Webinar 4 - SIEM Part 1

File Integrity & Authentication Monitoring

Sebastian Fazzino – CISSP, CISM, CGEIT

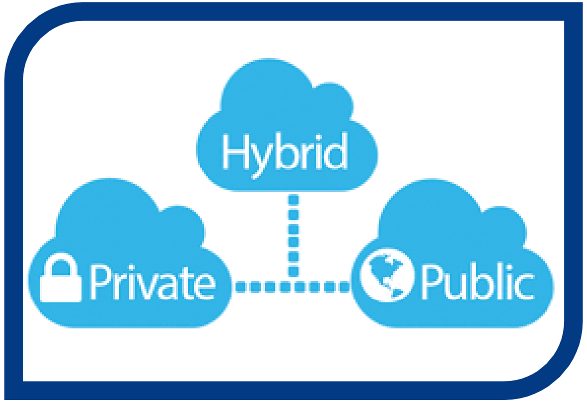
February 24, 2022

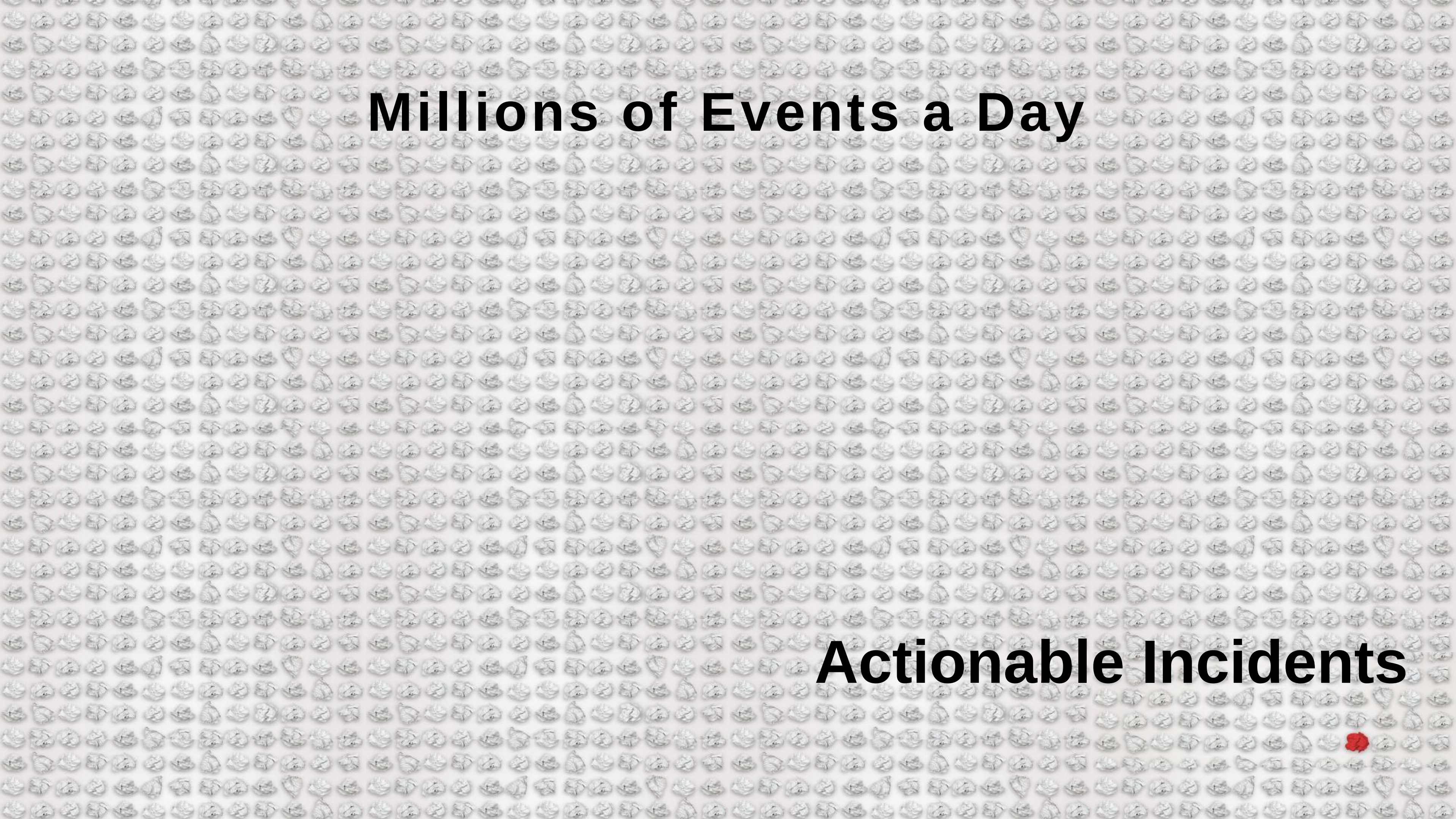
Today’s Banking Security Dilemma

Cyber Threats

Talent Shortage

Complex Environments

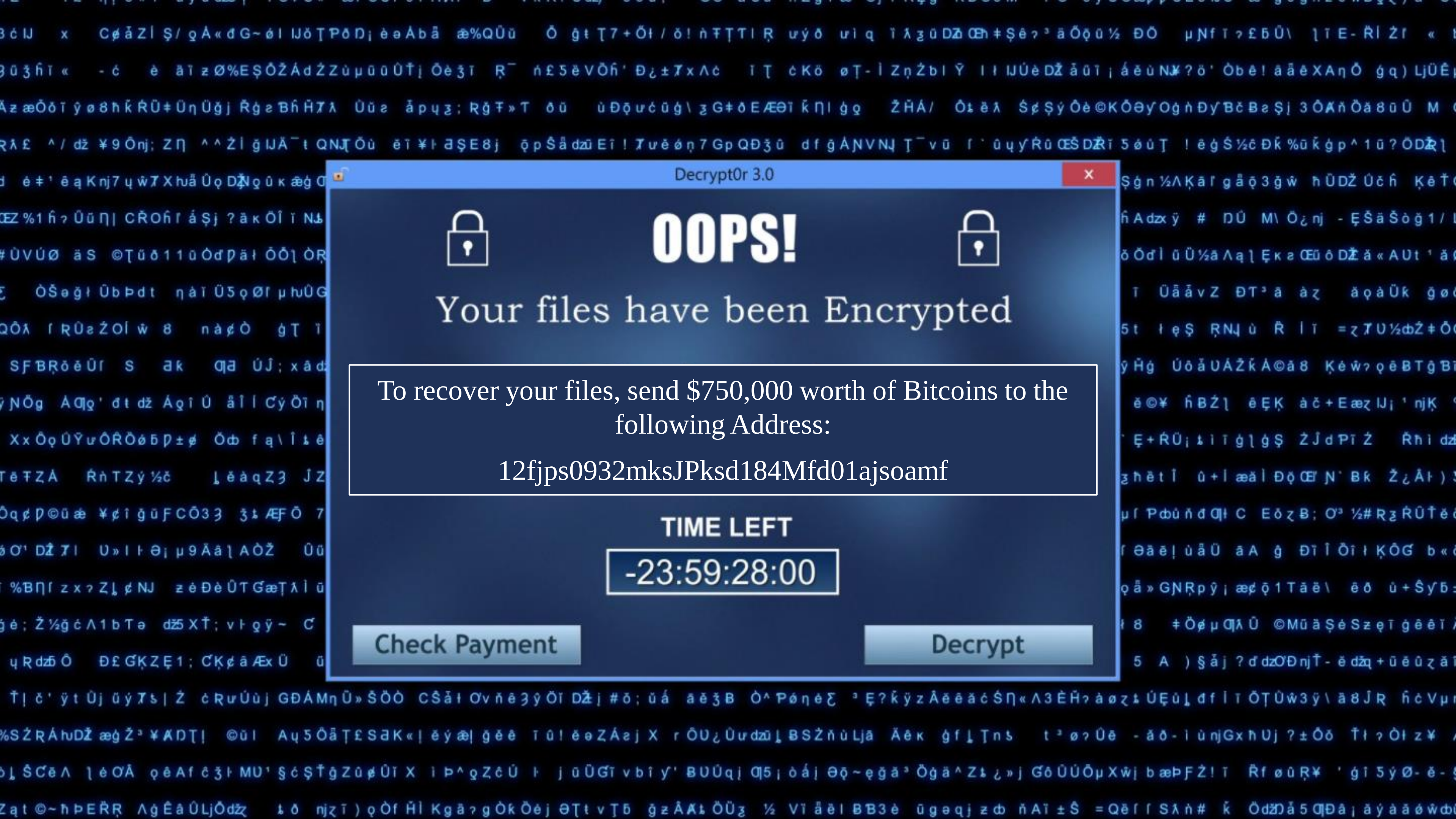




Millions of Events a Day

Actionable Incidents

ZERO DAY



OOPS!

Your files have been Encrypted

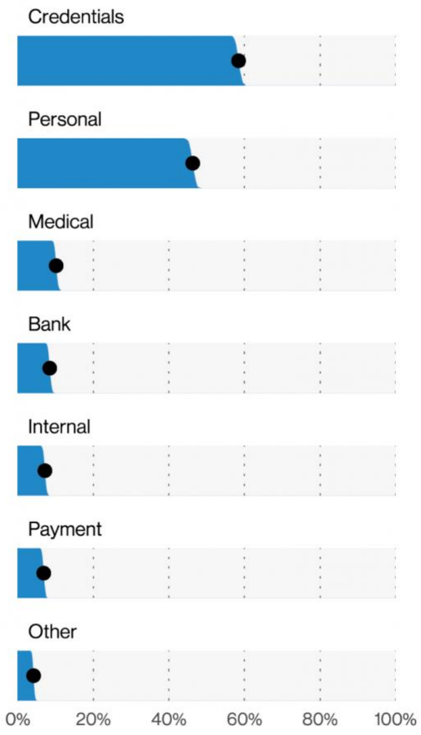
To recover your files, send $750,000 worth of Bitcoins to the following Address:

12fjps0932mksJPksd184Mfd01ajsoamf

TIME LEFT

-23:59:28:00

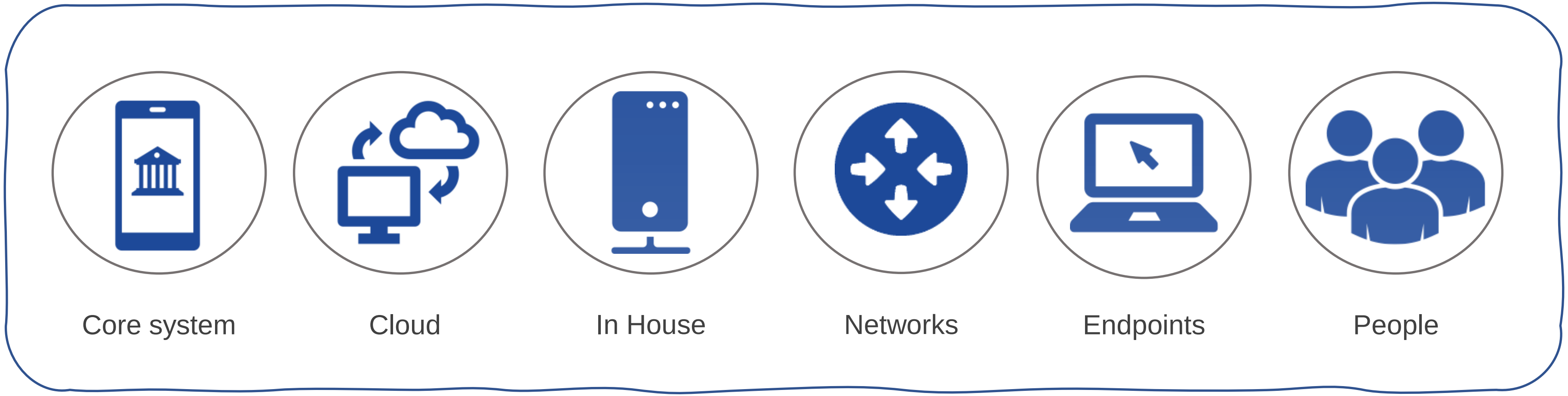
Criminals Want Credentials



- Credentials are the glazed donut of data types
- Stolen Credentials Fuel Rise In Ransomware
- Social Engineering
- Brute Force/Credential Stuffing Attacks

Source: Verizon 2021 Data Breach Investigations

Your Institution



Core system

Cloud

In House

Networks

Endpoints

People

Protecting your Institution

Data Security

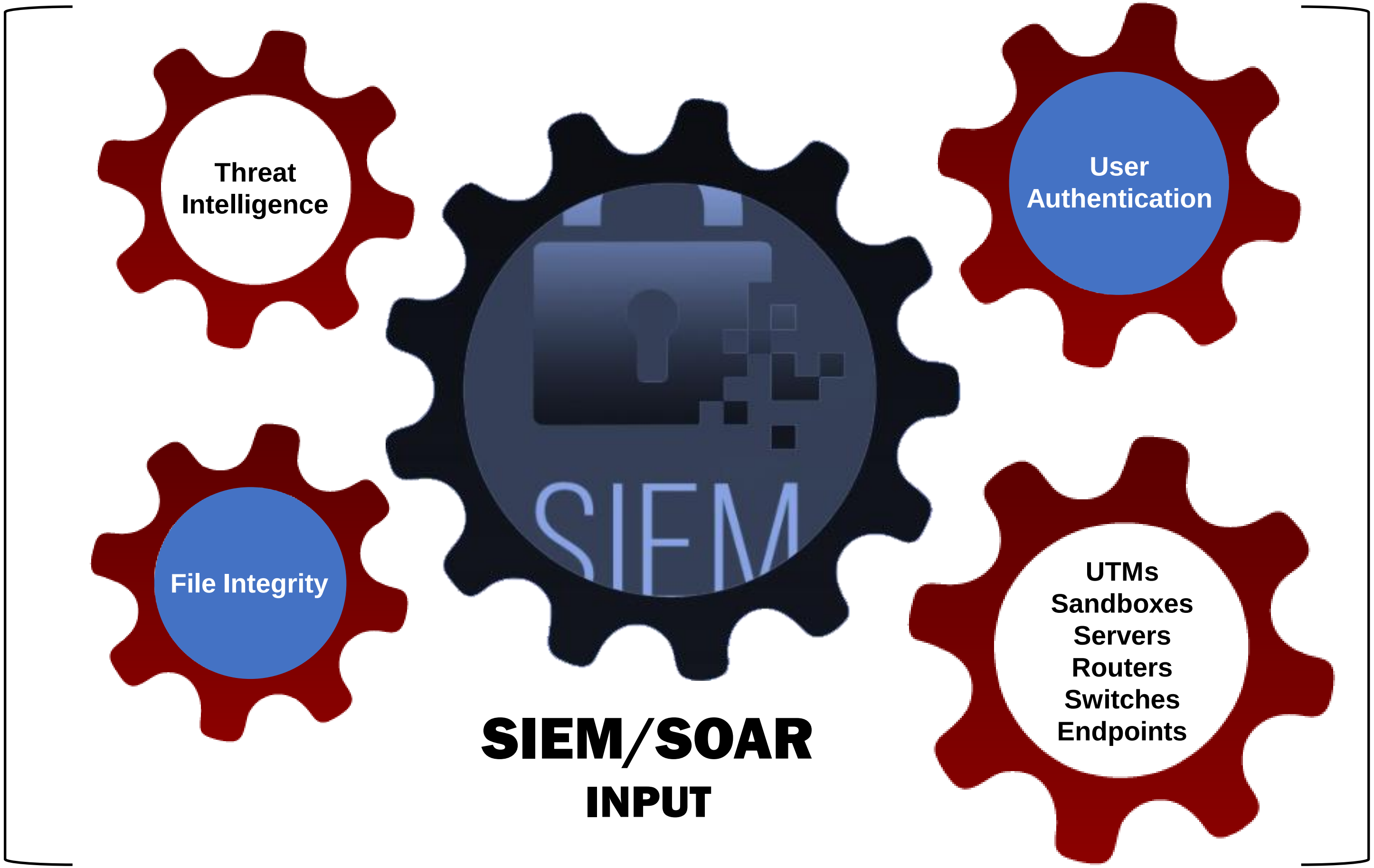
- Confidentiality, Integrity

System Availability

- 24x7 access

Regulatory Compliance

Security Engineering Configuration Management



Threat Intelligence

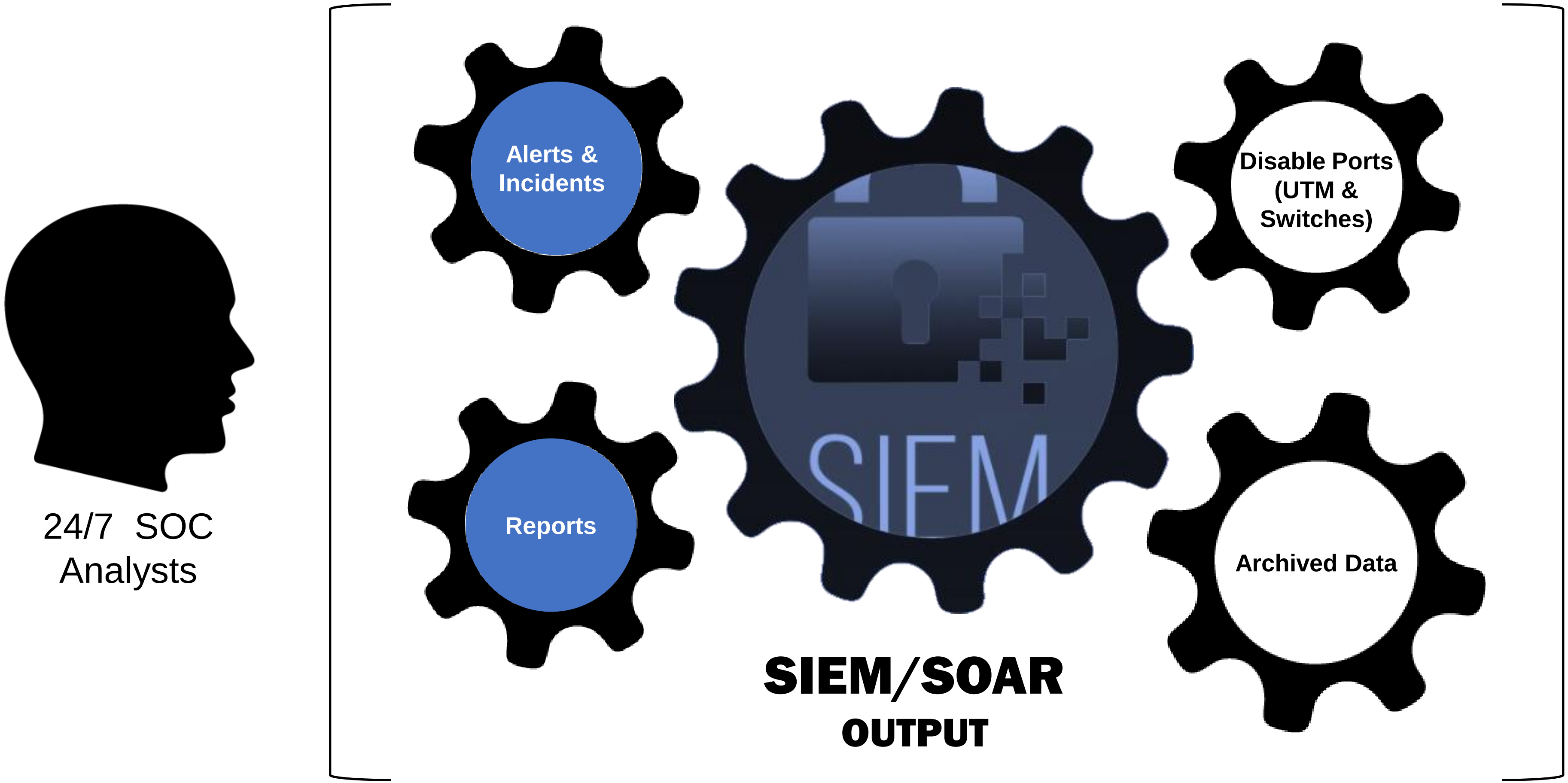
File Integrity

User Authentication

UTMs
Sandboxes
Servers
Routers
Switches
Endpoints

SIEM/SOAR

INPUT



24/7 SOC Analysts

Alerts & Incidents

Reports

Disable Ports (UTM & Switches)

Archived Data

SIEM/SOAR

OUTPUT

Authentication Monitoring

cisco | DUO

OPSWAT.

{okta}

Radius

Office 365

Multi-factor Authentication

FORTINET

FortiAuthenticator

vmware

Horizon View

SIEM Authentication Monitoring

- Integrate the monitoring of your authentication services into a SIEM platform.
- Provide rapid notifications of authentication requests that may be resulting from suspicious or malicious behavior.

SIEM Authentication Monitoring

- Notify and Report the following type of events:
  - ✓Successful logons
  - ✓Successful logon from outside the USA
  - ✓Administrator failed logons
  - ✓Failed logons followed by a successful logon
  - ✓Multiple logon failures
  - ✓Admin logons
  - ✓User logoff
  - ✓User lockout
  - ✓User account disabled
  - ✓User password expired

Administrator Failed Logons

- An alert is issued for failed logons on an administrator-level account.
- Email and phone call to the contacts for review
- Successful administrator logons are recorded and are accessible via Reports

Multiple Logon Failures

- An alert is issued when multiple non-administrative accounts failing to authenticate over a short period.
- This activity may indicate that the account is under attack, or a system is misconfigured.
- Email and phone call to the contacts for review

Failed Logons Followed by Successful Logon

- An alert is issued when multiple failed logons followed by a successful login is detected
- This activity may be benign, but it could also be malicious activity and indicate a successful brute force attempt to crack a password.
- Email and phone call to the contacts for review

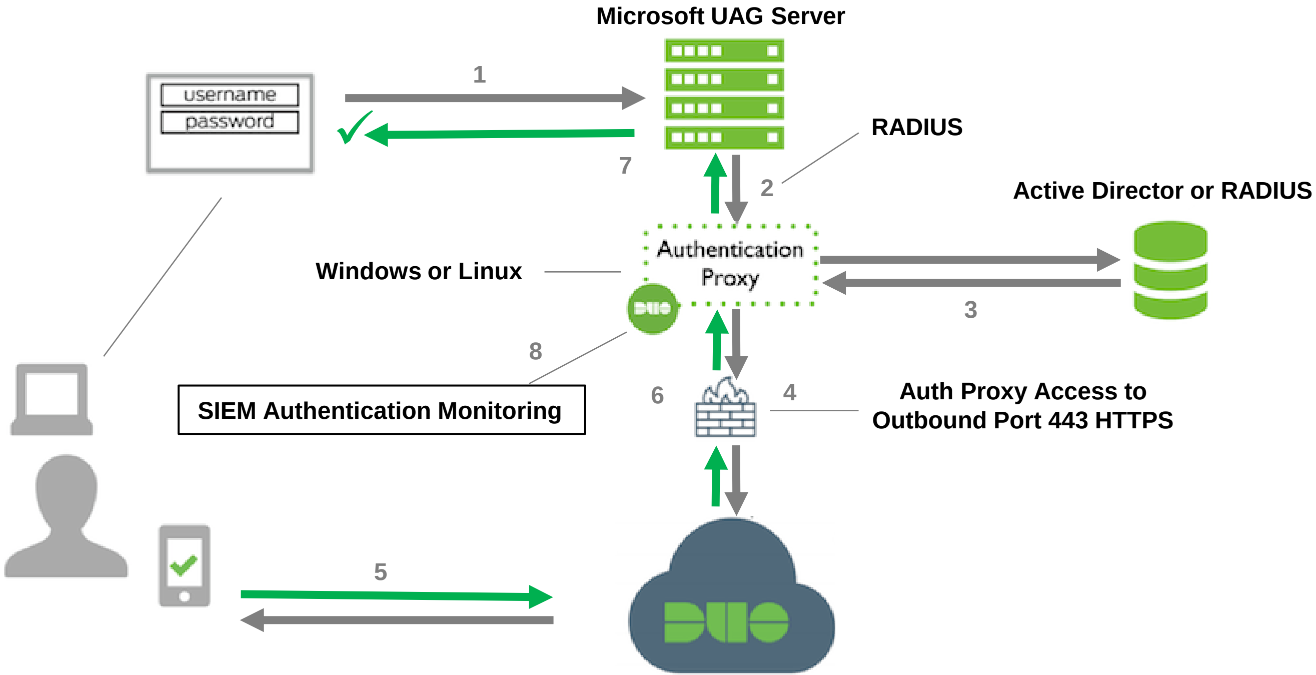
Successful Logons

- Successful logon activity is captured.
- This activity is generally not a security risk and as such is not actively alerted.
- Reports provide an overview of the activity and trends for user authentication.

Successful Logon from Outside the USA

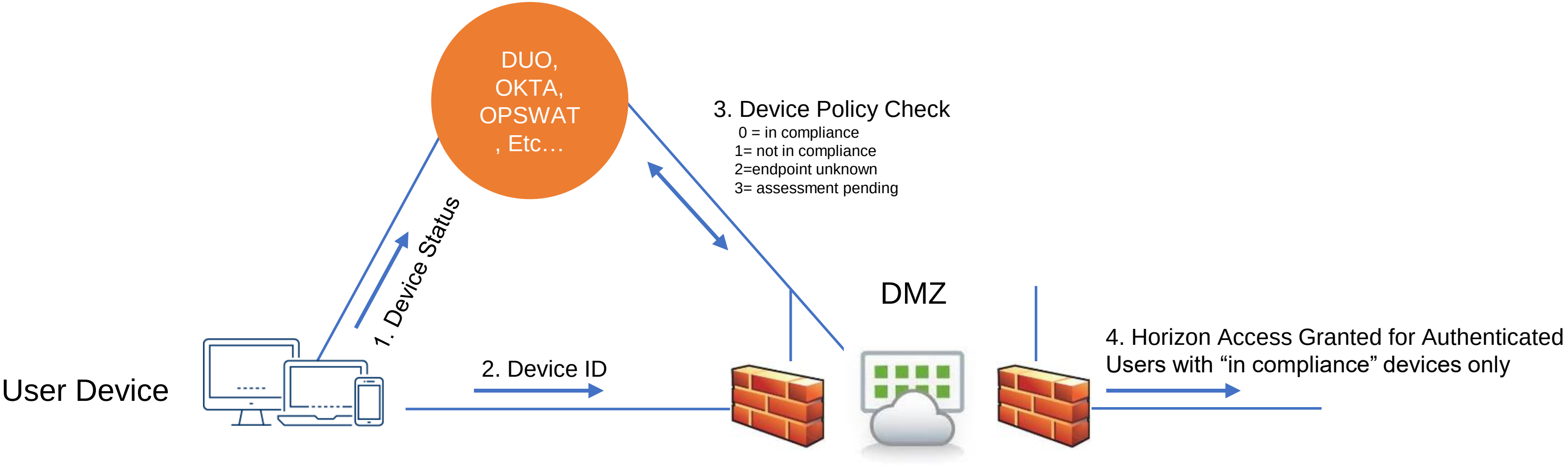
- Alerts are generated for successful logon activity sourced from outside the United States of America (50 states)
- This activity could be benign, but it could also be indicative of a compromised account.
- Email and phone call to the contacts for review

SIEM Authentication Monitoring


Microsoft UAG Server
username
password
1
7
RADIUS
2
Active Director or RADIUS
Authentication Proxy
Windows or Linux
3
8
SIEM Authentication Monitoring
6
4
Auth Proxy Access to Outbound Port 443 HTTPS
5

VDI - Remote User Access Control

- Ensure compliance with remote users connecting from personal devices



SIEM Authentication Monitoring

- Authentication requests could be the result of suspicious or malicious behavior
- Review your Access Management Policy.
- Monitoring Mitigates!

File Integrity Monitoring (FIM)

1

Support Data Classification

2

Examine files and folders to see when they change, how they change & who changed them

3

Determine what can be done to restore those files if those modifications are unauthorized

File Integrity Monitoring Advantages

Protect IT Infrastructure

FIM solutions monitor file changes on servers, databases, network devices, directory servers, applications, cloud environments, virtual images, and alert you of unauthorized changes.

Reduce Noise

Noise: A strong FIM solution uses change intelligence to only notify you when needed.

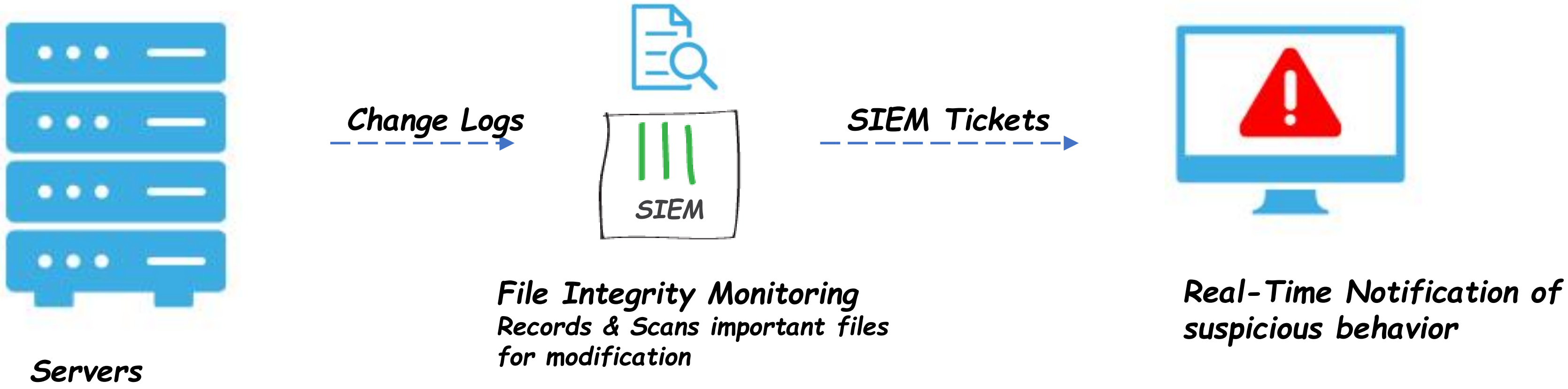
Stay Compliant

FIM helps you meet many regulatory compliance standards like GLBA, PCI-DSS, SOX, NIST and best practice frameworks like the Center for Internet Security (CIS)

Best Practices to Deploy FIM

Set Policy	Define a relevant policy. Identify which files on which computers your institution needs to monitor.

SIEM File Integrity Monitoring



Servers

Change Logs

SIEM

File Integrity Monitoring

Records & Scans important files for modification

SIEM Tickets

Real-Time Notification of suspicious behavior

File Integrity Monitoring

- Every security breach begins with a single change.
- A small alteration to one file can expose your whole network to a potential attack.
- FIM is about keeping track of an established baseline and alerting you to any unexpected changes that may represent a security risk or a compromise in regulatory compliance.

In Summary

Authentication requests could be the result of suspicious or malicious behavior.

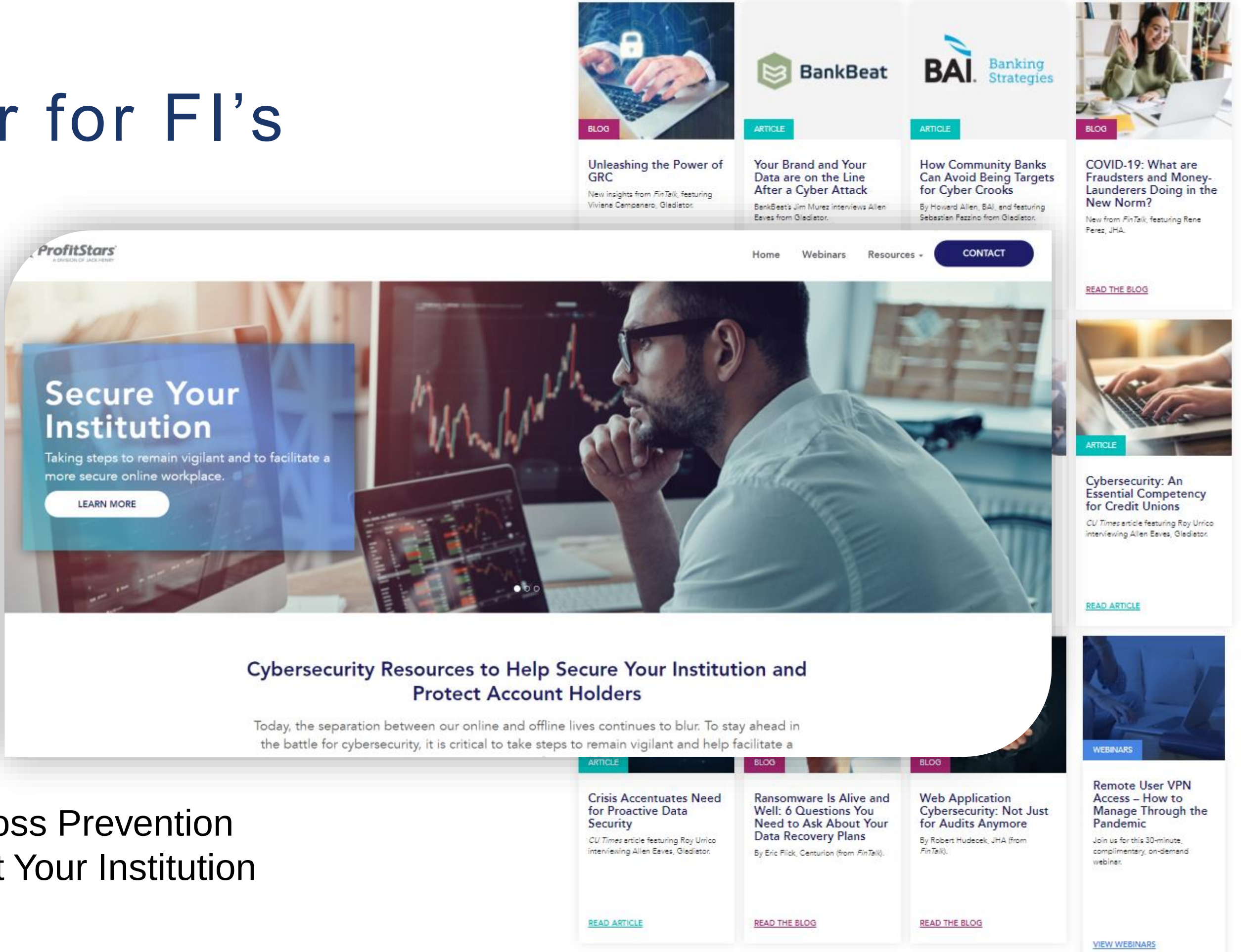
A small alteration to one file can expose your whole network to a potential attack.

Monitoring with a SIEM provides greater visibility to mitigate these risks!

Resource Center for FI’s

jackhenry.com/cybersavvy

- Blogs
- Whitepapers
- Webinars
- Published articles
- Cybersecurity Forums
- Webinar 5:
  - SIEM Part 2: Why Data Loss Prevention (DLP) Is Critical to Protect Your Institution



Unleashing the Power of GRC

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

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

BankBeat's Jim Murez interviews Allen Eaves from Gladiator.

How Community Banks Can Avoid Being Targets for Cyber Crooks

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

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

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

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

Cybersecurity: An Essential Competency for Credit Unions

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

Crisis Accentuates Need for Proactive Data Security

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

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

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

Web Application Cybersecurity: Not Just for Audits Anymore

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

Remote User VPN Access – How to Manage Through the Pandemic

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

Thank You!

Sebastian Fazzino, CISSP, CISM, CGEIT
sfazzino@jackhenry.com