stats

1	3	9	0	11	1
Sensors	Communities	Indicators Seen	Sightings Shared	Alerts	Suppre ns

Recent Alerts

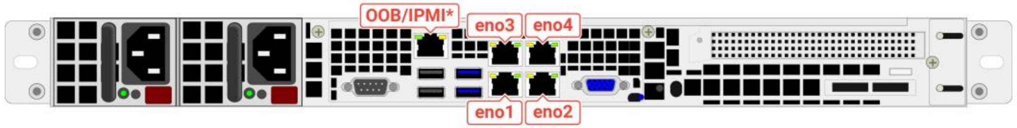
Sensors

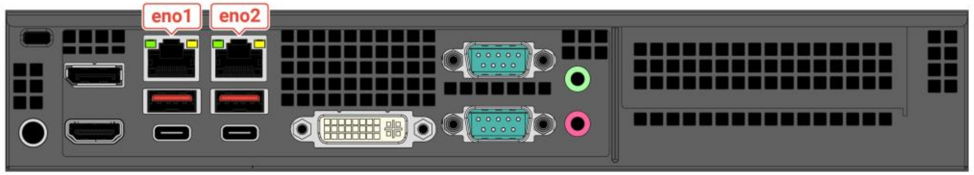
Physical Sensors

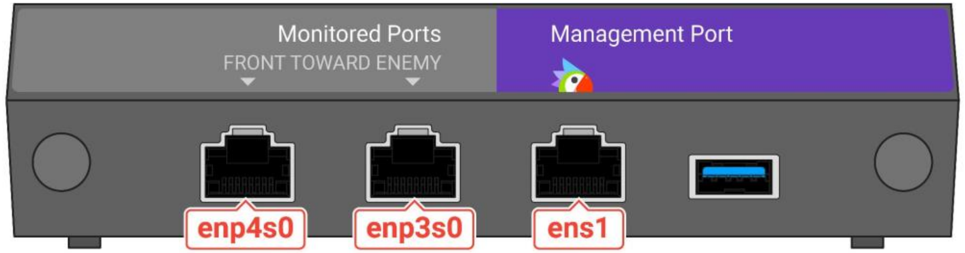
- 1U
- 2U
- Small form factor (SFF)
- Tiny form factor (TFF)

Virtual

- vSphere/ESXi
- Virtualbox
- Hyper-V

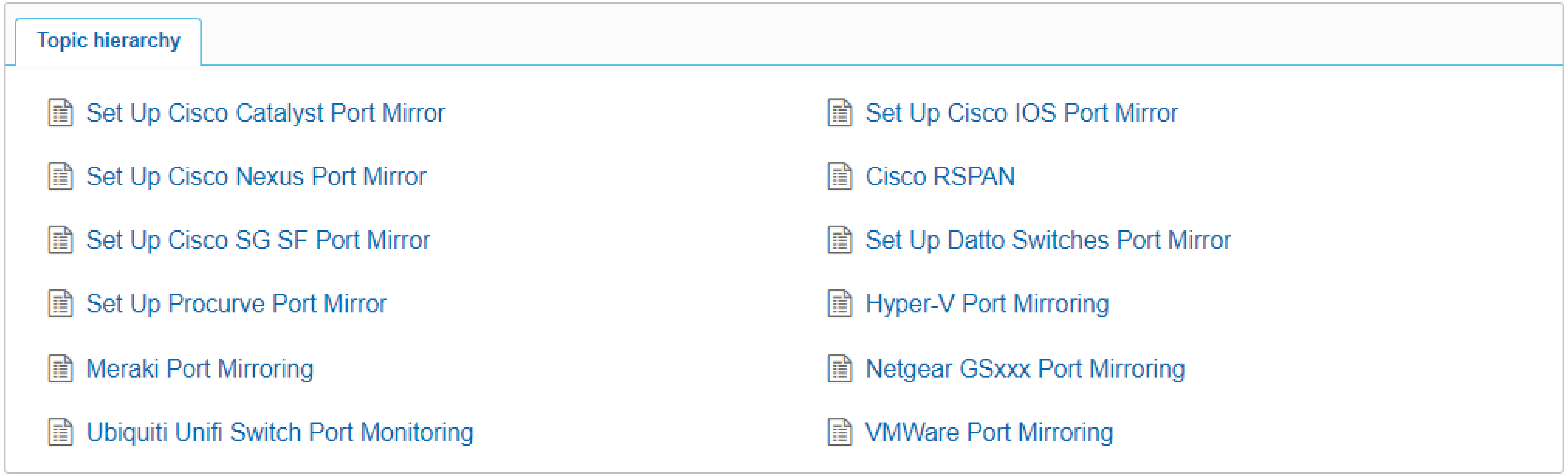






#ITNation

Port Mirroring Documentation



Topic hierarchy

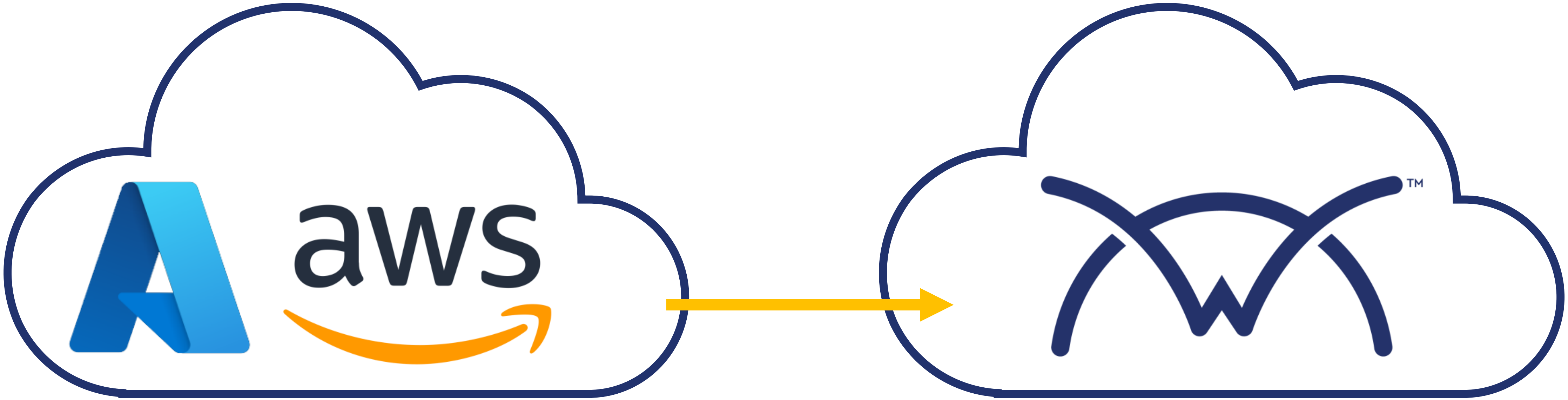
- Set Up Cisco Catalyst Port Mirror
- Set Up Cisco Nexus Port Mirror
- Set Up Cisco SG SF Port Mirror
- Set Up Procurve Port Mirror
- Meraki Port Mirroring
- Ubiquiti Unifi Switch Port Monitoring
- Set Up Cisco IOS Port Mirror
- Cisco RSPAN
- Set Up Datto Switches Port Mirror
- Hyper-V Port Mirroring
- Netgear GSxxx Port Mirroring
- VMWare Port Mirroring

https://docs.connectwise.com/SIEM/Mirroring

Virtual Sensors

- 2 Network cards/virtual switches
- VMWare: Enable promiscuous mode and mirror
- Hyper-V: Enable NDIS capture and run PS code to enable VM for mirror

Cloud Sensors



Log Shipper

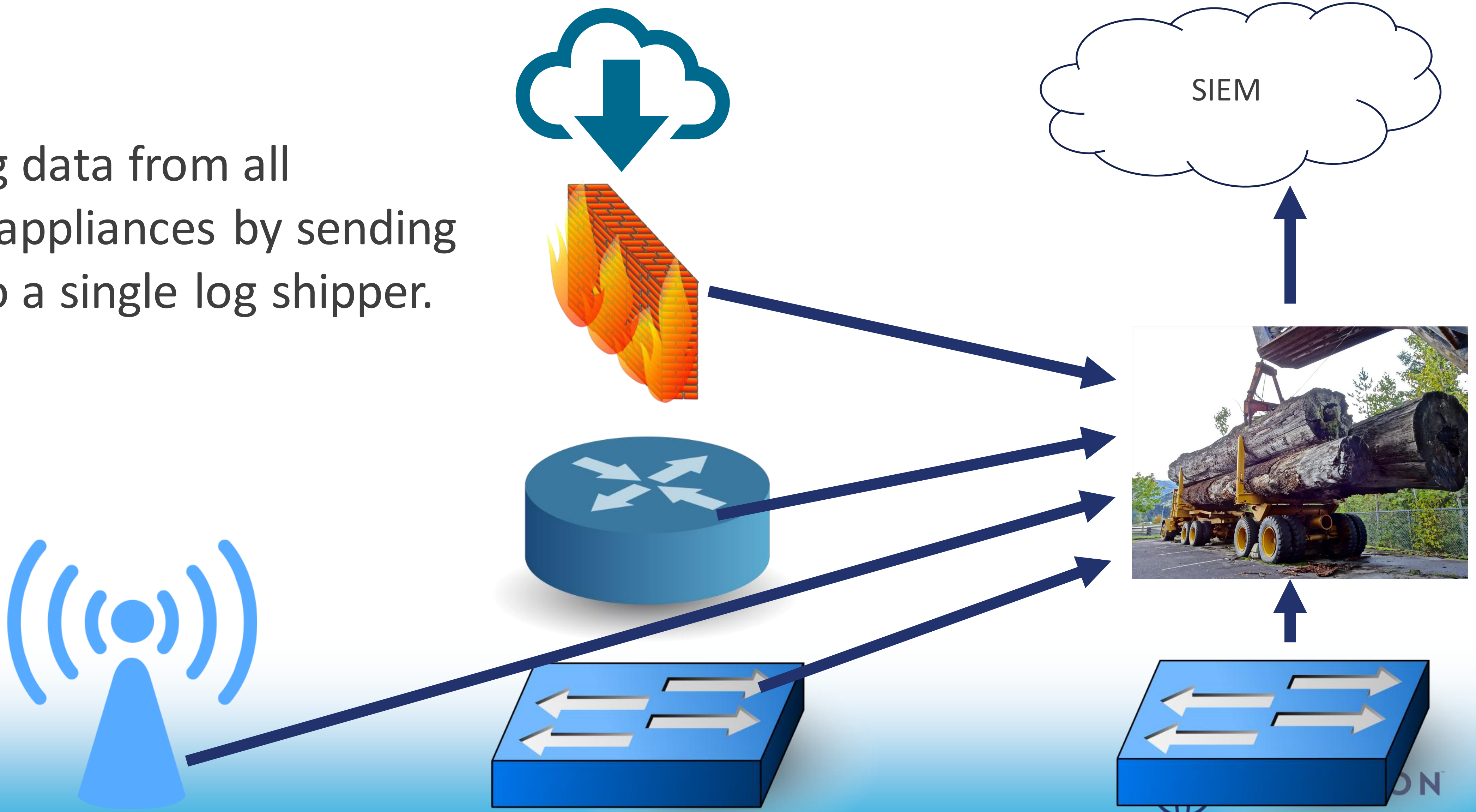
Winlogbeat: Sends your Windows event logs for processing and storage

Auditbeat: Sends audit data from the endpoint for processing and storage

Sysmon: A free utility from
Microsoft Sysinternals groups that provides
a higher fidelity of insight into how your
Windows systems are operating

Syslog Aggregation and Ingestion

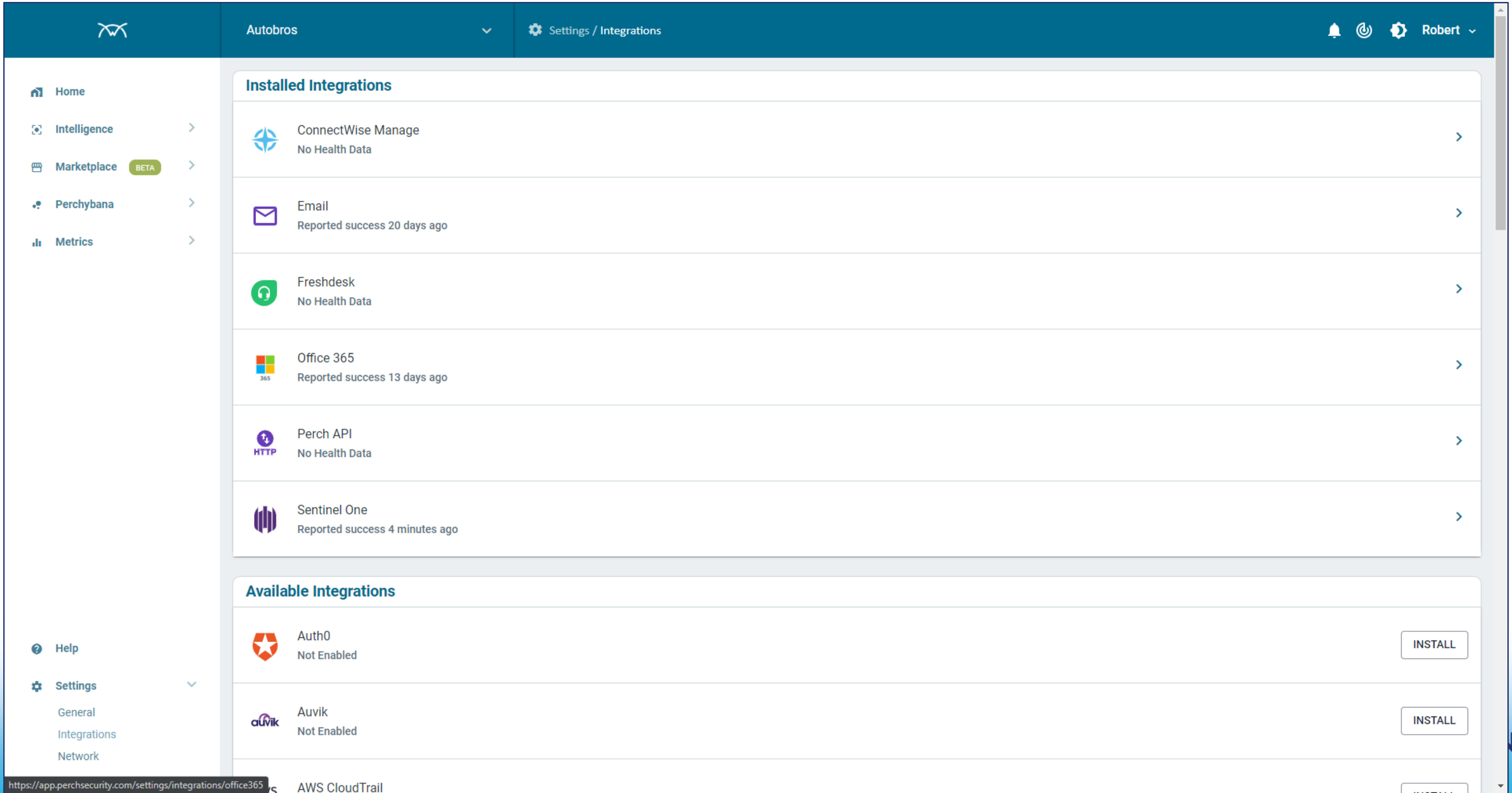
Ingest log data from all network appliances by sending syslogs to a single log shipper.



Integrations

- ConnectWise PSA
- ConnectWise Automate
- ConnectWise ScreenConnect
- SentinelOne
- Bitdefender
- Google Workspaces
- Office 365

Integrations:



Installed Integrations

ConnectWise Manage
No Health Data

Email
Reported success 20 days ago

Freshdesk
No Health Data

Office 365
Reported success 13 days ago

Perch API
No Health Data

Sentinel One
Reported success 4 minutes ago

Available Integrations

Auth0
Not Enabled
INSTALL

Auvik
Not Enabled
INSTALL

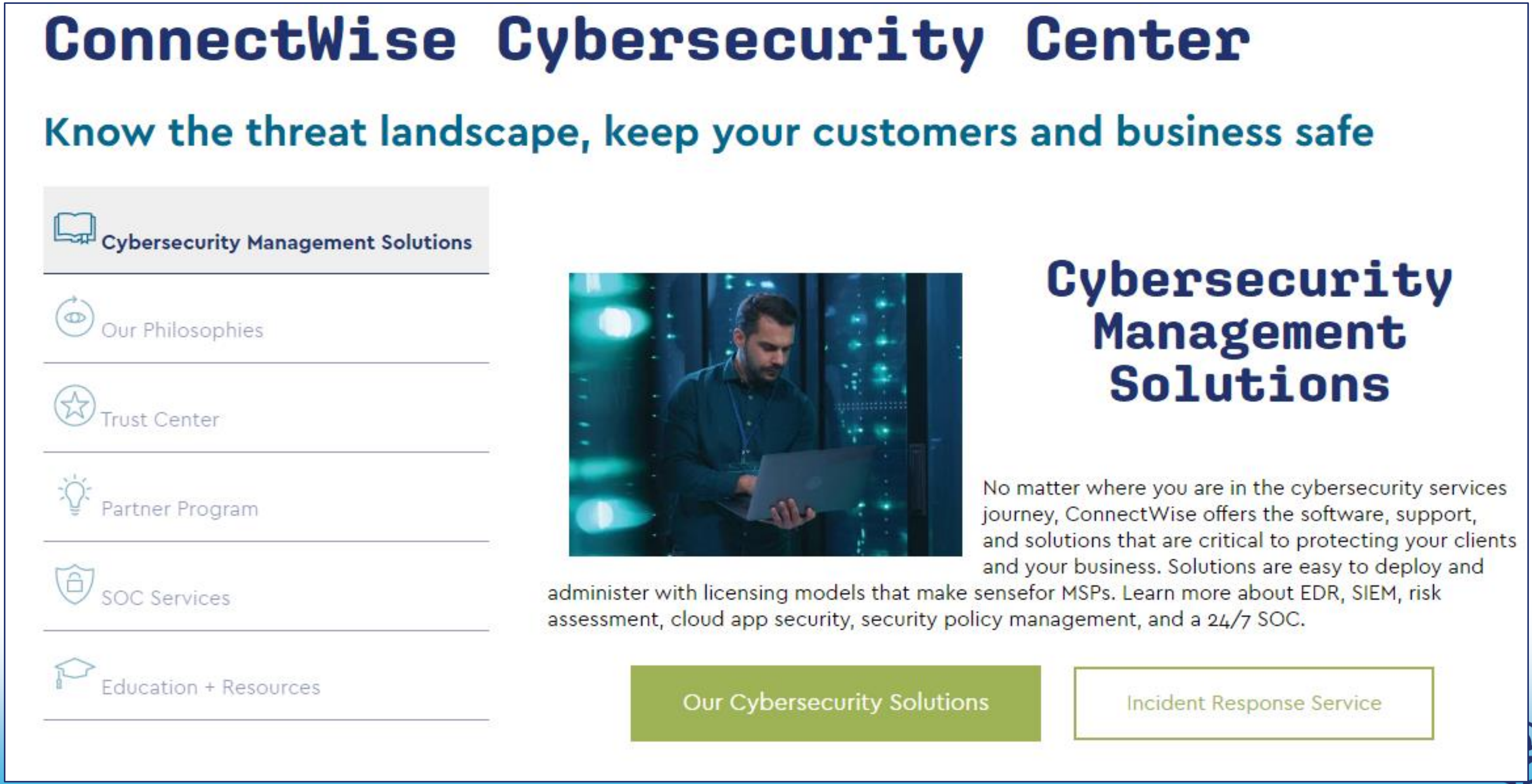
AWS CloudTrail

Simply SIEM

Wrap-up

IT NATION™ SECURE

ConnectWise Cybersecurity Center



ConnectWise Cybersecurity Center

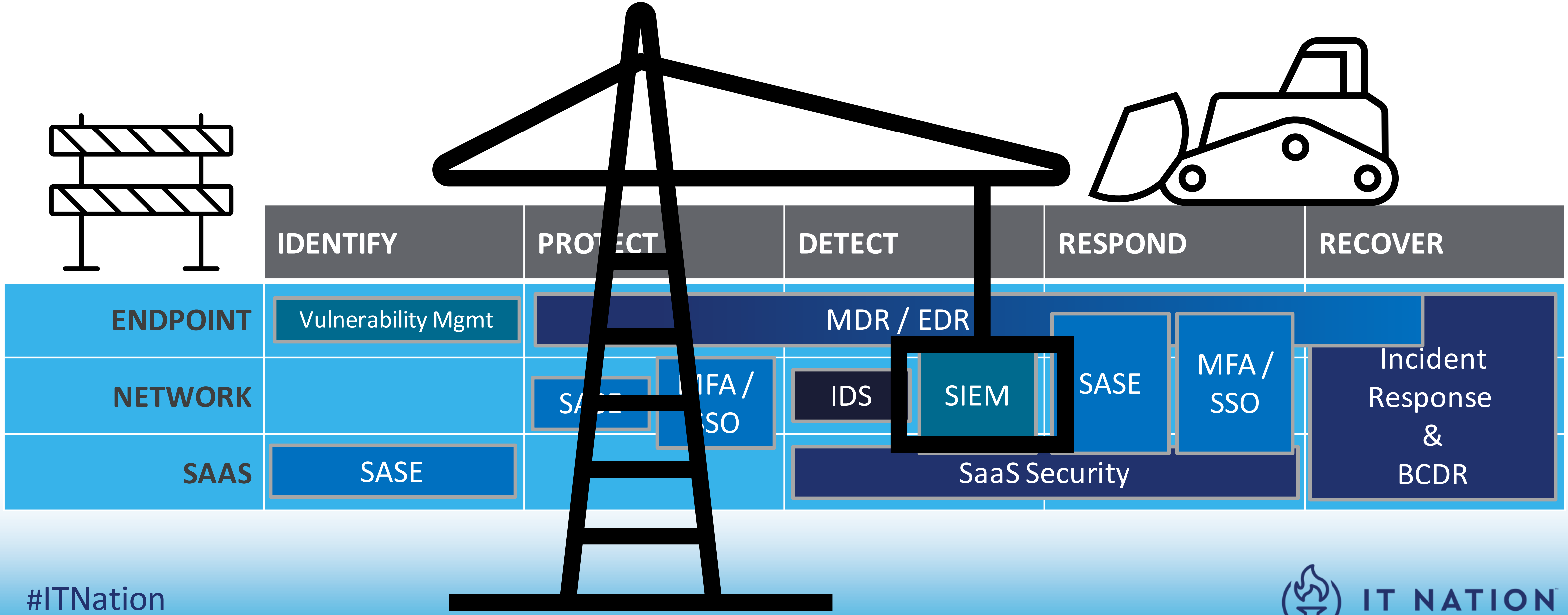
Know the threat landscape, keep your customers and business safe

Cybersecurity Management Solutions

No matter where you are in the cybersecurity services journey, ConnectWise offers the software, support, and solutions that are critical to protecting your clients and your business. Solutions are easy to deploy and administer with licensing models that make sensefor MSPs. Learn more about EDR, SIEM, risk assessment, cloud app security, security policy management, and a 24/7 SOC.

ConnectWise Partner Program

Let us help you build the stack!



IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

ENDPOINT

NETWORK

SAAS

Vulnerability Mgmt

MDR / EDR

SASE

MFA / SSO

IDS

SIEM

SASE

MFA / SSO

Incident Response & BCDR

SASE

SaaS Security

ConnectWise Partner Program

REGISTERED PARTNER

Grow at your own pace

SELF-PACED JOURNEY

- Access to on demand education
- Brandable marketing assets
- Marketing automation platform
- Free fundamentals certification

ACCELERATE PARTNER

Grow with expert guidance

BUSINESS READINESS

- Sales, marketing, tech readiness
- Optional internal assessment
- Implement cybersecurit y
- Pricing and bundling tips
- Free advanced certifications

LEAD GENERATION

- Dedicated marketing concierge
- Market Development Funds
- Earn Co-Op Funds on growth
- Ready to use campaigns and assets for clients & prospects
- Access to subject matter experts for events

CLOSING DEALS

- Dedicated partner development manager
- Sales training for your team
- Sales framework coaching
- Access to pre-sales resources
- Co-Sell opportunities
- Sales debrief

New cybersecurity tracks: *Compliance, cyber insurance and addition of* BCDR *to the Partner Program*

Key Takeaways

- SIEM reduces damages from events
- Co-managed is truly co-managed
- Join communities for threat detection indicators
- Join the Partner Program to make the most of the SIEM

Don't forget to fill out your

SESSION SURVEY

Thank You

#ITNation

IT NATION