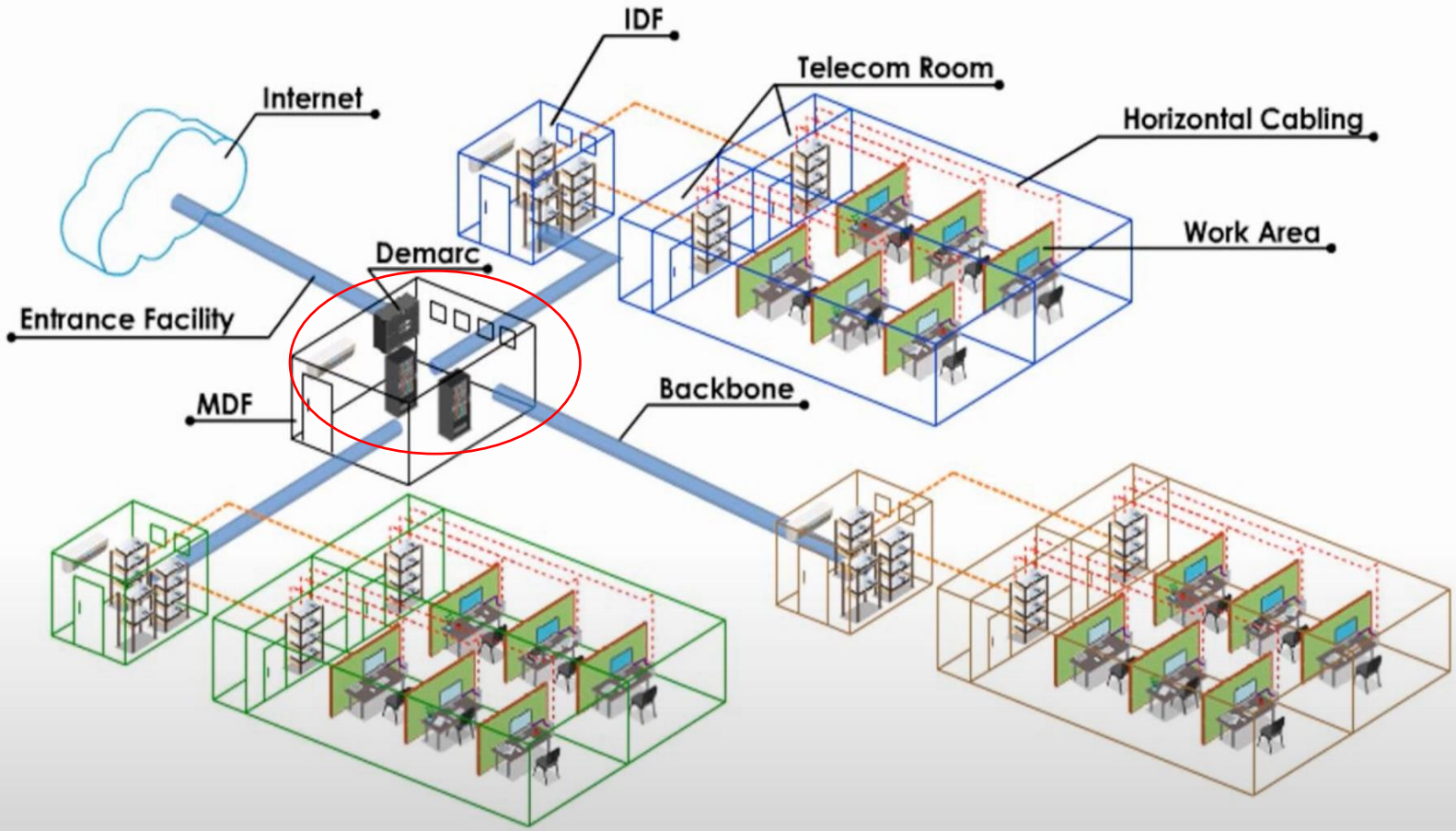
SECURITY OPERATIONS CENTER (SOC)

What Is a Security Operations Center (SOC)?

- A centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.
- A SOC acts like the hub or central command post, taking in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside.

SOC Placement



What Makes a SOC Effective? Fusing People, Processes, and Technology

- To create an effective SOC, you need three components — **people**, **processes**, and **technology** — to build an efficient security operation.

- A strong security operations platform can automatically take care of nearly every aspect of the **detection**, **response**, and **recovery processes.**

People

Security analysts work primarily in the monitoring and detection phases of a SOC.

Incident responder tasks may include:
Conducting deeper analysis of suspicious security events using:

- Search analytics capabilities
- Threat intelligence sources
- Basic forensics techniques
- Malware analysis tools
- Performing response activities whenever an incident necessitates
- Keeping management apprised of the status of incident response efforts

Security architect is typically someone within the security organization with a deep understanding of the organization’s security program and infrastructure.

SOC staffing models

- Fully Outsourced
- Fully In-House
- Hybrid (Combination of Employees and Outsourcing)

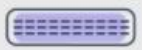
Technology

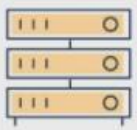
WORKSTATIONS

NETWORK HARDWARE & SOFTWARE


FIREWALL


ROUTER


SWITCH


SERVER


MAINFRAME


IDS/IPS

SYSTEM IMPORTS

EVENT LOG DATA
Operating System
Applications
Devices
Databases

CONTENXTUAL LOG DATA
Vulneralbility Scans
User Information
Asset Information
Threat Intelligence

SIEM SYSTEM

- Ingestion and interpretation of logs
- Updated threat intelligence feeds
- Correlation and analyics
- Avanced profiling
- Security alerts
- Data presentation
- Compliance

SYSTEM OUTPUTS

SYSTEM ADMIN
Analysis
Reports
Real Time Monitoring

Technology

WORKSTATIONS

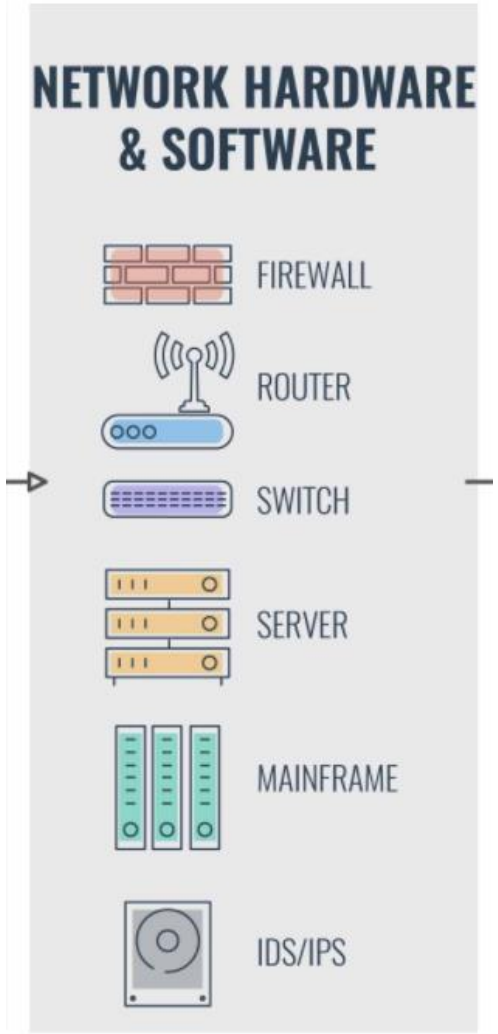
macOS®

Linux™

Windows

CentOS

Technology



pfsense

OPNsense

SURICATA

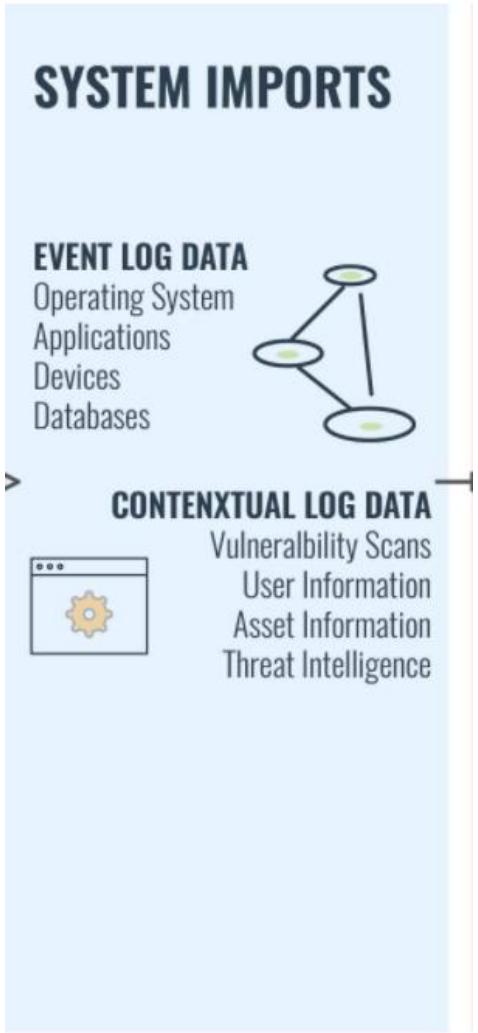
SNORT

Hewlett Packard Enterprise

aruba
a Hewlett Packard Enterprise company

OPENVPN

Technology



Nagios®

TCPDUMP

What is SIEM?

- **S**ecurity **I**nformation **M**anagement (**SIM**) is the collection, monitoring, and analysis of security-related data from computer logs. Also referred to as log management.

- **S**ecurity **E**vent **M**anagement (**SEM**) is the practice of network event management including real-time threat analysis, visualization, and incident response.

SIM VS SEM VS SIEM

SECURITY INFORMATION MANAGEMENT

SOFTWARE THAT AUTOMATES THE COLLECTION OF EVENT LOG DATA

Server Antivirus Firewall Switch/Routers

DATA GENERATED FROM NUMEROUS SOURCES

STRONG LOG MANAGEMENT CAPABILITIES

SECURITY EVENT MANAGEMENT

STRONG EVENT MANAGEMENT, REAL-TIME THREAT ANALYSIS, VISUALISATION, TICKETING, INCIDENT RESPONSE, AND SECURITY OPERATIONS

Oracle Database

DATA GENERATED FROM SQL/ORACLE DATABASES

POOR LOG MANAGEMENT CAPABILITIES

SECURITY INFORMATION AND EVENT MANAGEMENT

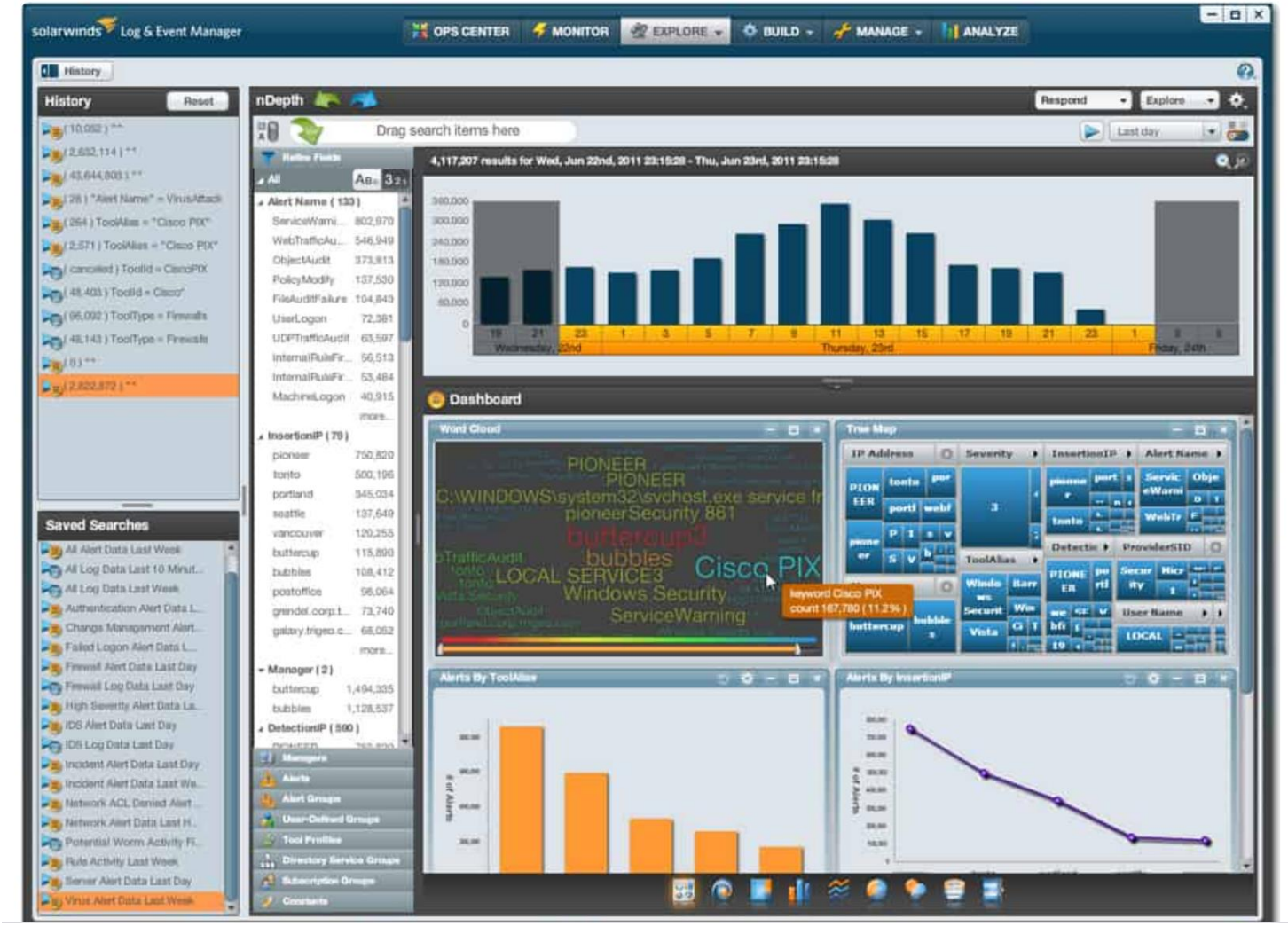
COMBINES SIM AND SEM CAPABILITIES

SolarWinds Security Event Manager (SEM)

One of the most competitive offerings on the market.

Key Features:

- Automated log searches for breaches
- Live anomaly detection
- Historical analysis
- System alerts
- 30-day free trial

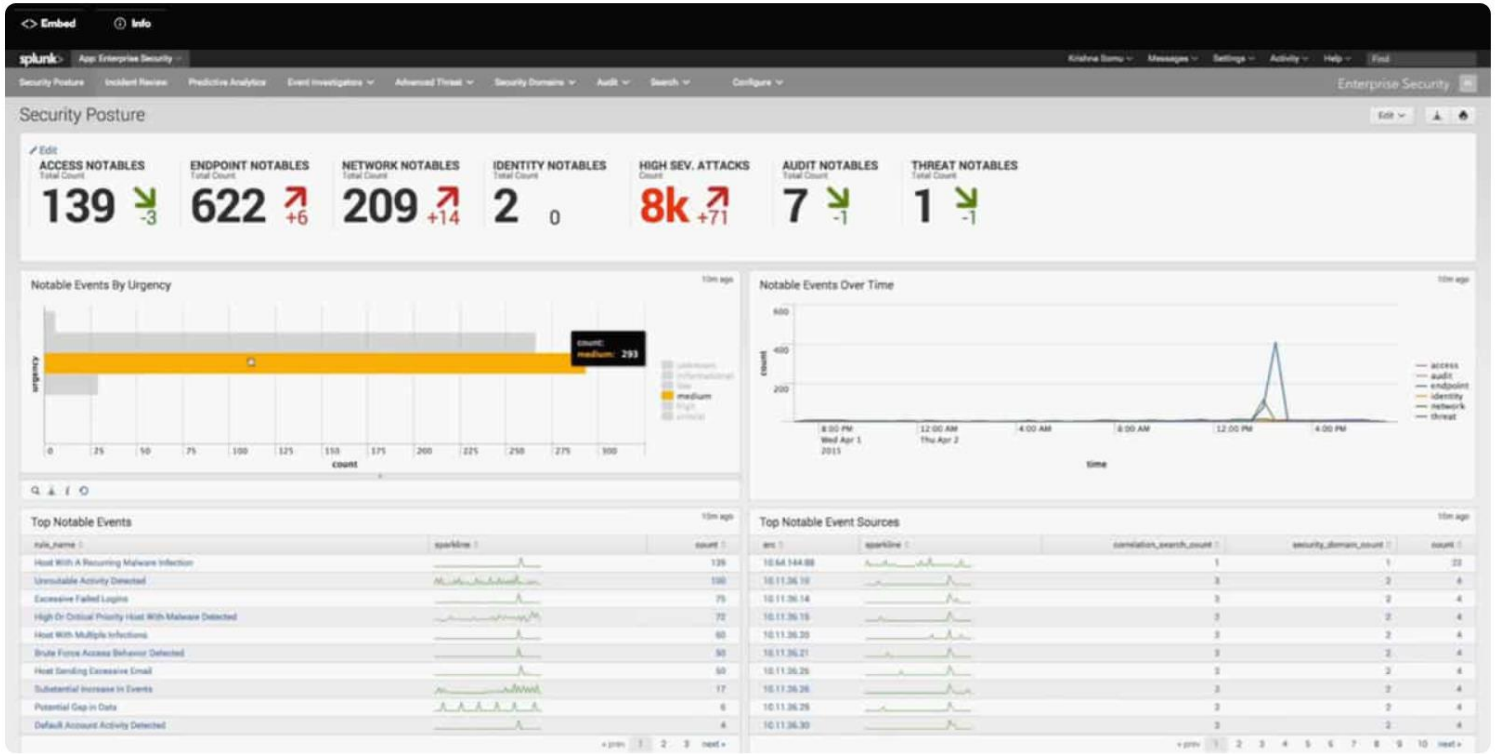


Splunk Enterprise Security

- One of the most popular SIEM management solutions in the world.
- What sets it apart from the competition is that it has incorporated analytics into the heart of its SIEM.

Key Features:

- Real-time network monitoring
- Asset Investigator
- Historical analysis

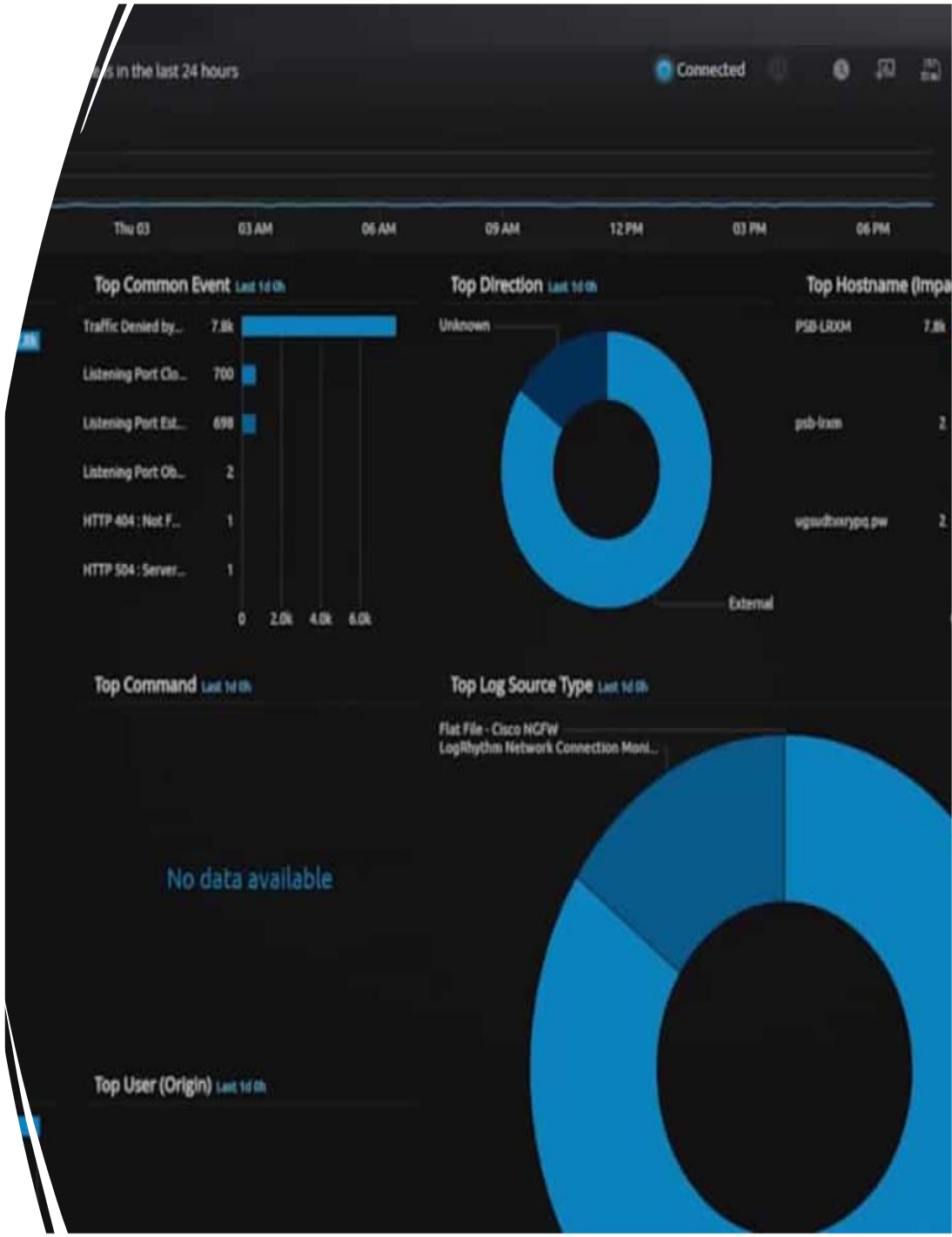


LogRhythm NextGen SIEM Platform

- **LogRhythm** have long established themselves as pioneers within the SIEM solution sector.
- From behavioral analysis to log correlation and artificial intelligence for machine learning, this platform has it all.

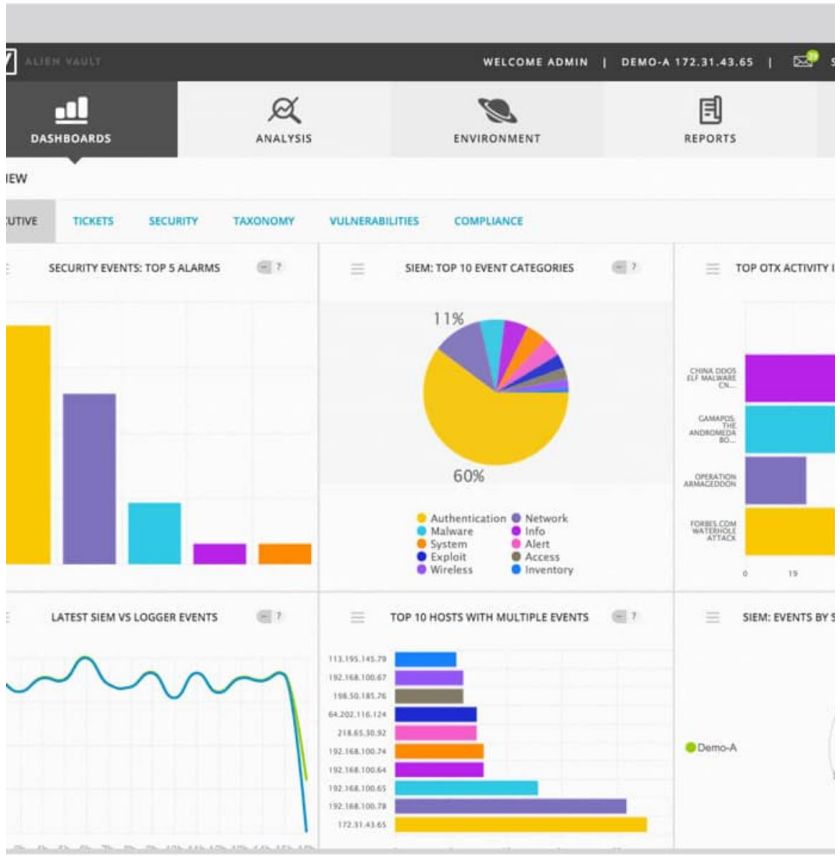
Key Features:

- AI-based
- Log file management
- Guided analysis



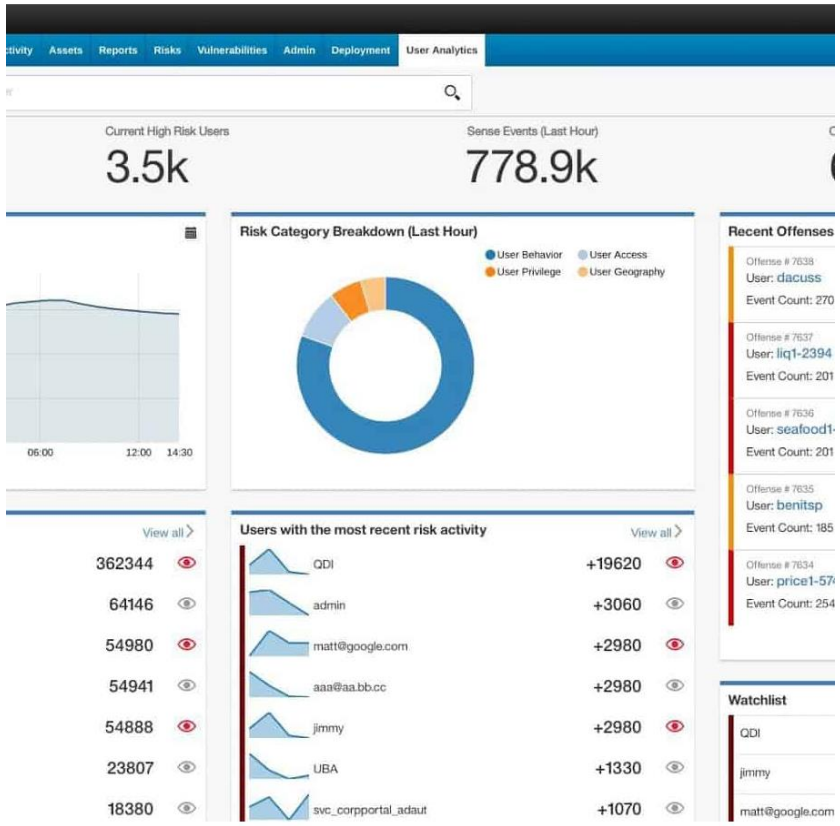
AT&T Cybersecurity AlienVault Unified Security Management

- As one of the more competitively priced SIEM solutions on this list, **AlienVault** (now part of **AT&T Cybersecurity)** is a very attractive offering.
- At its core, this is a traditional SIEM product with built-in intrusion detection, behavioral monitoring, and vulnerability assessment.
- AlienVault has the onboard analytics you would expect from scalable platform.



IBM QRadar SIEM

- Over the past few years or so, IBM's answer to SIEM has established itself as one of the best products on the market.
- The platform offers a suite of log management, analytics, data collection, and intrusion detection features to help keep your critical systems up and running.



McAfee Enterprise Security Manager

- **McAfee Enterprise Security Manager** is regarded as one of the best SIEM platforms in terms of analytics. The user can collect a variety of logs across a wide range of devices through the Active Directory system.

Key Features:

- Log consolidation
- Live monitoring

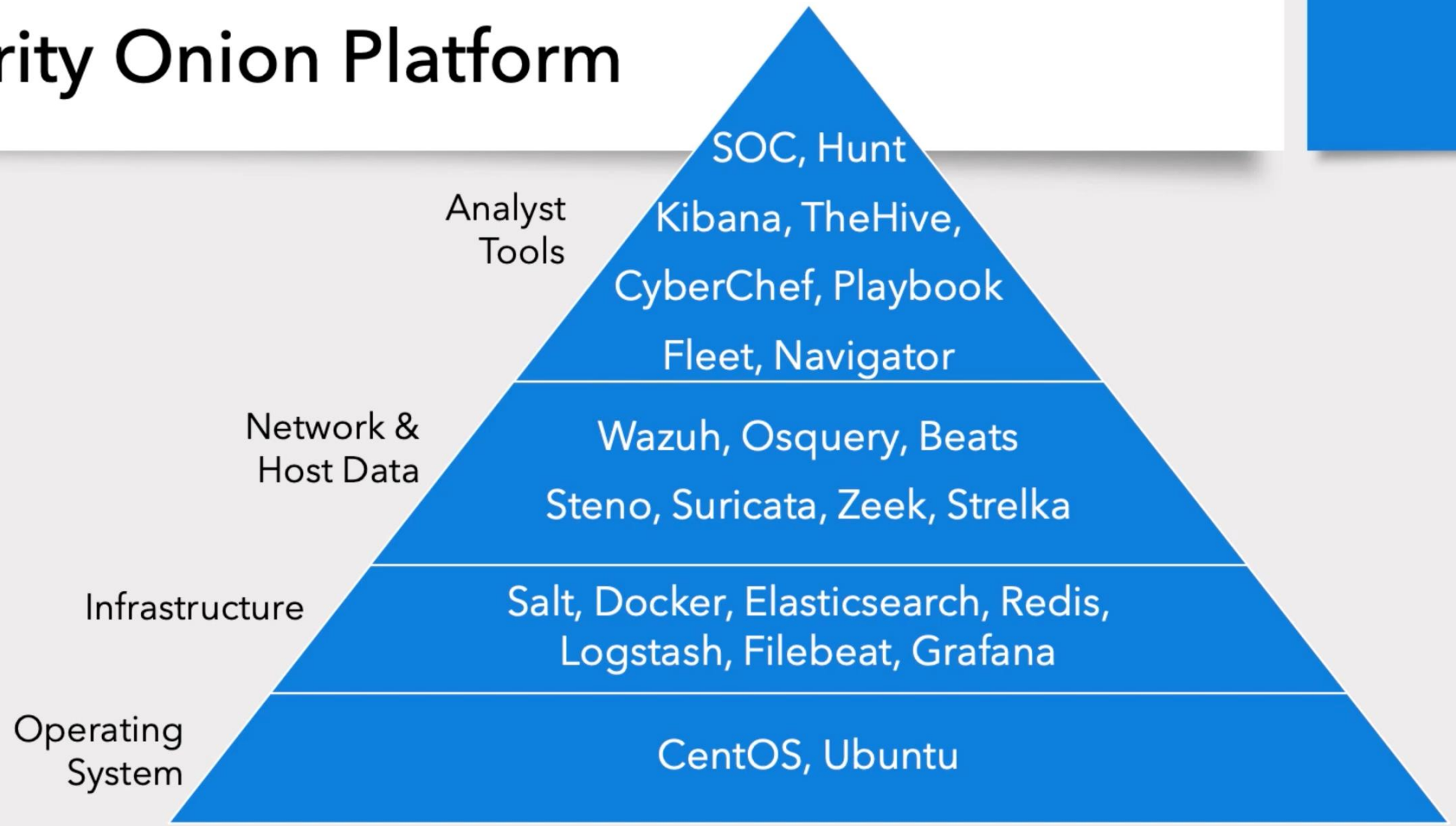
The Best SIEM Vendors

OPENSOURCE SIEM

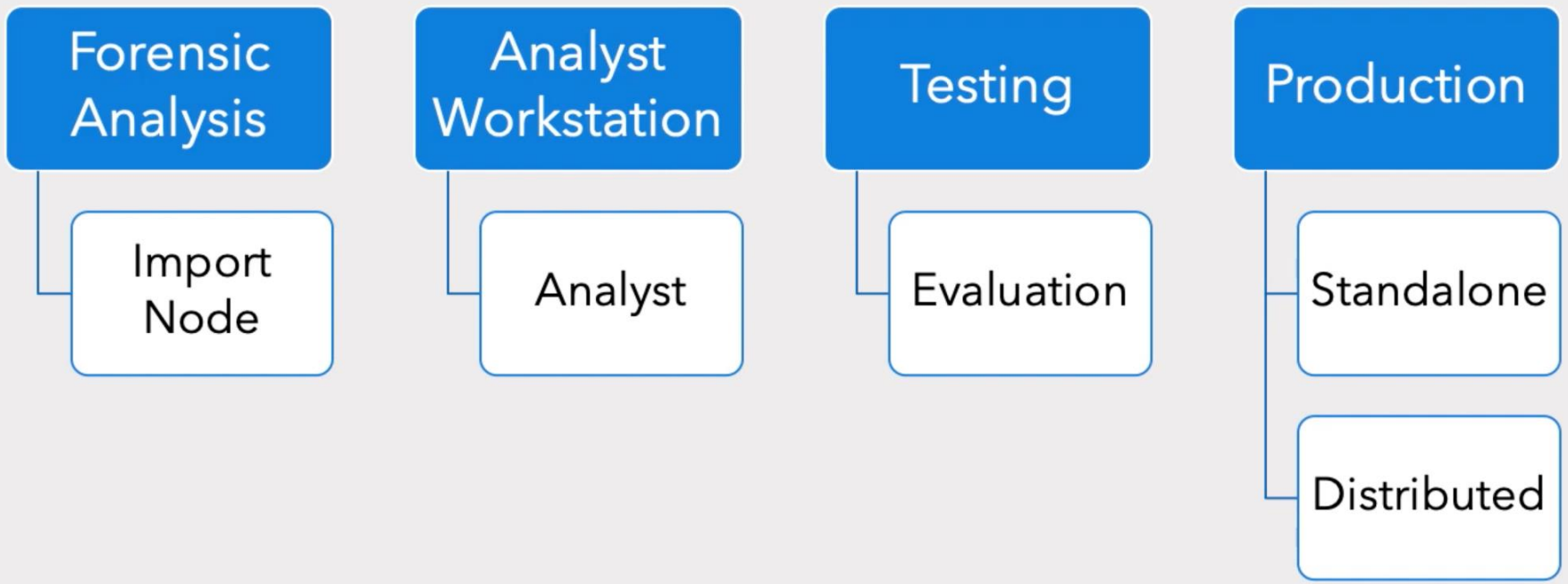
- Security Onion is a free and open Linux distribution for threat hunting, enterprise security monitoring, and log management.
- It includes TheHive, Playbook, Fleet, osquery, CyberChef , Elasticsearch, Logstash, Kibana, Suricata, Zeek, Wazuh, and many other security tools.
- Security Onion has been downloaded over 2 million times and is being used by security teams around the world to monitor and defend their enterprises.

https://docs.securityonion.net/_/downloads/en/2.3/pdf/

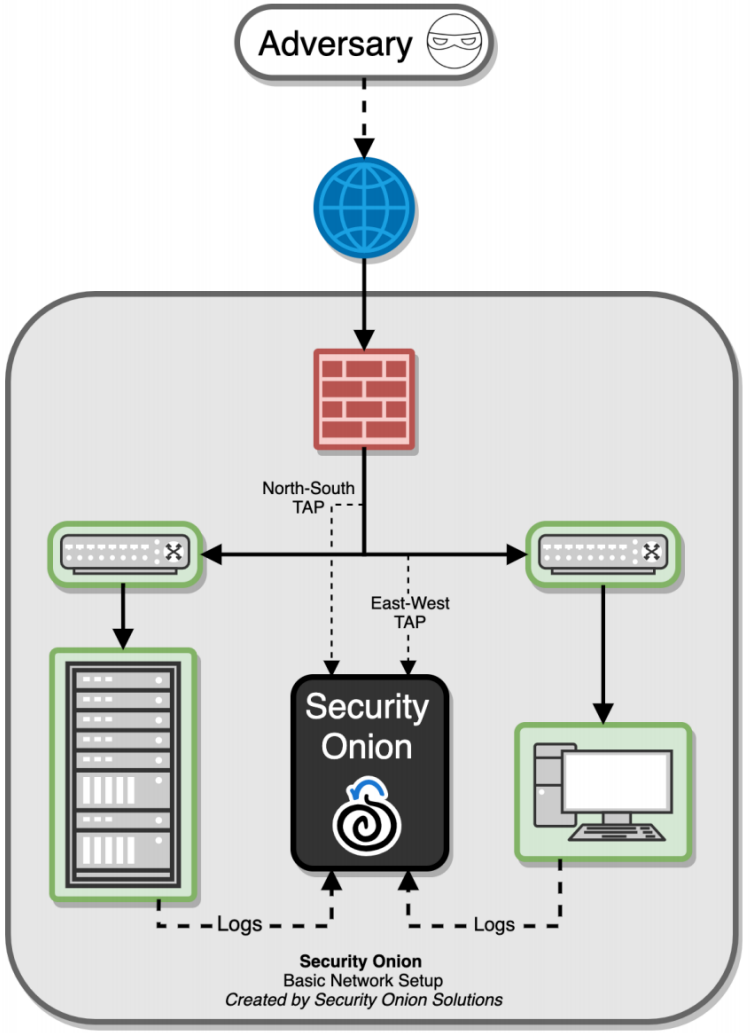
Security Onion Platform



Use Cases & Deployment Modes



- Security Onion in a traditional enterprise network with a firewall, workstations, and servers.
- You can use Security Onion to monitor north/south traffic to detect an adversary entering an environment, establishing command-and-control (C2), or perhaps data exfiltration.
- You'll probably also want to monitor east/west traffic to detect lateral movement.



Security Onion Tools

https://docs.securityonion.net/en/2.3/

7 Steps to Building a SOC with Limited Resources

Detect and Respond to Threats Fast (Even if You Can't Staff a 24x7 SOC)

The state of the understaffed SOC

Most organizations don’t have the resources to staff a 24x7 security operations center (SOC).

The result?

- Events not monitored around the clock
- Major delays in detecting and responding to incidents
- Inability to hunt for threats proactively

It’s a dangerous situation.

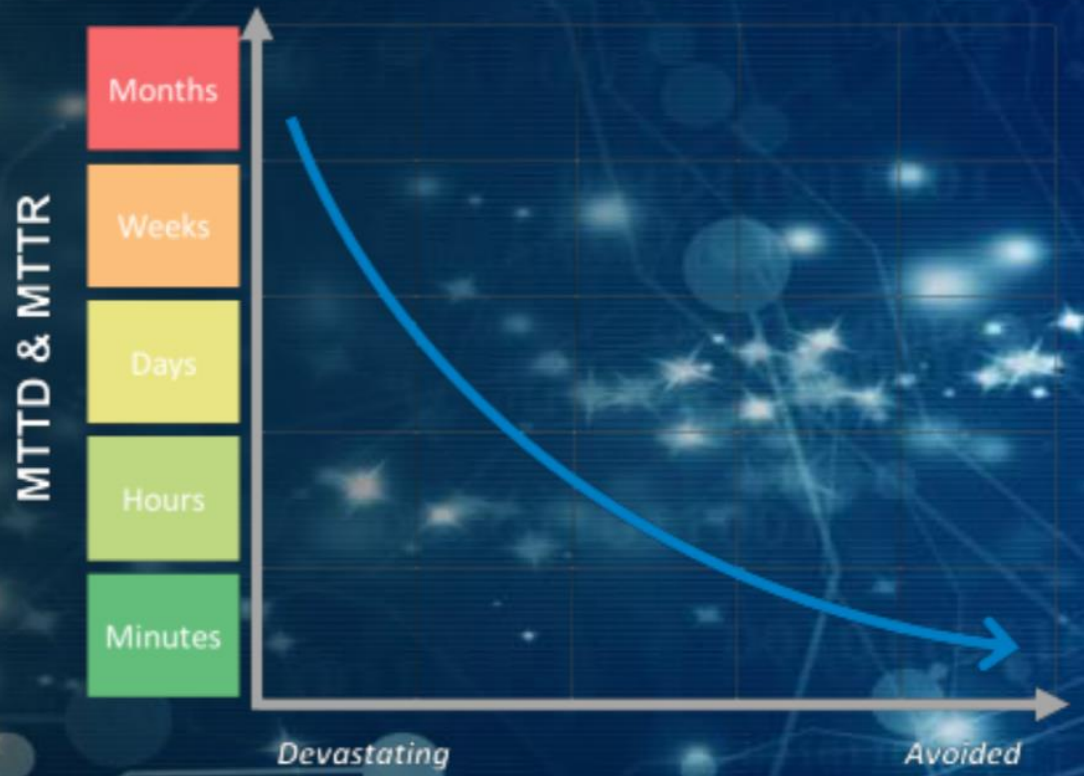
But there is a solution

With an automated SOC built for scale, your team can:

Detect threats swiftly: Your team can perform constant event monitoring.

Respond to threats rapidly. Your team can expedite incident response.

Building an efficient, automated SOC with the resources you have is about **combining people, process, and technology to achieve your goals**.



7 Steps to Building a SOC with Limited Resources

Learn to build a SOC that efficiently leverages Threat Lifecycle Management to rapidly detect and respond to threats.

Develop your strategy

The key to developing your strategy is to understand the current state of your organization.

- ✓ Assess your existing capabilities
- ✓ At first, limit your scope to core functions:
  - Monitoring
  - Detection
  - Response
  - Recovery
- ✓ Delay non-core functions until your core functions are sufficiently mature
- ✓ Identify and define business objectives

Design the solution

Good places to start.

- ✓ Choose a few business-critical use cases (e.g., a phishing attack)
- ✓ Define your initial solution based on these use cases
- ✓ Consider that your solution must be able to meet future needs

A narrow scope will reduce the time to initial implementation which will help you achieve results faster.

Take three actions

1. Define your functional requirements.
   (Be sure these are tied to business objectives.)
2. Choose a SOC model based on your functional requirements.
3. Design your technical architecture.
   a) Choose your Threat Lifecycle Management platform
   b) Identify business and information systems to be integrated
   c) Define your workflows
   d) Pinpoint areas for automation
   e) Test the architecture

Create processes, procedures and training

In Step 3, it's important to make sure that all six phases of the Threat Lifecycle Management Framework are covered.

TIME TO DETECT

Collect Data

Security event data

Log and machine data

Forensic sensor data

Discover

Search analytics

Machine analytics

Qualify

Assess threat to determine risk and whether full investigation is necessary

TIME TO RESPOND

Investigate

Analyze threat to determine nature and extent of the incident

Neutralize

Implement countermeasures to mitigate threat and associated risk

Recover

- Cleanup
- Report
- Review
- Adapt

Prepare your environment

Before deployment, make sure crucial security elements are in place:

- ✓ Ensure SOC staff desktops, laptops and mobile devices are secure
- ✓ Put secure remote access mechanisms in place for SOC staff (and outsourcers if applicable)
- ✓ Require strong authentication

Implement your solution

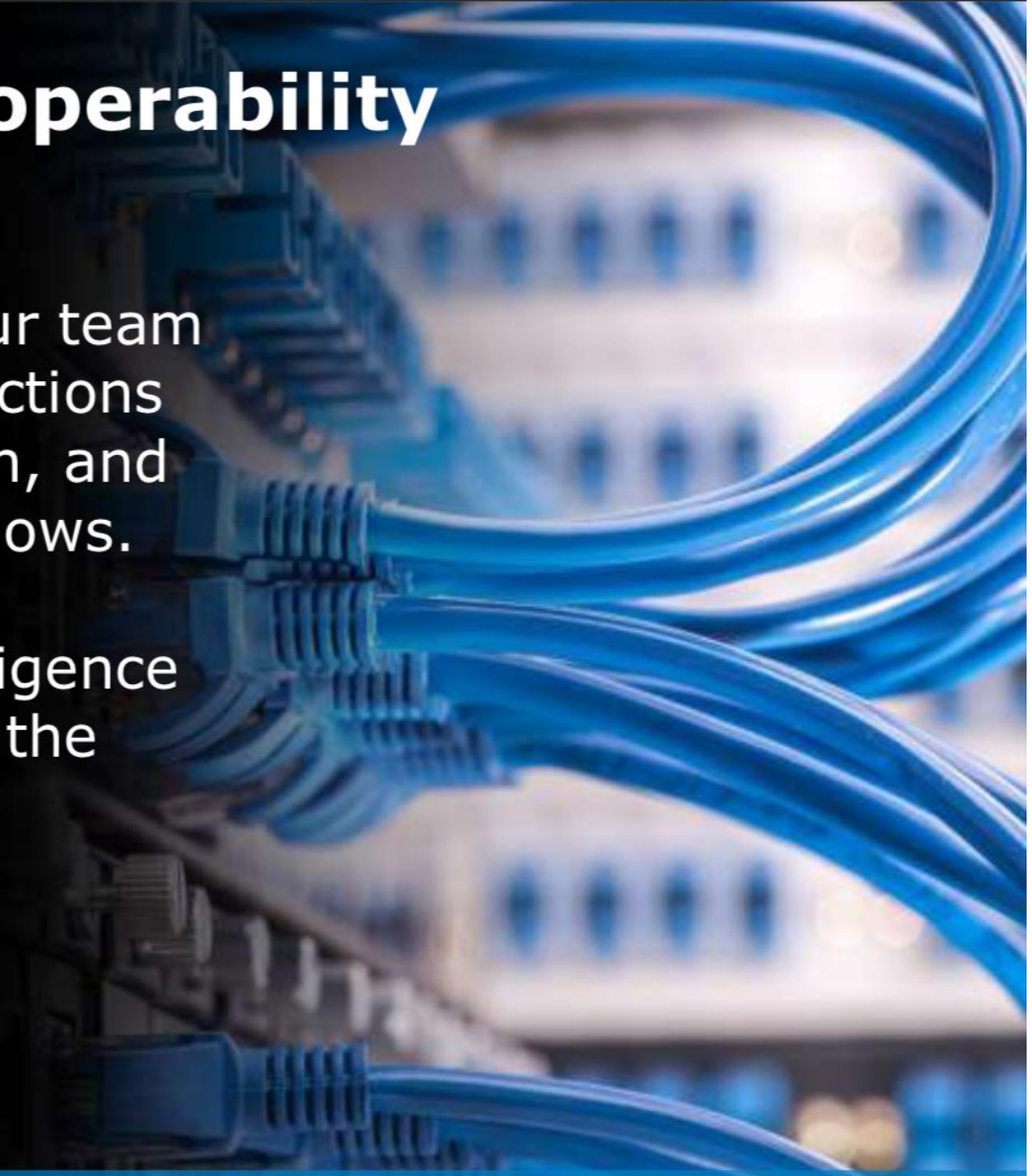
Take full advantage of your technology to minimize the workload on your staff:

1. Bring up your log management infrastructure.
2. Onboard your minimum collection of critical data sources.
3. Bring up your security analytics capabilities.
4. Onboard your security automation and orchestration capabilities.
5. Begin deploying use cases to focus on end-to-end threat detection and response realization.

Realize seamless interoperability

System interoperability is critical for your team to collect data from sources and issue actions and commands to apply context, contain, and remediate in alignment with your workflows.

You should also incorporate threat intelligence feeds and automated inputs to improve the accuracy of your SOC's detection.



Deploy end-to-end use cases

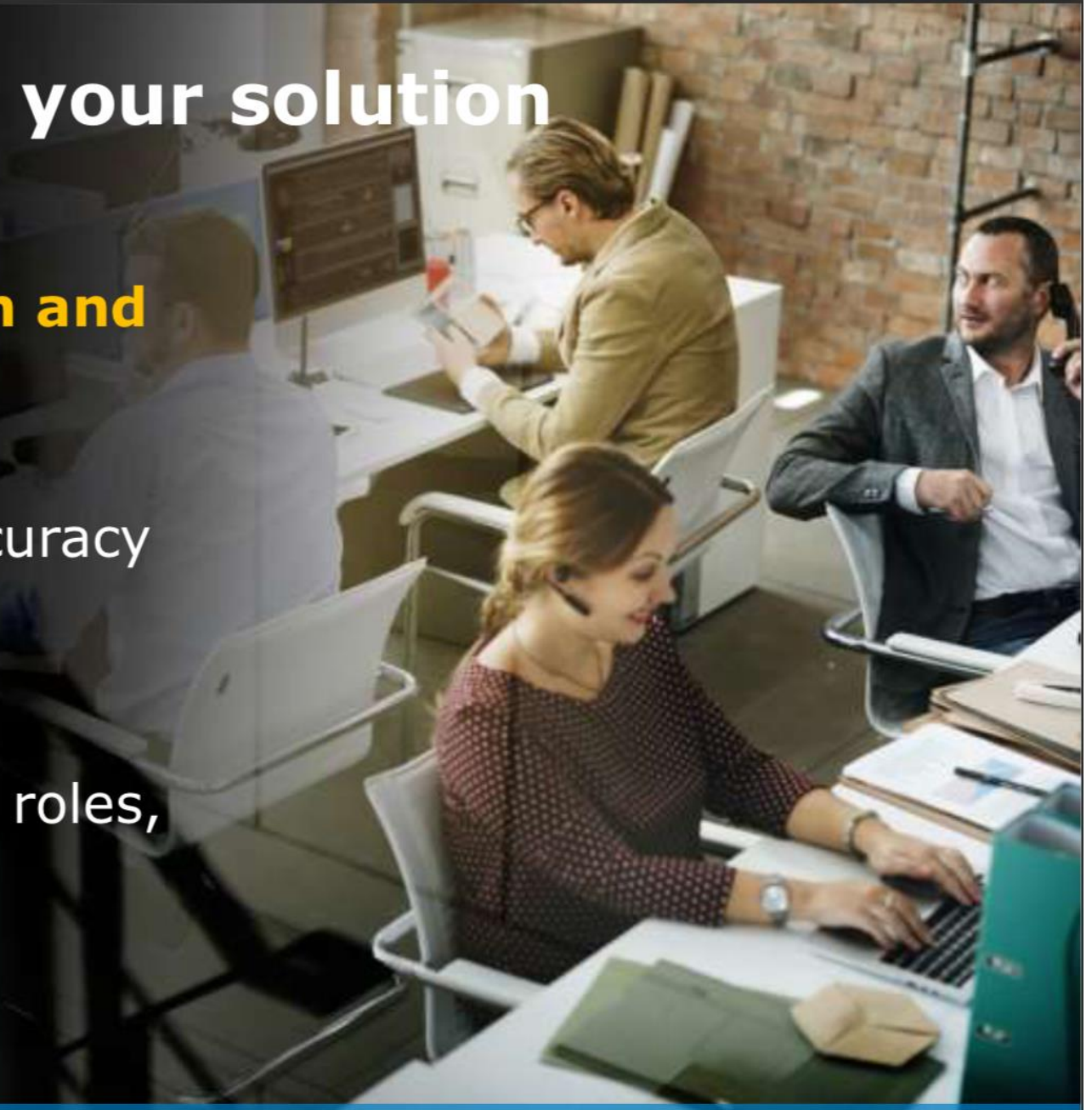
Your tech is in place and your capabilities are deployed. Now for the fun part.

- ✓ Implement your use cases across your analytics and security automation and orchestration tiers.
- ✓ Test your use cases rigorously over a variety of shifts and during shift changes.
- ✓ Proof the reliability and security of your solution.

Maintain and evolve your solution

A SOC isn't something to turn on and stop thinking about. It requires ongoing maintenance, such as:

- ✓ Tuning to improve detection accuracy
- ✓ Adding other systems as inputs or outputs
- ✓ Reviewing the SOC model, SOC roles, staff counts



Send your question

- Email:

- manaagas@clsu.edu.ph
- marlon.naagas@prime.edu.ph