# Cyber Toolkit: Modern Defenses for Modern Cyber Warfare

Eric Gravett, InfoSec & GRC Specialist

jack henry™ cyber warfare webinar series | 05/11/2023

# Cyber Warfare Webinar Series

1. Ransomware: The Attack You See Coming but Still Aren’t Preventing
2. Improve Compliance by Modernizing User Access Reviews
3. Start Planning Now: Cyber Threats and Trends for 2023
4. Cyber Warfare: Achieving Resiliency Through the Cloud
5. Avoid Landmines with Your Backup and Recovery Strategy
6. Cyber Toolkit: Modern Defenses for Modern Cyber Warfare

YOU ARE HERE

https://www.jackhenry.com/resources?types=type-webinar

# “Modern”

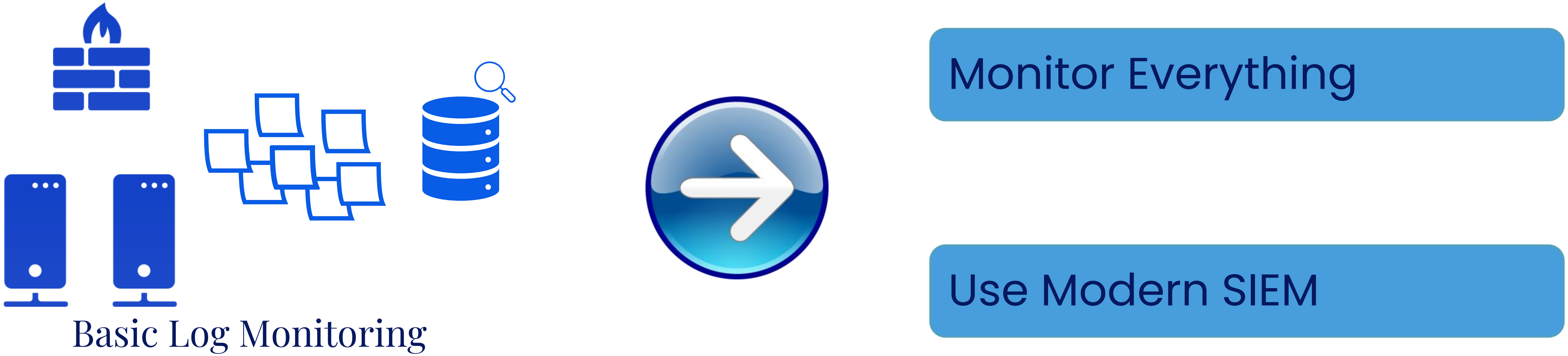
Not this kind of “modern”

NICHOLAS LIM | 19/06/2017
WWW.ARTSTATION.COM/ARTIST/NICHOLASLIM

# Modernize defenses based on changing threats

# Modernize Your Defenses

# security information & event management (SIEM)



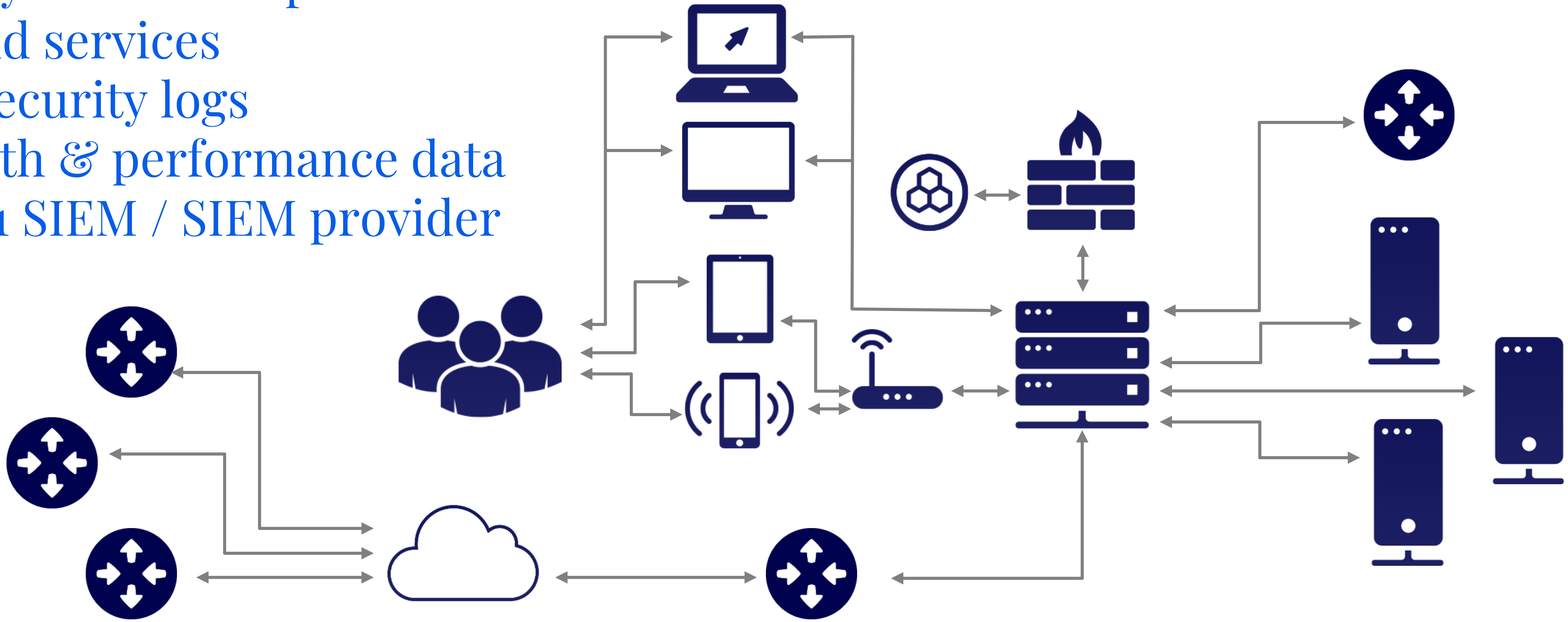
Basic Log Monitoring

Monitor Everything

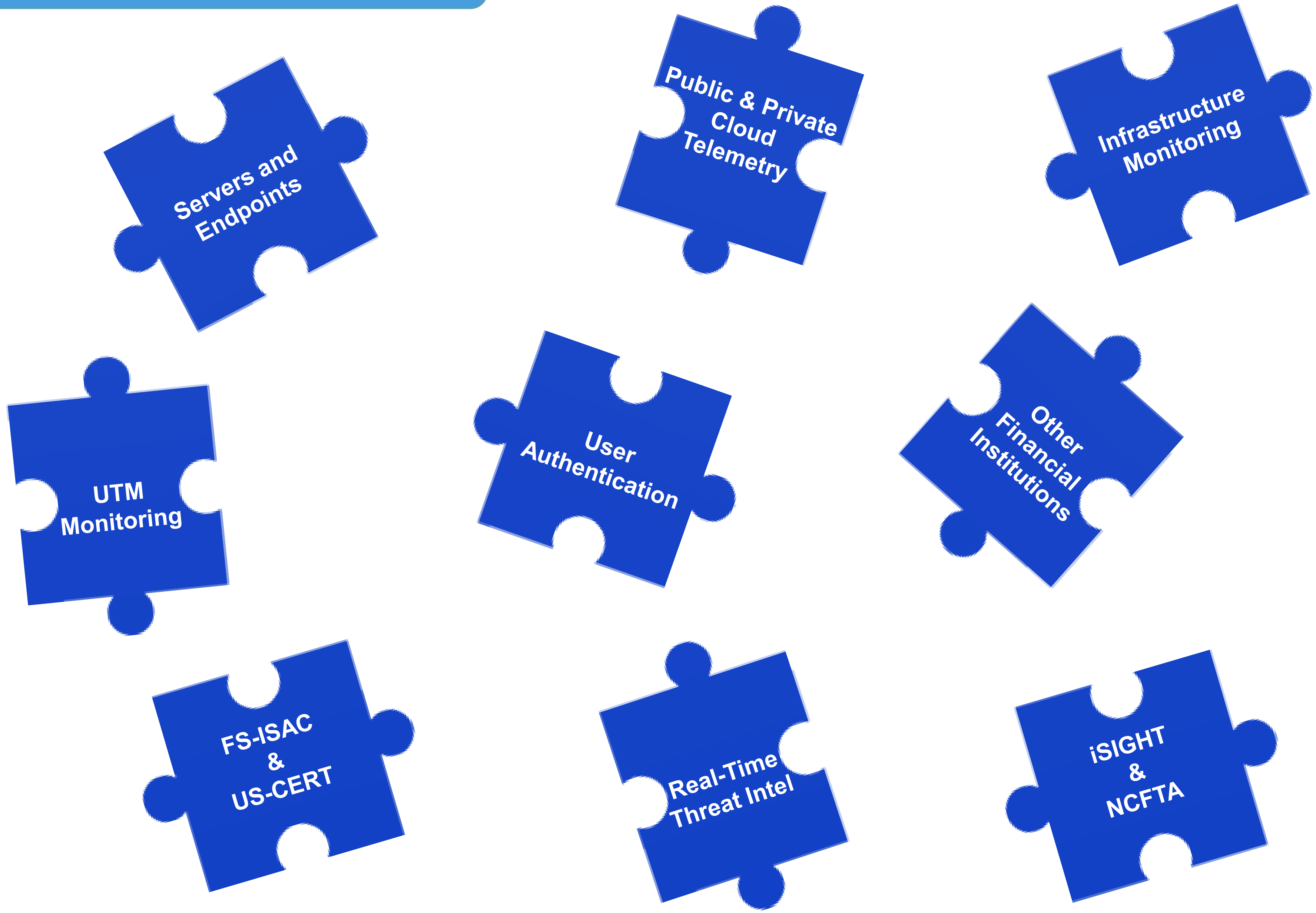
Use Modern SIEM

# Monitor Everything

Every device and platform
Cloud services
All security logs
Health & performance data
Use 1 SIEM / SIEM provider



# Use Modern SIEM



Servers and Endpoints

Public & Private Cloud Telemetry

Infrastructure Monitoring

UTM Monitoring

User Authentication

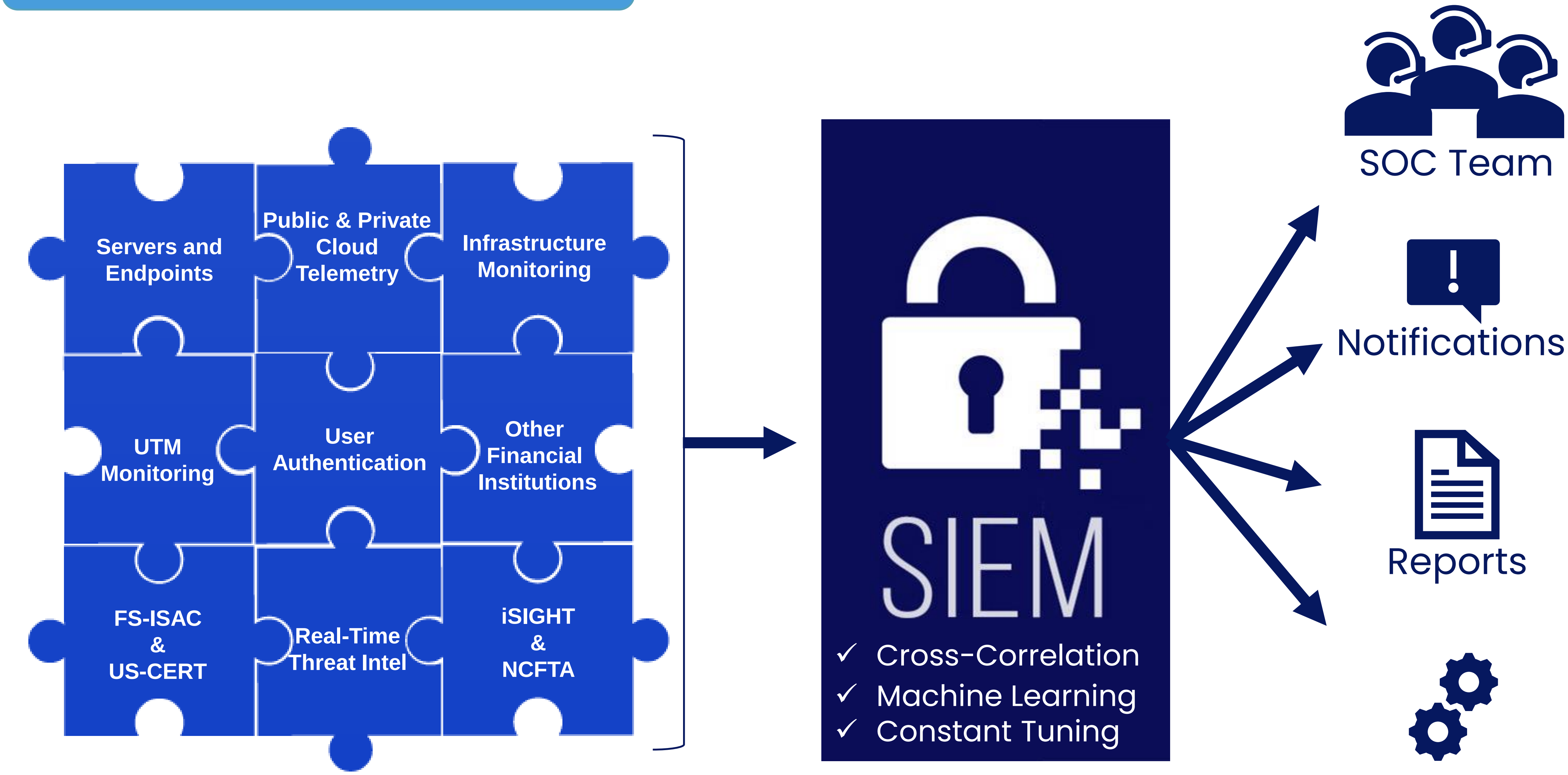
Other Financial Institutions

FS-ISAC & US-CERT

Real-Time Threat Intel

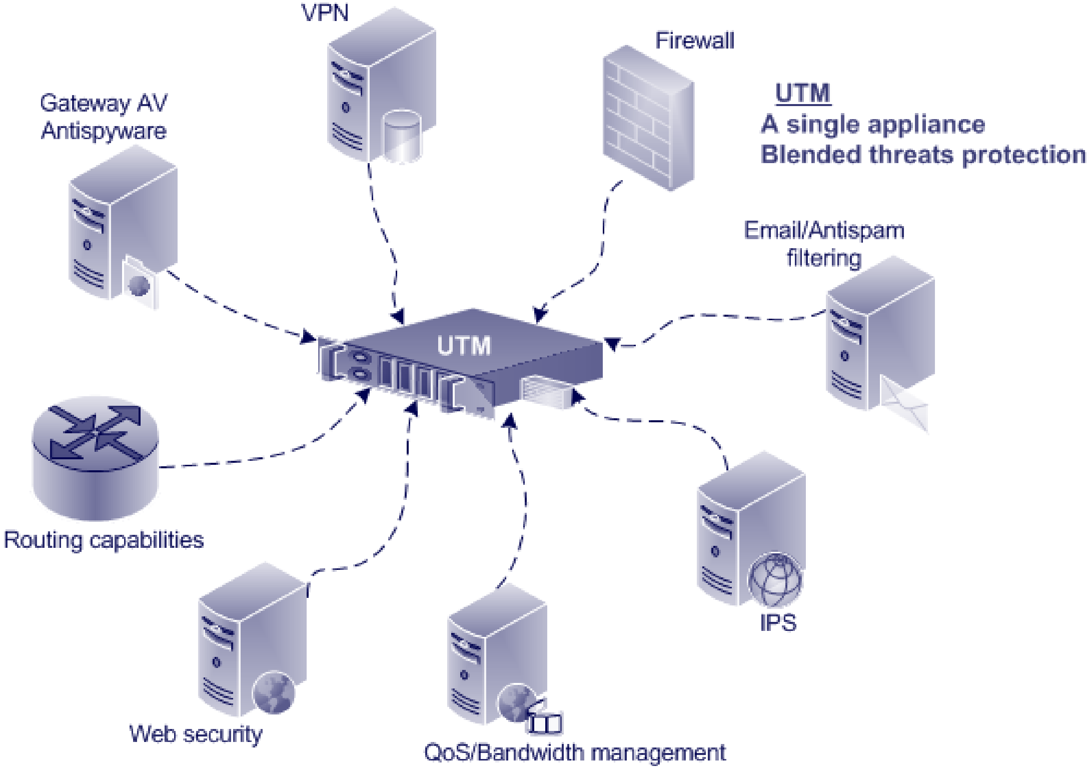
iSIGHT & NCFTA

# Use Modern SIEM



- ✓ Cross-Correlation
- ✓ Machine Learning
- ✓ Constant Tuning

# internet perimeter



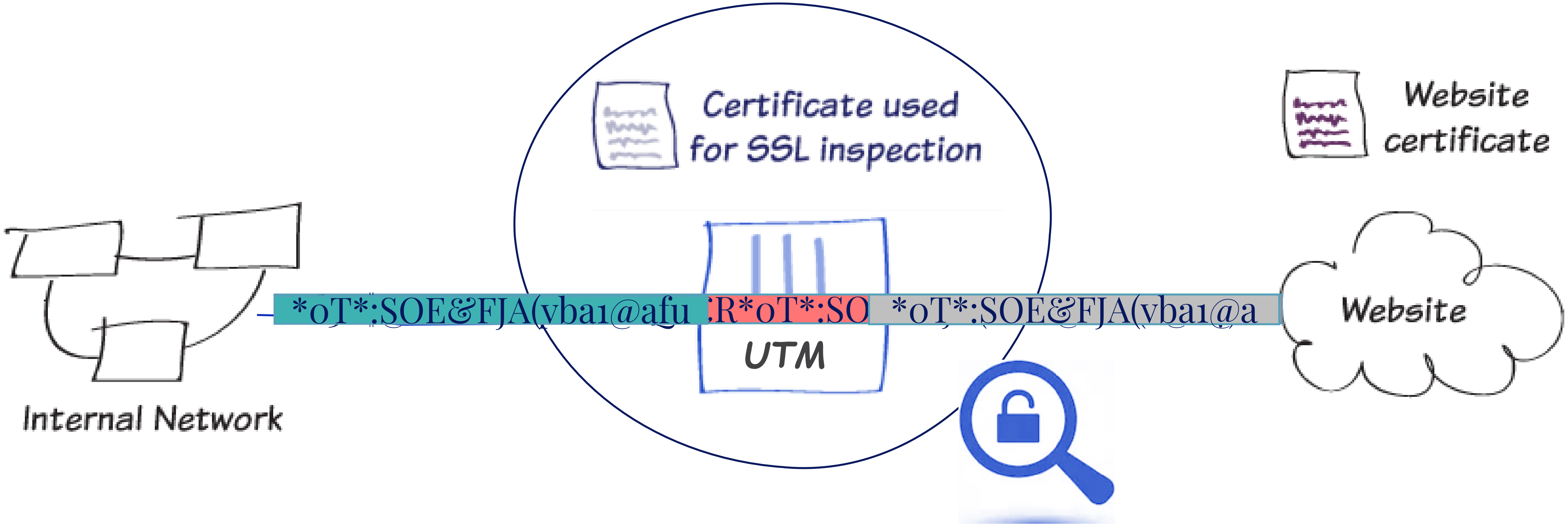
**UTM**
A single appliance
Blended threats protection

SSL/TLS Deep Inspection

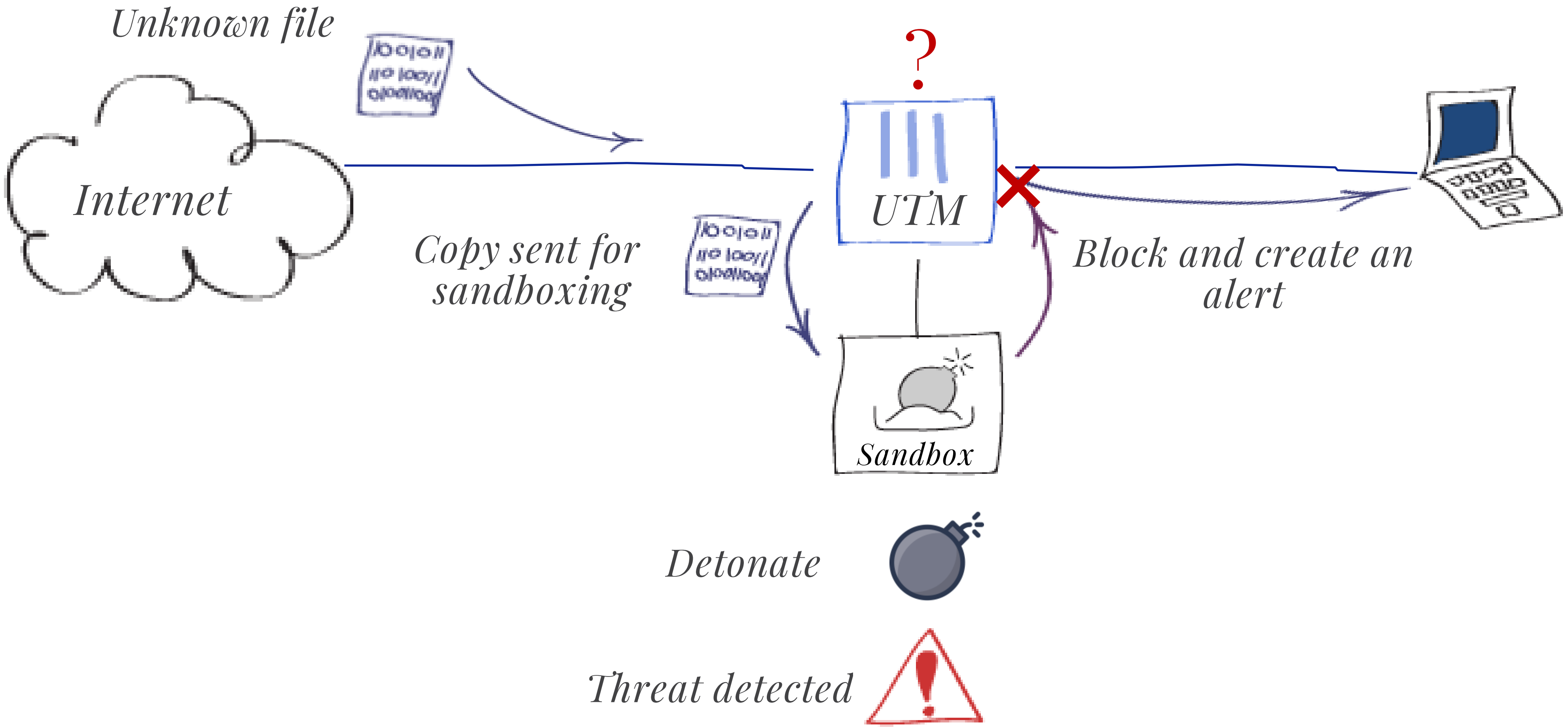
Sandboxing

Data Leak Prevention

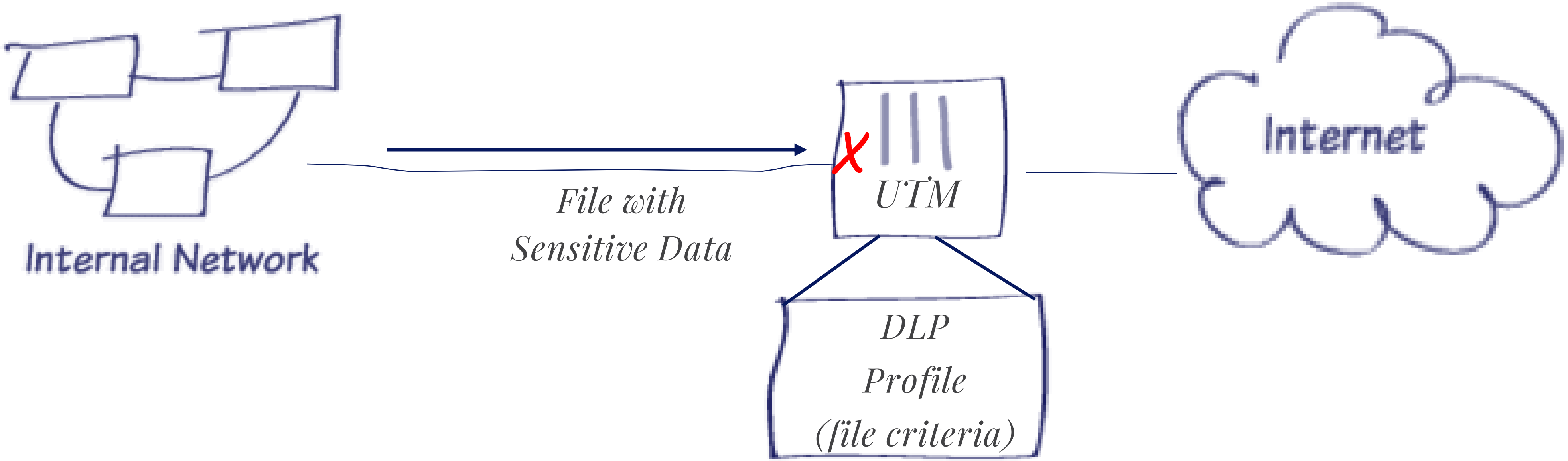
# SSL/TLS Deep Inspection



# Sandboxing


Unknown file
Internet
?
UTM
Copy sent for sandboxing
Block and create an alert
Sandbox
Detonate
Threat detected

# Data Leak Prevention



File with Sensitive Data

UTM

DLP Profile (file criteria)

SSN or CC Numbers
Watermarked Files

# endpoint protection using no TLAs

(you’re welcome)

Norton from symantec
McAfee
KASPERSKY lab *
AVG Anti-Virus
avast! be free
AVIRA
NOD32 antivirus
bitdefender secure your every bit
TREND MICRO
F-Secure
eset
G DATA

* Please don’t use this one

Modern Features

Logging to SIEM

Managed 24/7

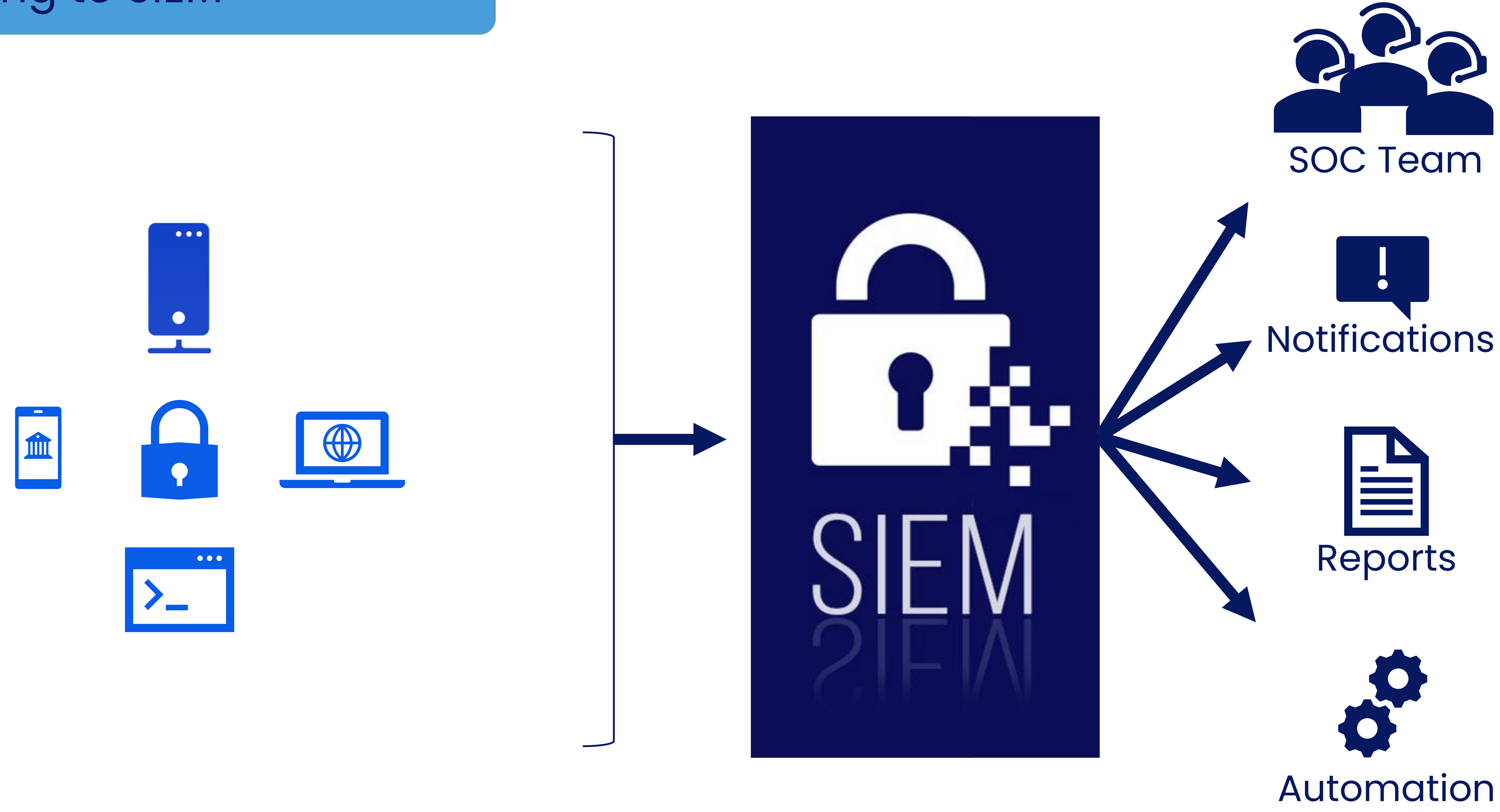
# Modern Features

Behavioral Analysis

Application Control

Breach Containment

# Logging to SIEM



# Managed 24/7

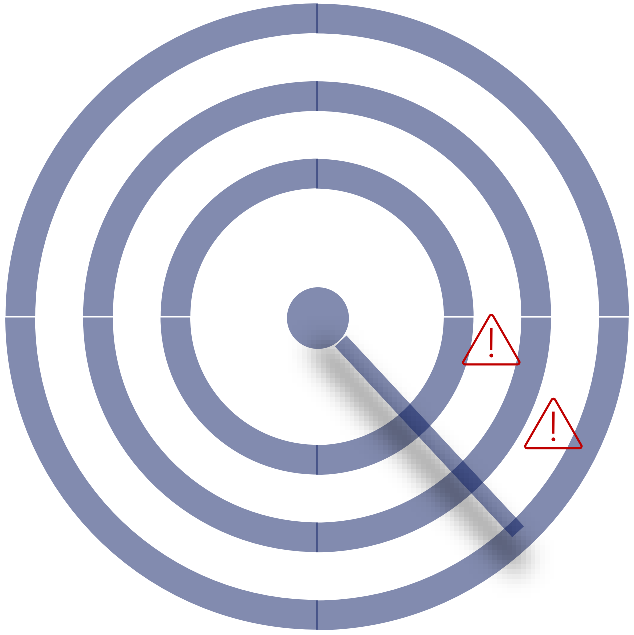
Managed 24/7 by **Experts**

internal team or use MSSP

Alert Procedures

- response
- containment
- recovery

# vulnerability scanning



Frequency

Usable Reports

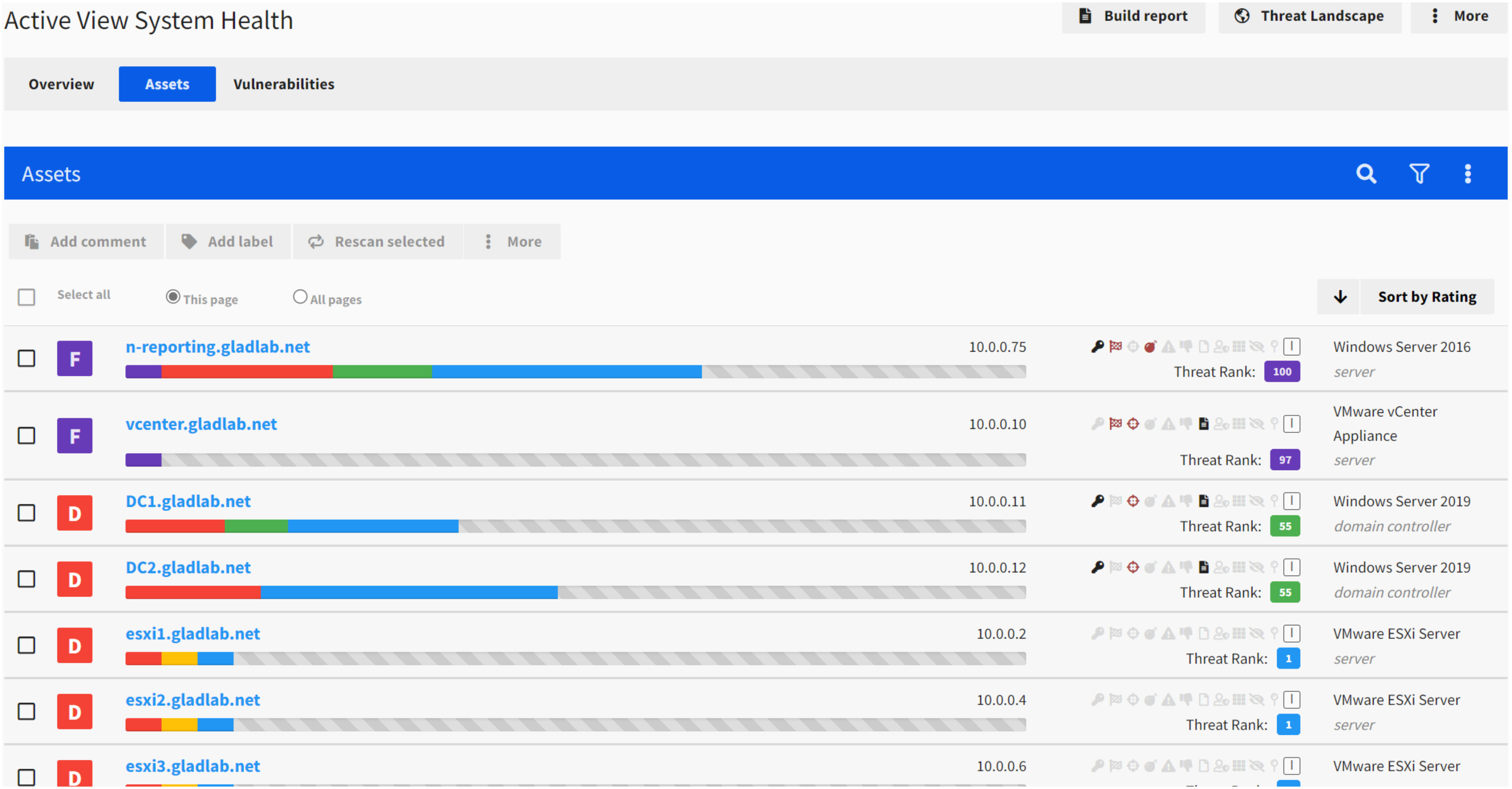
Mitigation Procedures

# Frequency

~~Quarterly / Monthly~~

Weekly
(at minimum)

# Usable Reports

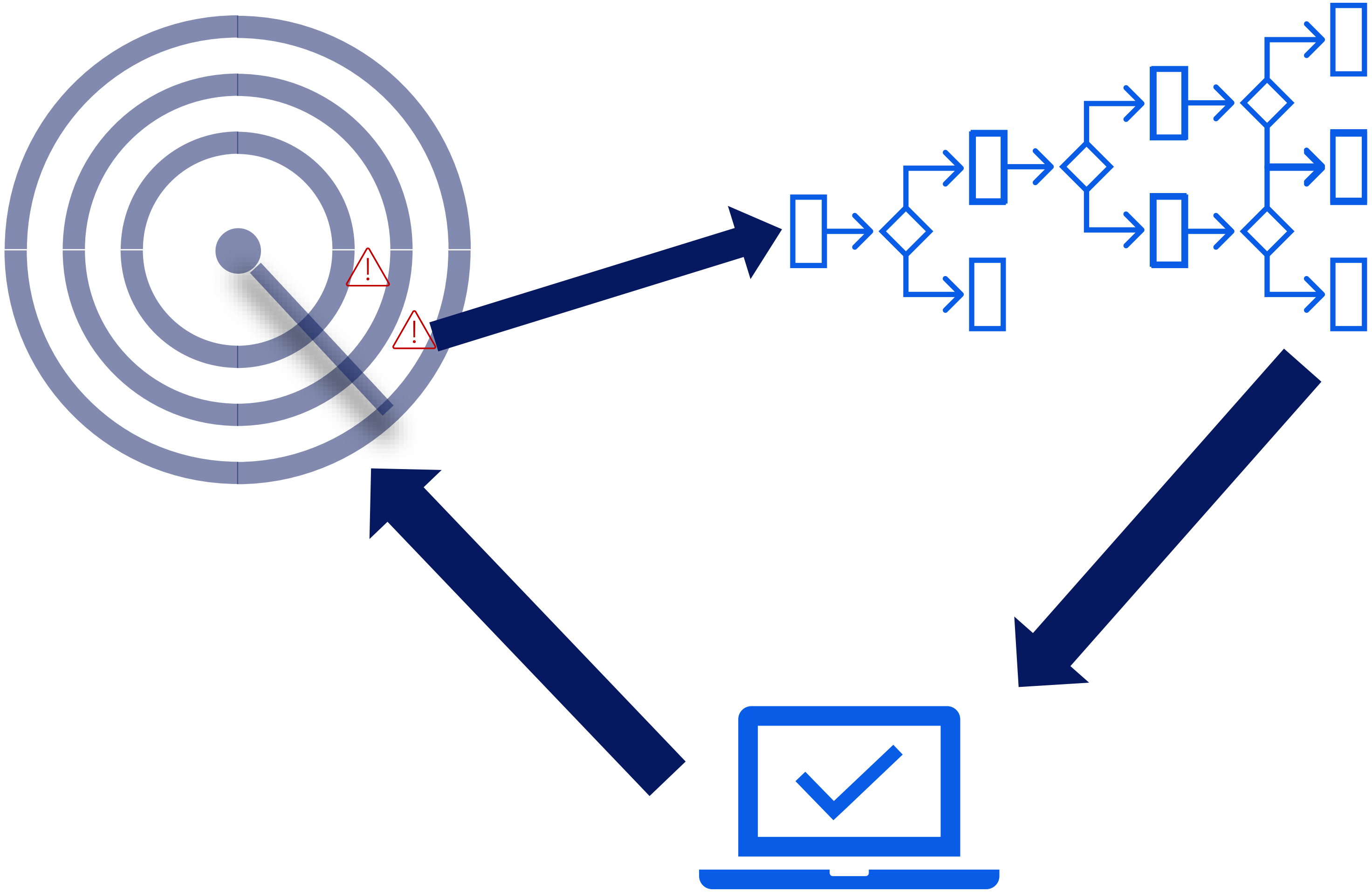


## Active View System Health

### Assets

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| □ | F | n-reporting.gladlab.net | 10.0.0.75 | Threat Rank: 100 | Windows Server 2016 | *server* |
| □ | F | vcenter.gladlab.net | 10.0.0.10 | Threat Rank: 97 | VMware vCenter Appliance | *server* |
| □ | D | DC1.gladlab.net | 10.0.0.11 | Threat Rank: 55 | Windows Server 2019 | *domain controller* |
| □ | D | DC2.gladlab.net | 10.0.0.12 | Threat Rank: 55 | Windows Server 2019 | *domain controller* |
| □ | D | esxi1.gladlab.net | 10.0.0.2 | Threat Rank: 1 | VMware ESXi Server | *server* |
| □ | D | esxi2.gladlab.net | 10.0.0.4 | Threat Rank: 1 | VMware ESXi Server | *server* |
| □ | D | esxi3.gladlab.net | 10.0.0.6 |  | VMware ESXi Server |  |

# Mitigation Procedures



# Thank You!

# Questions?

jack henry™

Eric Gravett | egravett@jackhenry.com | jackhenry.com

© 2022 Jack Henry & Associates, Inc.®