Increase Cyber Resiliency Through Complete Visibility

Sebastian Fazzino – CISSP, CISM, CGEIT

November 2, 2020

© 2020 Jack Henry & Associates, Inc.®

Sebastian Fazzino – CISSP, CISM, CGEIT
Director, Sales Operations ProfitStars

- 30 Years IT Operations, Sales & Marketing
- 20 Years, Cybersecurity & IT Compliance
- 20 Years servicing Financial Institutions
- ISACA, ISSA, InfraGard, AFT

It’s a scary world…

“90% of financial institutions reported being targeted by malware”

“Cybercrime Up 600% Due To COVID-19 Pandemic”

“Ransomware attacks are estimated to cost $6 trillion annually by 2021"

“34% of businesses hit with malware took a week or more to regain access to their data."

“92% of malware is delivered by email"

“7 out of every 10 malware payloads were ransomware"

“Over 18 million websites are infected with malware at a given time each week."

“98% of cyber attacks rely on social engineering"

“The total malware infections have been on the rise for the last ten years"

© 2020 Jack Henry & Associates, Inc.®

The 3 S’s of Cyber Defense

SIEM

Security Information & Event Management

SOAR

Security Orchestration Automation & Response

SOC

Security Operations Center

What is the difference with Next Gen SIEM (NG SIEM)?

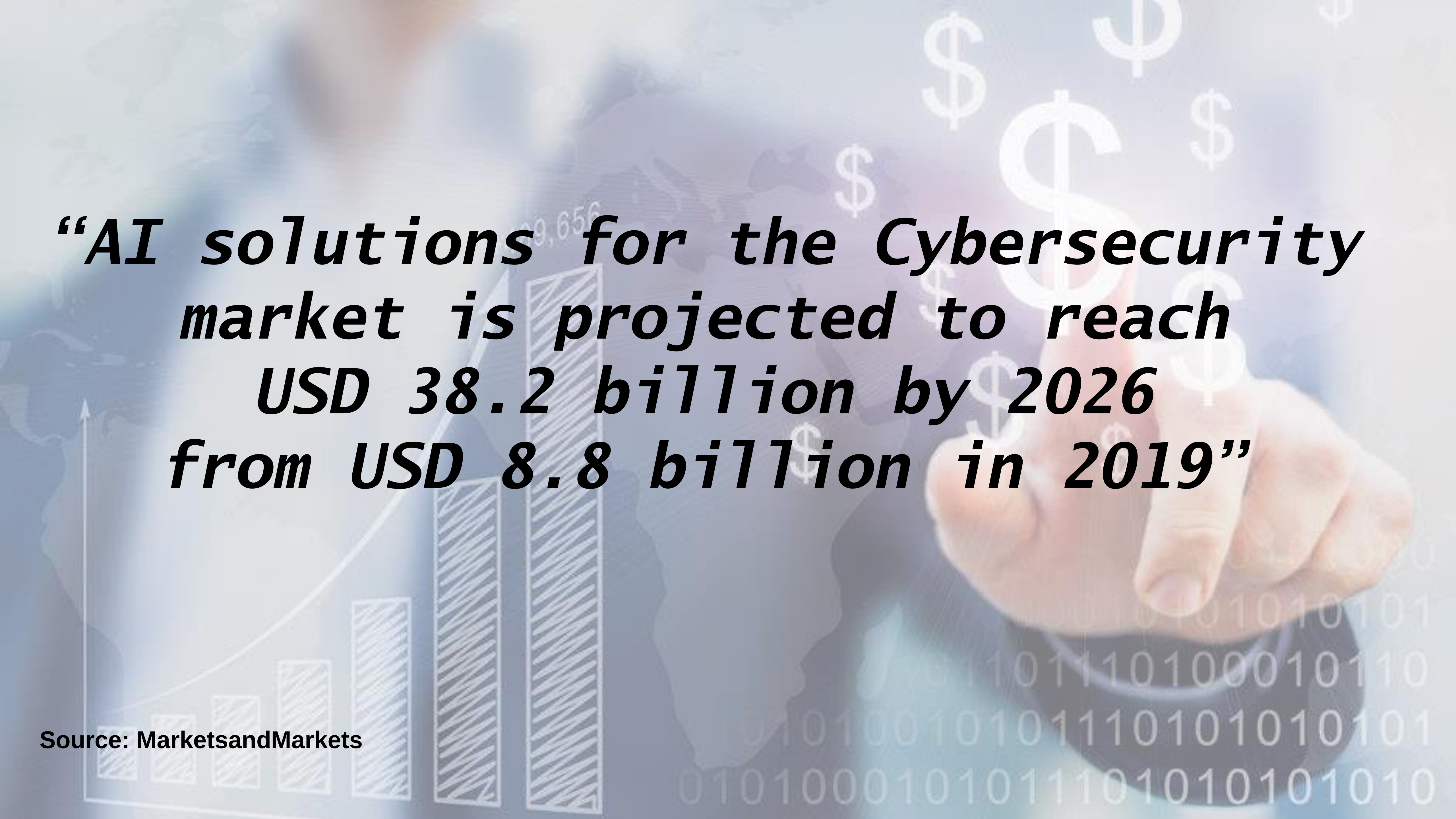
- Leverage NoSQL db’s (not only SQL)
- Asset and infrastructure awareness
- Apply context to security
- Machine Learning (ML)
  - – Cluster like events together and identify anomalies from learned behavior

© 2019 Jack Henry & Associates, Inc.®

What is the difference with NG SIEM?

- Timeline generation of related events
- Use Incident Response playbooks to perform automated responses to known threats
- Push response actions to devices like firewalls or IPSs

© 2019 Jack Henry & Associates, Inc.®

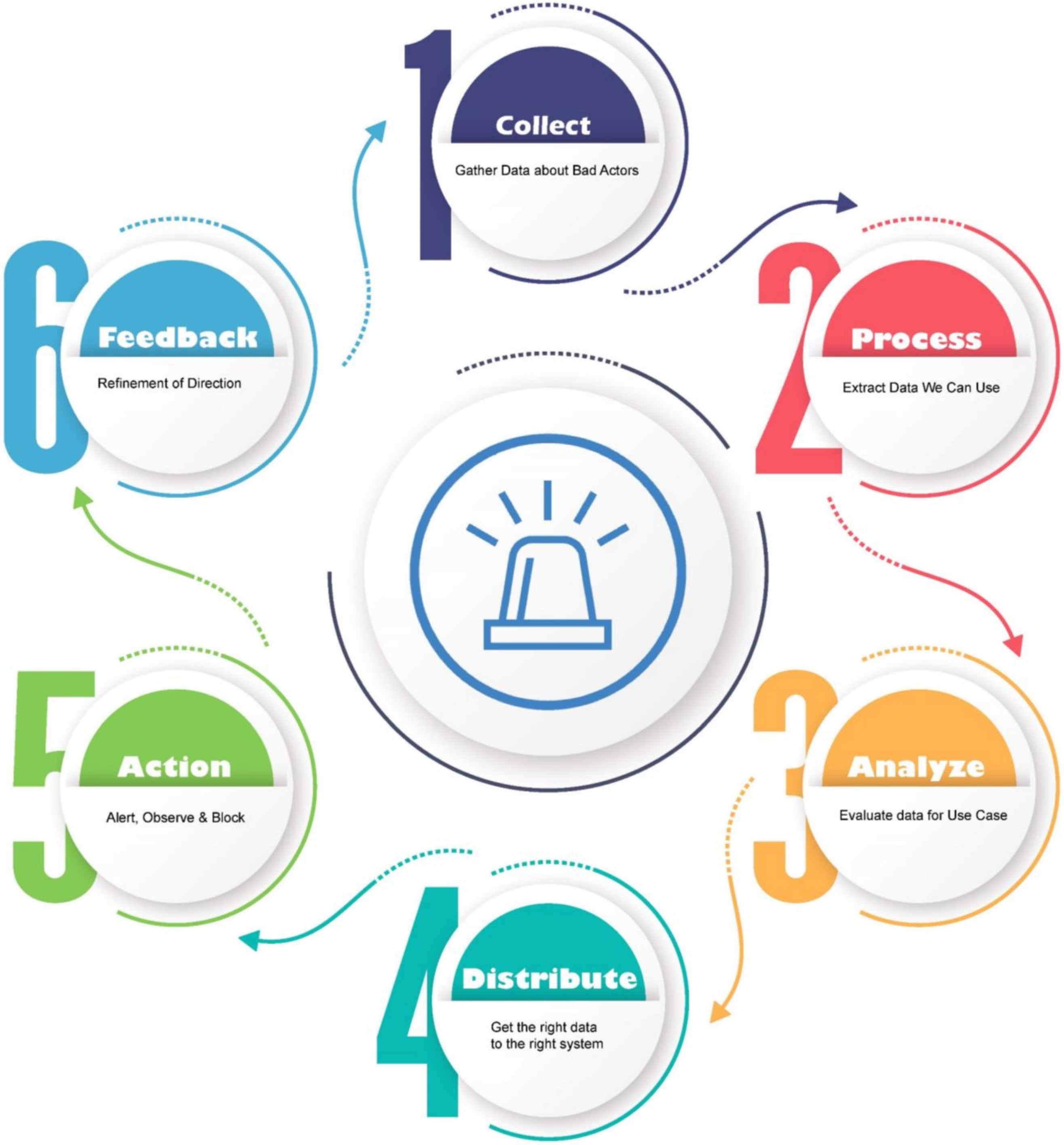


“AI solutions for the Cybersecurity market is projected to reach USD 38.2 billion by 2026 from USD 8.8 billion in 2019”

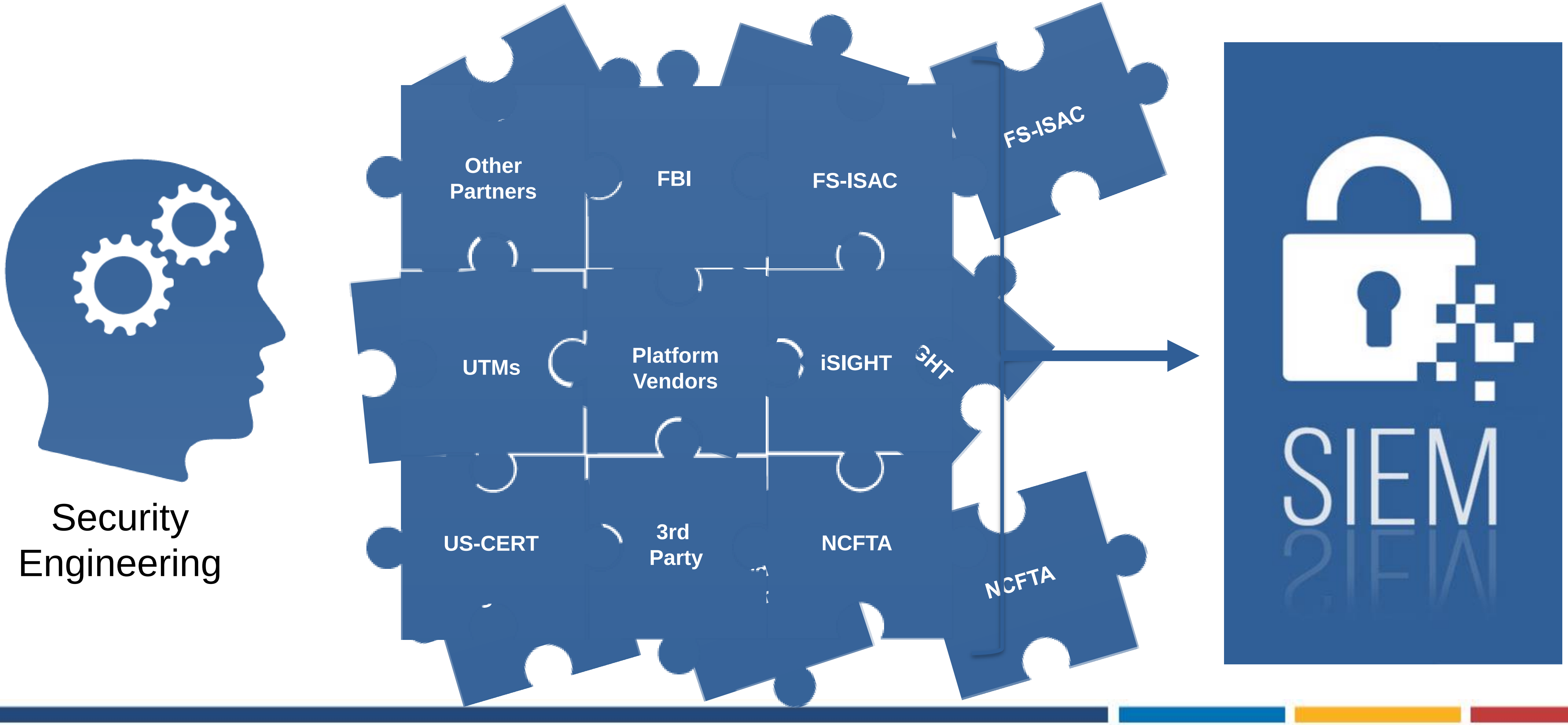
Source: MarketsandMarkets

Threat Intel

Threat intelligence is a component of security intelligence and includes both the information relevant to protecting an institution from external and inside threats as well as the processes, policies and tools designed to gather and analyze that information.



Applied Threat Intelligence



Security Engineering

Other Partners

FBI

FS-ISAC

FS-ISAC

UTMs

Platform Vendors

iSIGHT

GHT

US-CERT

3rd Party

NCFTA

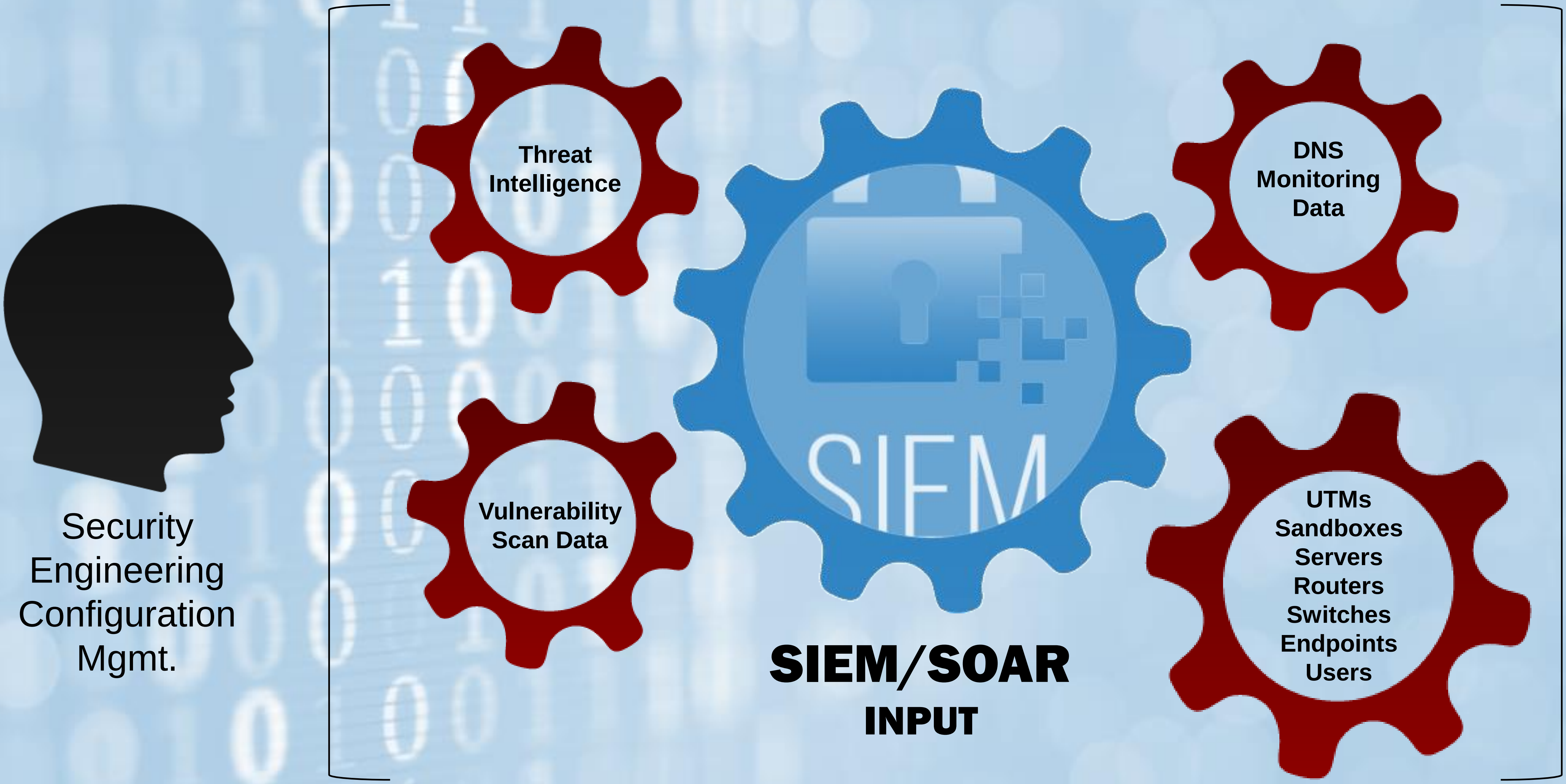
NCFTA

SIEM

© 2020 Jack Henry & Associates, Inc.®

CMDB - SIEM
(Configuration Management Database)

- Discover network assets dynamically
- Prioritizing threats by assets
- Alert on configuration changes
- Prioritizing threats by users



Security Engineering Configuration Mgmt.

Threat Intelligence

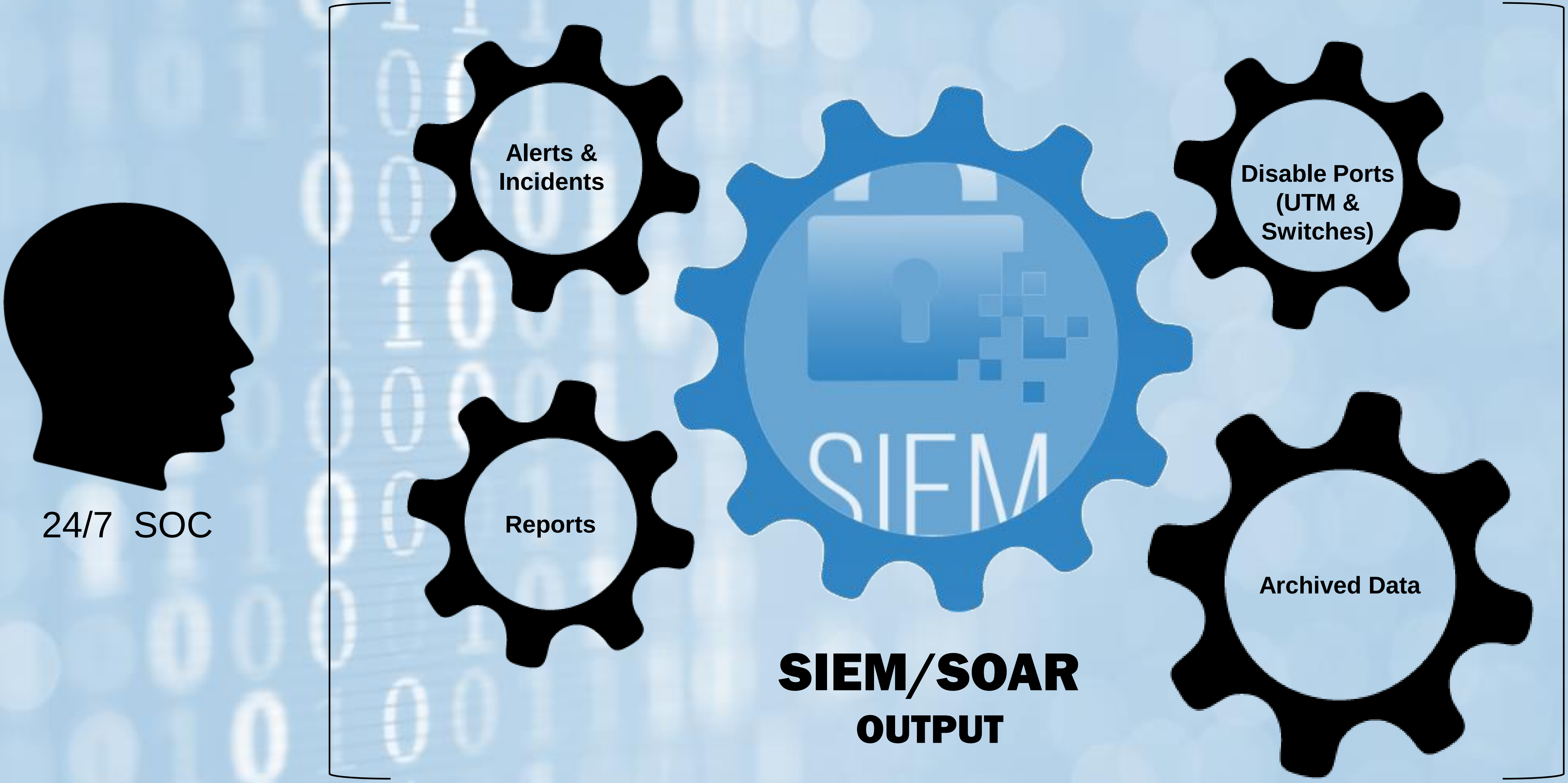
Vulnerability Scan Data

DNS Monitoring Data

UTMs
Sandboxes
Servers
Routers
Switches
Endpoints
Users

SIEM/SOAR

INPUT



24/7 SOC

Alerts & Incidents

Reports

Disable Ports (UTM & Switches)

Archived Data

SIEM/SOAR

OUTPUT

User & Entity Behavioral Analytics (UEBA)

1 SIEM profiles activity
Who | Where | How Many

Eg. User regularly logs on Mon - Fri 8am - 6pm

2 Behaviour compared against profile using probability distribution

Eg. User suddenly logs in Sunday at 8pm

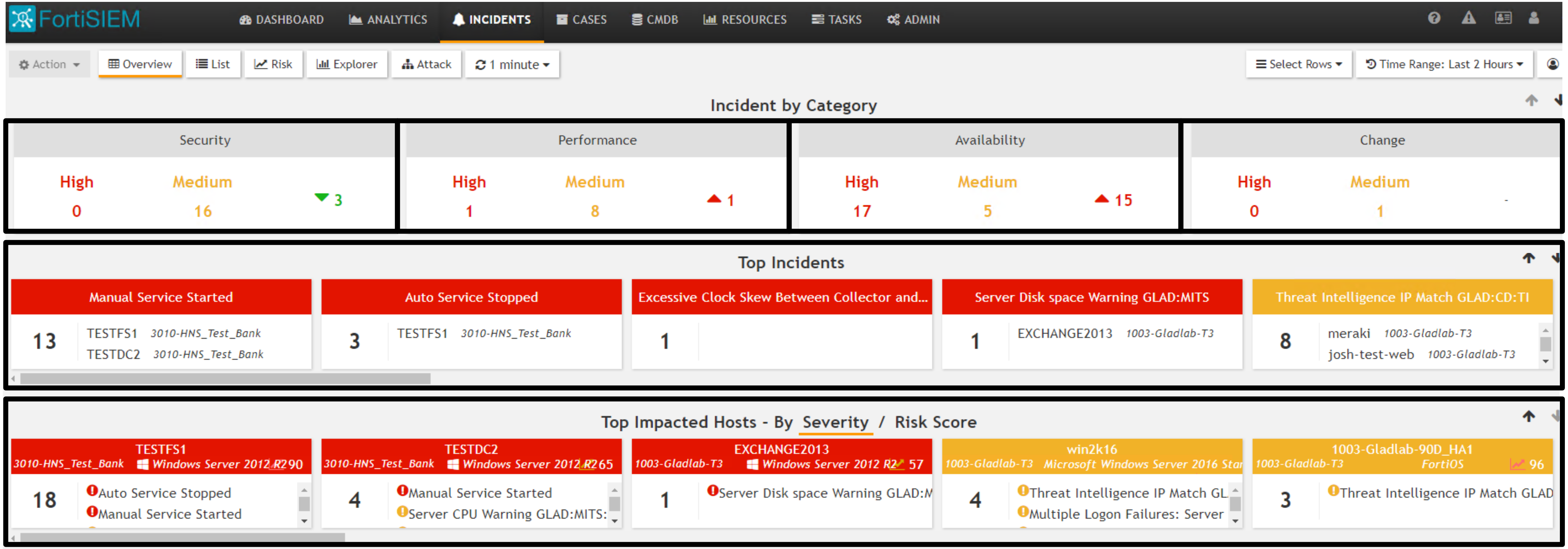
3 UEBA alerts are triggered when behaviour deviates from profile

UEBA alert !

- Advanced Behavioral Analytics Detects User Login Anomalies

© 2020 Jack Henry & Associates, Inc.®

Actionable Data Presented to SOC



Incident by Category

Security			Performance			Availability			Change		
High	Medium		High	Medium		High	Medium		High	Medium	
0	16	▼ 3	1	8	▲ 1	17	5	▲ 15	0	1	-

Top Incidents

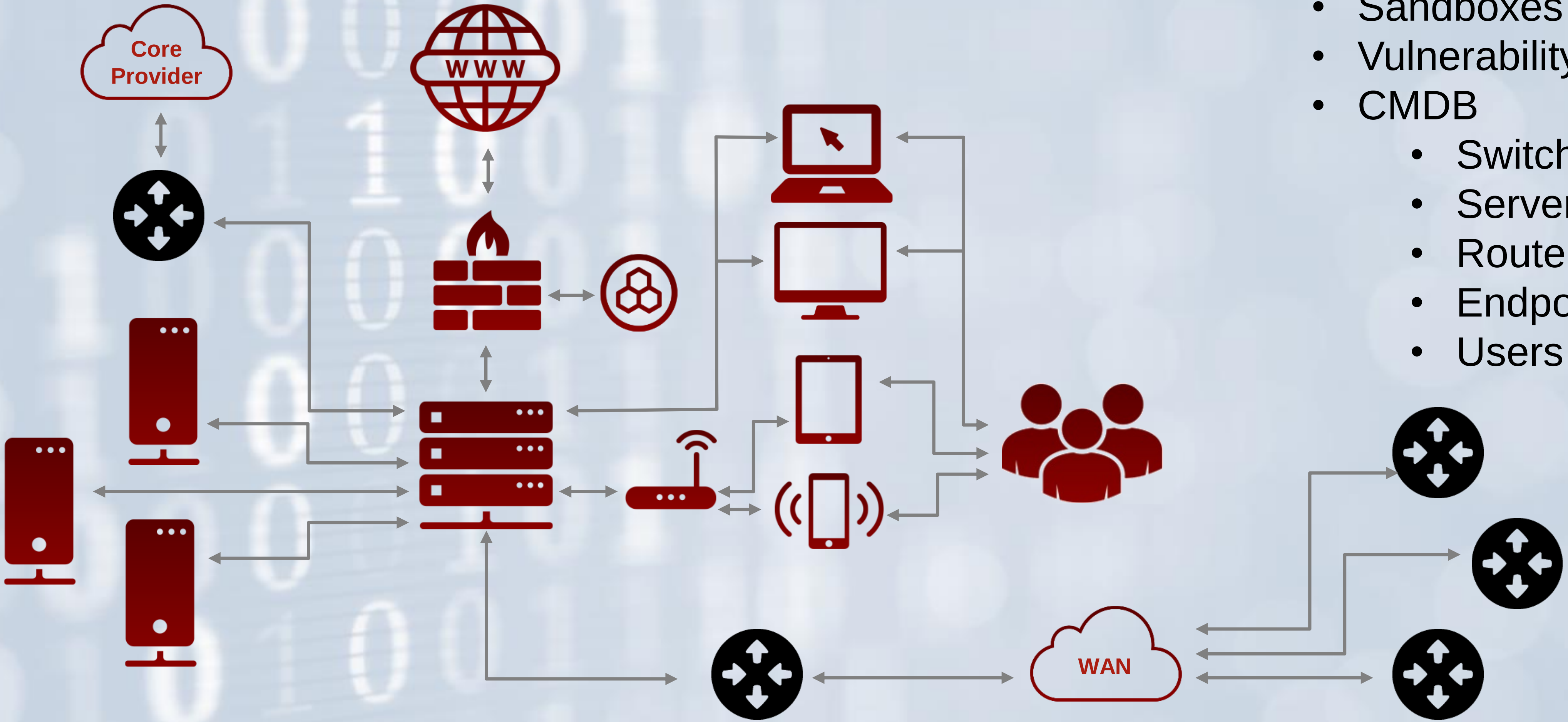
Manual Service Started	Auto Service Stopped	Excessive Clock Skew Between Collector and...	Server Disk space Warning GLAD:MITS	Threat Intelligence IP Match GLAD:CD:TI
13 TESTFS1 *3010-HNS_Test_Bank* TESTDC2 *3010-HNS_Test_Bank*	3 TESTFS1 *3010-HNS_Test_Bank*	1	1 EXCHANGE2013 *1003-Gladlab-T3*	8 meraki *1003-Gladlab-T3* josh-test-web *1003-Gladlab-T3*

Top Impacted Hosts - By Severity / Risk Score

TESTFS1 *3010-HNS_Test_Bank* *Windows Server 2012 R2* 90	TESTDC2 *3010-HNS_Test_Bank* *Windows Server 2012 R2* 65	EXCHANGE2013 *1003-Gladlab-T3* *Windows Server 2012 R2* 57	win2k16 *1003-Gladlab-T3* *Microsoft Windows Server 2016 Star*	1003-Gladlab-90D_HA1 *1003-Gladlab-T3* *FortiOS* 96
18 Auto Service Stopped Manual Service Started	4 Manual Service Started Server CPU Warning GLAD:MITS:	1 Server Disk space Warning GLAD:M	4 Threat Intelligence IP Match GL Multiple Logon Failures: Server	3 Threat Intelligence IP Match GLAD

© 2020 Jack Henry & Associates, Inc.®

Achieve Total Visibility



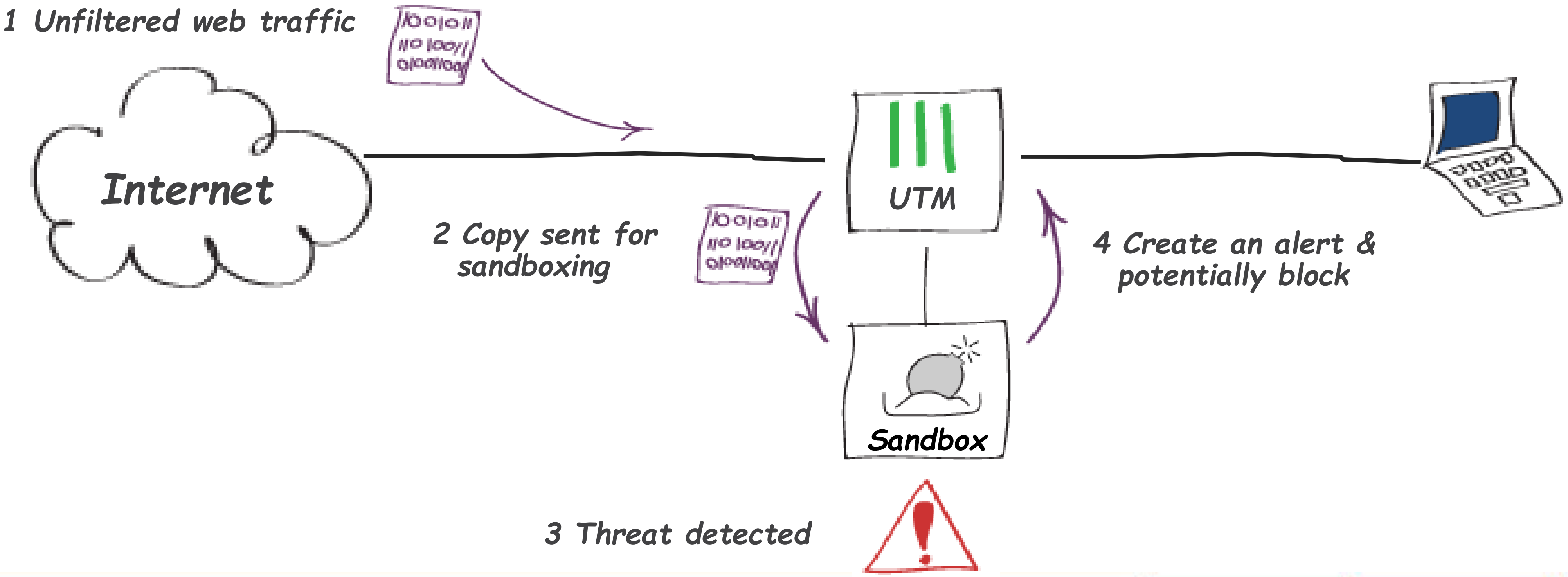
NG SIEM/SOAR:

- Threat Intelligence
- DNS Monitoring Data
- UTMs
- Sandboxes
- Vulnerability Scan Data
- CMDB
  - Switches
  - Servers
  - Routers
  - Endpoints
  - Users

What else can we do to increase Cyber Resiliency?

Sandbox

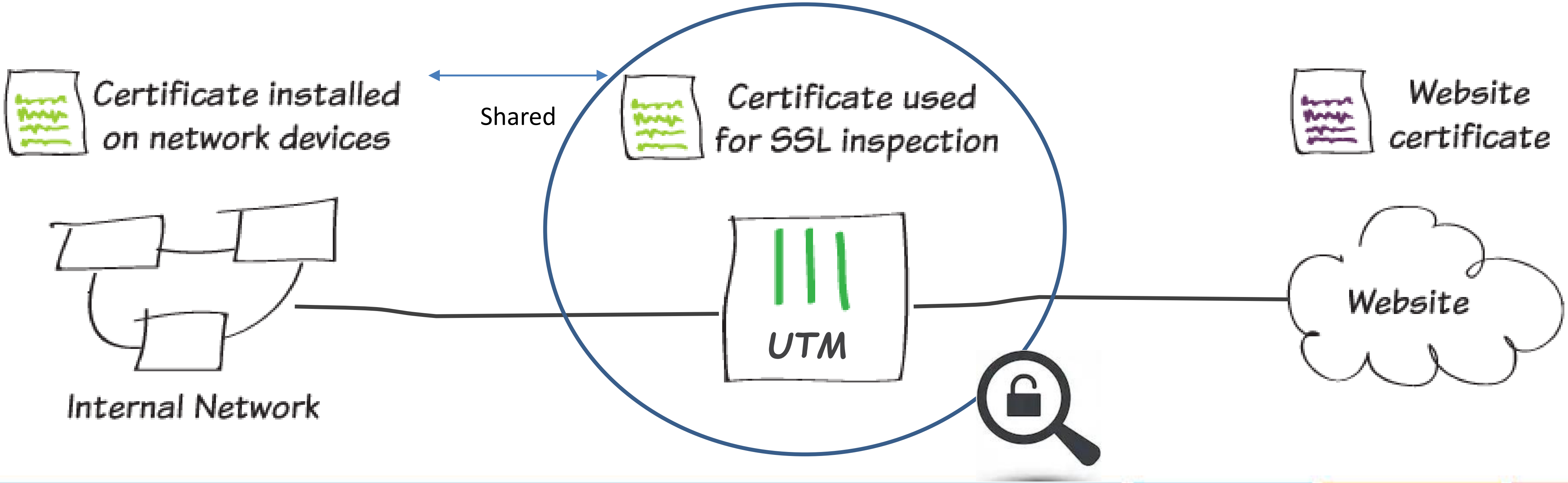
- Early Breach Detection
- Detects unknown threats


1 Unfiltered web traffic
Internet
2 Copy sent for sandboxing
UTM
Sandbox
3 Threat detected
4 Create an alert & potentially block

© 2020 Jack Henry & Associates, Inc.®

Encrypted Web Browsing

- 75% of web traffic is encrypted
- Encrypted data cannot be inspected
- SSL – DPI (Secure Socket Layer – Deep Packet Inspection)

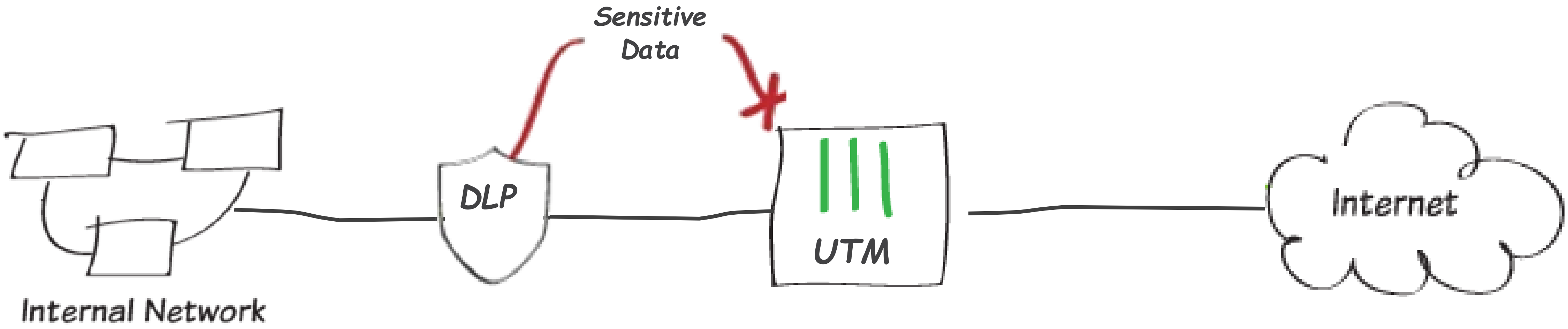


Certificate installed on network devices
Shared
Certificate used for SSL inspection
Website certificate
Internal Network
UTM
Website

© 2020 Jack Henry & Associates, Inc.®

Data Leak Prevention (DLP)

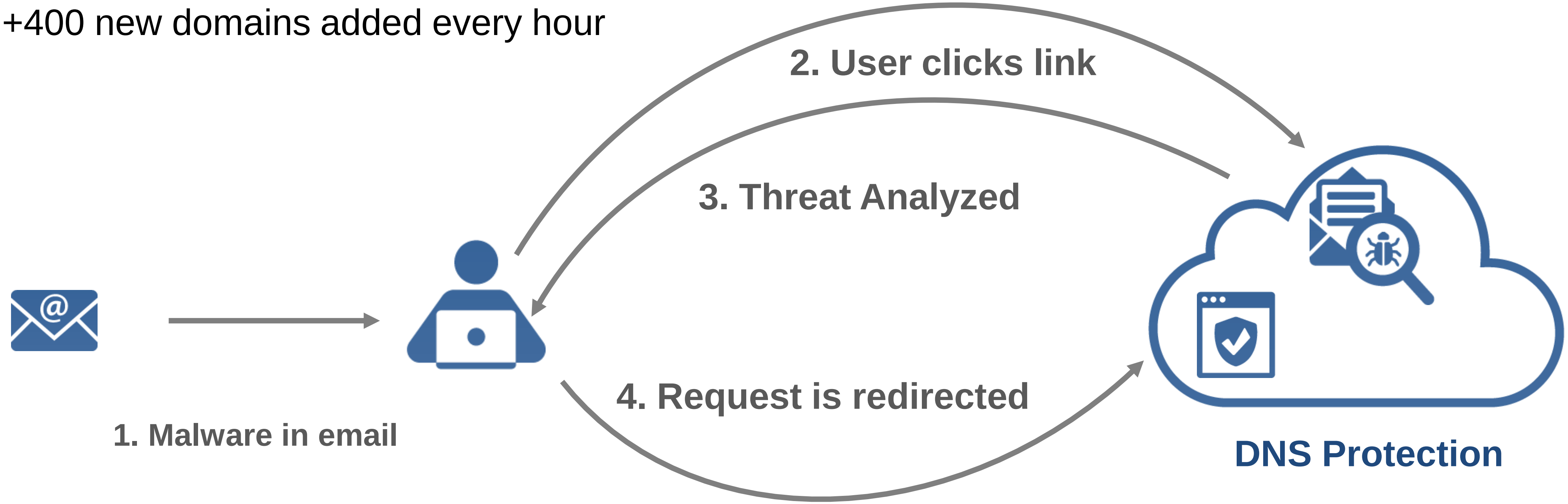
- Keep files containing sensitive information from leaving your network
- Data Leak Prevention (DLP) security profile
- Retain Windows executable (.exe) files and files matching a specific file name pattern



© 2020 Jack Henry & Associates, Inc.®

DNS Protection

- Block access to websites with known malicious code
  - +1.3 Million malicious domain entries
- Detect & block newly observed domains
  - +400 new domains added every hour



2. User clicks link

3. Threat Analyzed

1. Malware in email

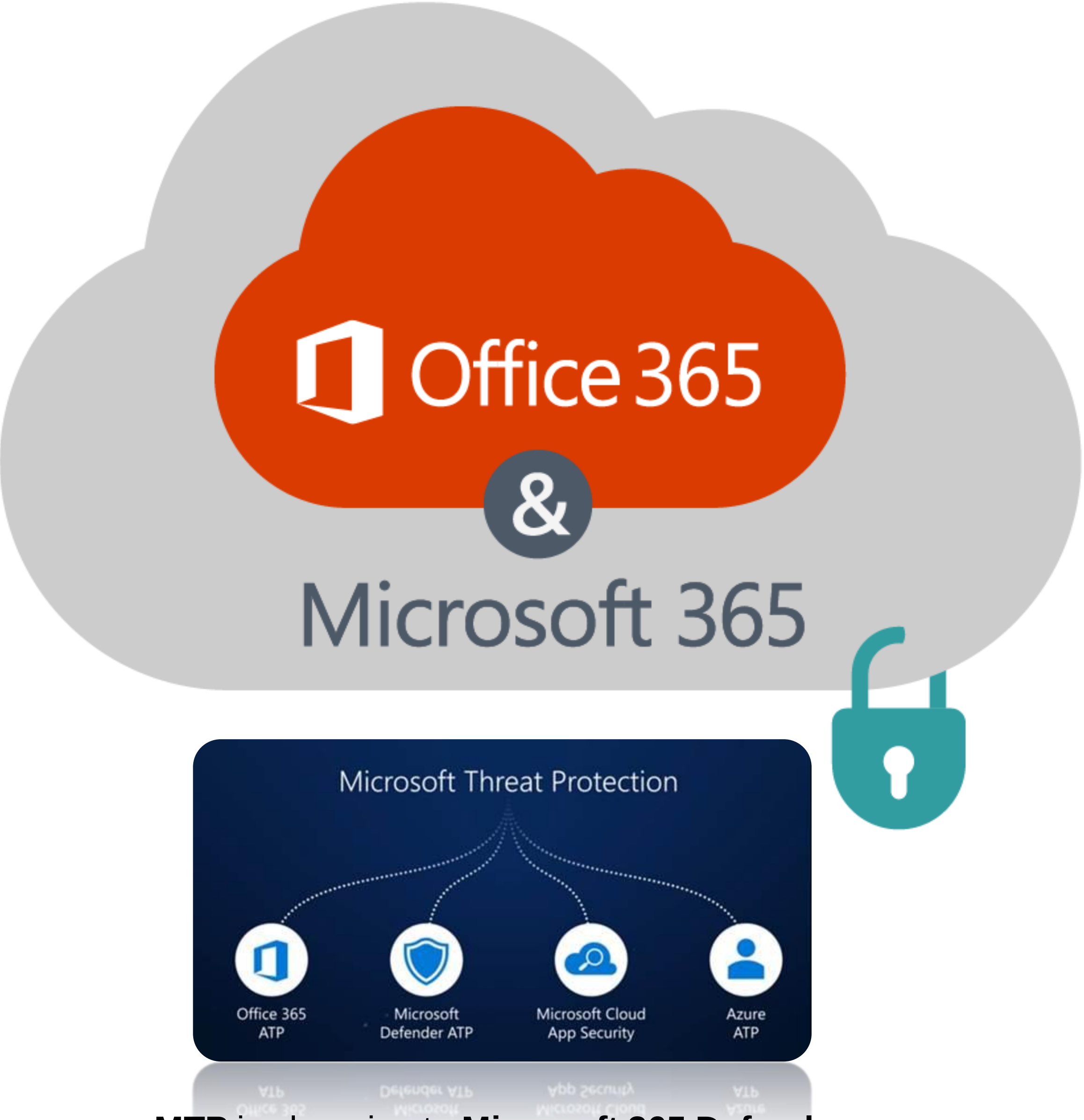
4. Request is redirected

DNS Protection

© 2020 Jack Henry & Associates, Inc.®

Securing Email with M365 E3 & E5

- Microsoft Threat Protection
  - Supports MFA
  - Windows Defender Antivirus
    - Part of MS Defender ATP
  - Encrypted Email
  - Data Loss Prevention (SSN, CC, Acct, etc.)
  - Mobile Device Management – basic included
    - Intune add-on
  - Advanced Threat Protection (AV-SPAM)
  - Sensitivity Labels
    - "Do not forward" & "Do not copy"
- NG-SIEM integration

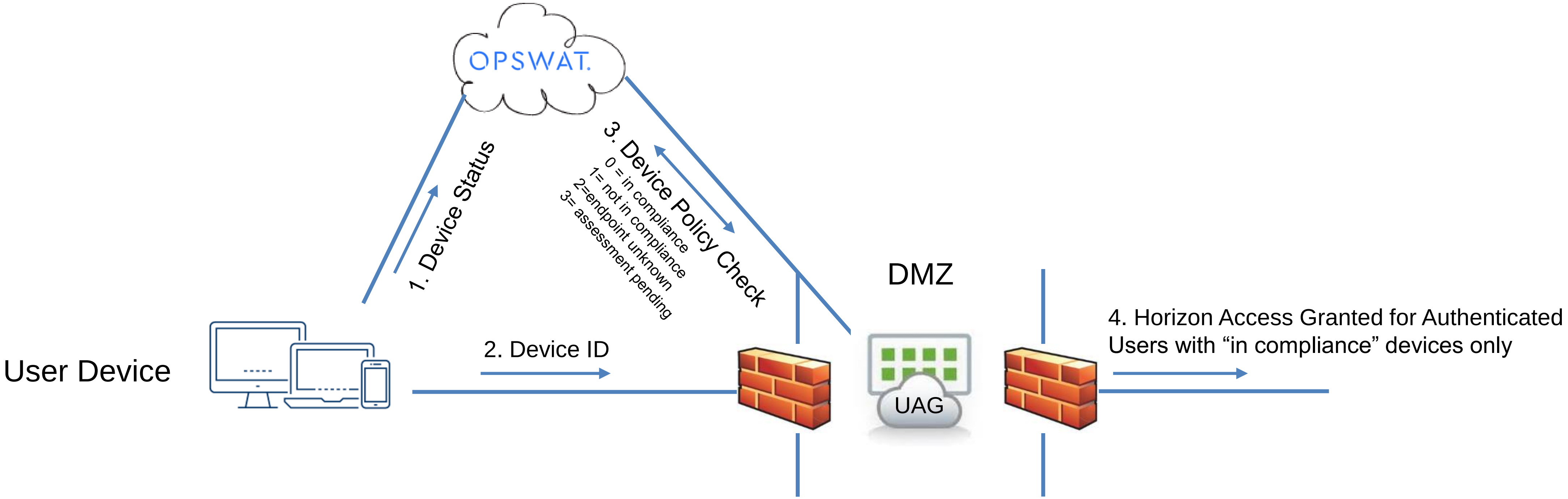


MTP is changing to **Microsoft 365 Defender**

© 2020 Jack Henry & Associates, Inc.®

Remote User Access Control with VMware

- Ensure compliance with remote users connecting from personal devices
- VMware Unified Access Gateway
- Endpoint Compliance Check



OPSWAT.

1. Device Status

3. Device Policy Check

0 = in compliance
1= not in compliance
2=endpoint unknown
3= assessment pending

DMZ

User Device

2. Device ID

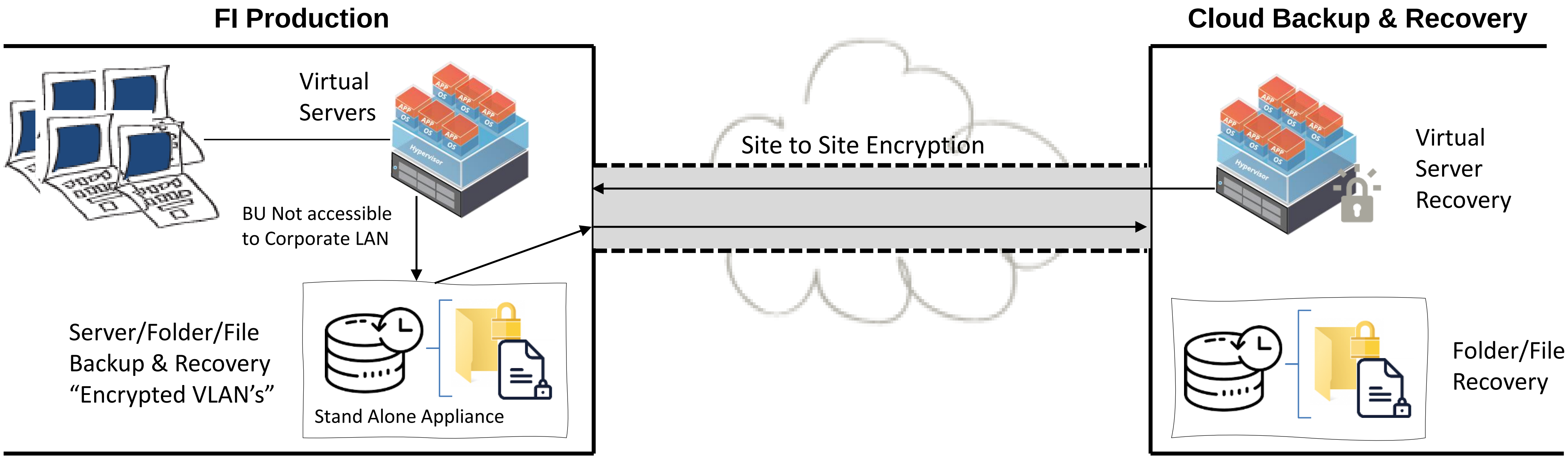
UAG

4. Horizon Access Granted for Authenticated Users with “in compliance” devices only

© 2020 Jack Henry & Associates, Inc.®

Air Gapped Backup & Recovery

- Protect data from ransomware
- Air gapped from FI's network
- Granular folder/file restoration
- Virtual server recovery

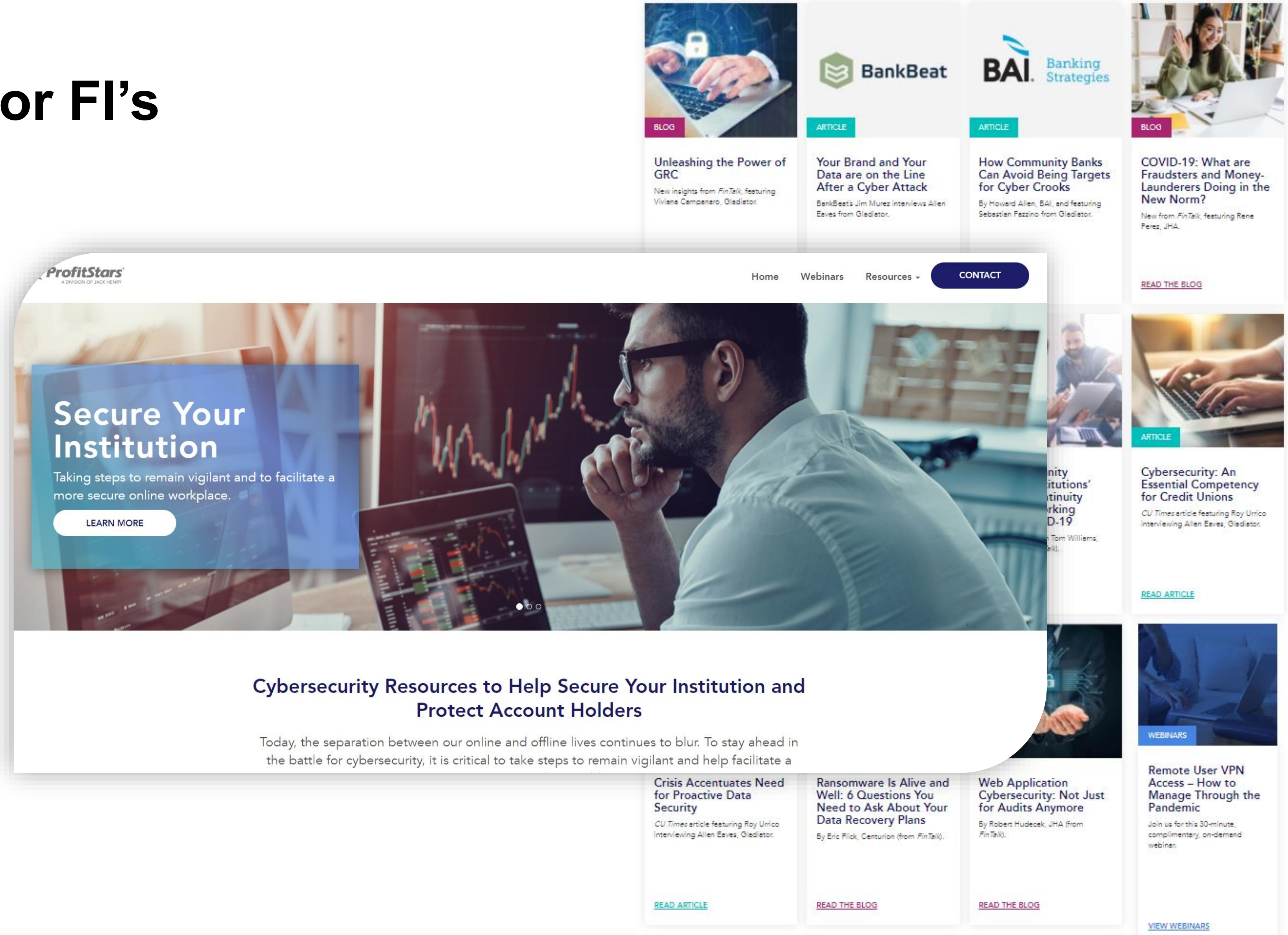


© 2020 Jack Henry & Associates, Inc.®

Resource Center for FI’s

profitstars.com/cybersavvy

- Blogs
- Whitepapers
- Webinars
- Published articles
- Cybersecurity Forums



Secure Your Institution

Taking steps to remain vigilant and to facilitate a more secure online workplace.

Cybersecurity Resources to Help Secure Your Institution and Protect Account Holders

Today, the separation between our online and offline lives continues to blur. To stay ahead in the battle for cybersecurity, it is critical to take steps to remain vigilant and help facilitate a

BLOG

Unleashing the Power of GRC

New insights from *FinTalk*, featuring Viviana Campanero, Gladiator.

ARTICLE

Your Brand and Your Data are on the Line After a Cyber Attack

BankBeat’s Jim Murez interviews Allen Eaves from Gladiator.

ARTICLE

How Community Banks Can Avoid Being Targets for Cyber Crooks

By Howard Allen, BAI, and featuring Sebastian Fazzino from Gladiator.

BLOG

COVID-19: What are Fraudsters and Money-Launderers Doing in the New Norm?

New from *FinTalk*, featuring Rene Perez, JHA.

READ THE BLOG

nity
itutions’
tinuity
rking
D-19

Tom Williams,
alk).

ARTICLE

Cybersecurity: An Essential Competency for Credit Unions

CU Times article featuring Roy Urrico interviewing Allen Eaves, Gladiator.

READ ARTICLE

Crisis Accentuates Need for Proactive Data Security

CU Times article featuring Roy Urrico interviewing Allen Eaves, Gladiator.

READ ARTICLE

Ransomware Is Alive and Well: 6 Questions You Need to Ask About Your Data Recovery Plans

By Eric Flick, Centurion (from *FinTalk*).

READ THE BLOG

Web Application Cybersecurity: Not Just for Audits Anymore

By Robert Hudecek, JHA (from *FinTalk*).

READ THE BLOG

WEBINARS

Remote User VPN Access – How to Manage Through the Pandemic

Join us for this 30-minute, complimentary, on-demand webinar.

VIEW WEBINARS

Gladiator™

- **TotalProtect Suite**
  - Complete suite of cybersecurity services
  - New advanced SIEM / SOAR Platform
  - Enhanced Threat Intel Platform, built solely for FI’s
  - Complete UTM Management & Monitoring
  - SIEM Monitoring, Alerting & Reporting
  - DNS Protection
  - Enterprise Vulnerability Scanning
  - OS and Application Patching
  - Endpoint Security Management
  - Data Backup and Recovery
- **The Power of Next-Gen SIEM and SOAR, Part 1 & 2**

https://discover.profitstars.com/cyber-security/business-resources

© 2020 Jack Henry & Associates, Inc.®

Thank You!

© 2020 Jack Henry & Associates, Inc.®