COMMUNITY BANC
CONSULTING, INC.
cbcohio.com

SIEM - Security Information and Event Management

The New Requirement for Your Information Security Program

PRESENTED BY PAUL ELDER

COMMUNITY BANC CONSULTING

cbcohio.com

What & History

SIEM pronounced Sim. Some do say SEEM, but not as common.

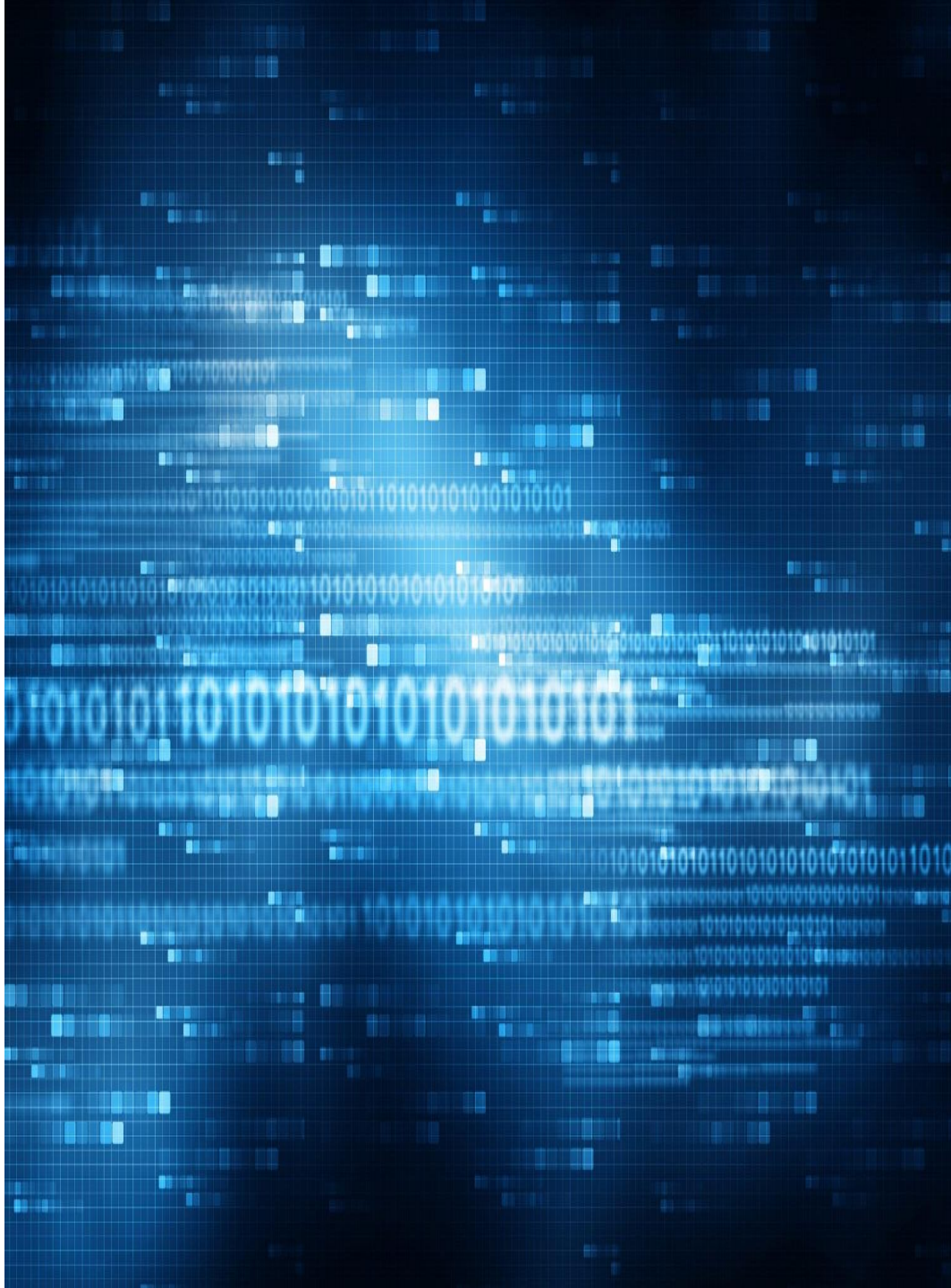
Evolved from log management.

Combination of
SEM – Security Event Management - analyzes log and event data in real time to provide threat monitoring, event correlation and incident response

SIM – Security Information Management - collects, analyzes and reports on log data

Been around about 10 years.

Available as software, appliances, virtual appliances, SaaS, on-prem, cloud, hybrid.



Why Now? Requirement?

Just in Baseline

Cyber Risk Management Oversight>Governance> Audit

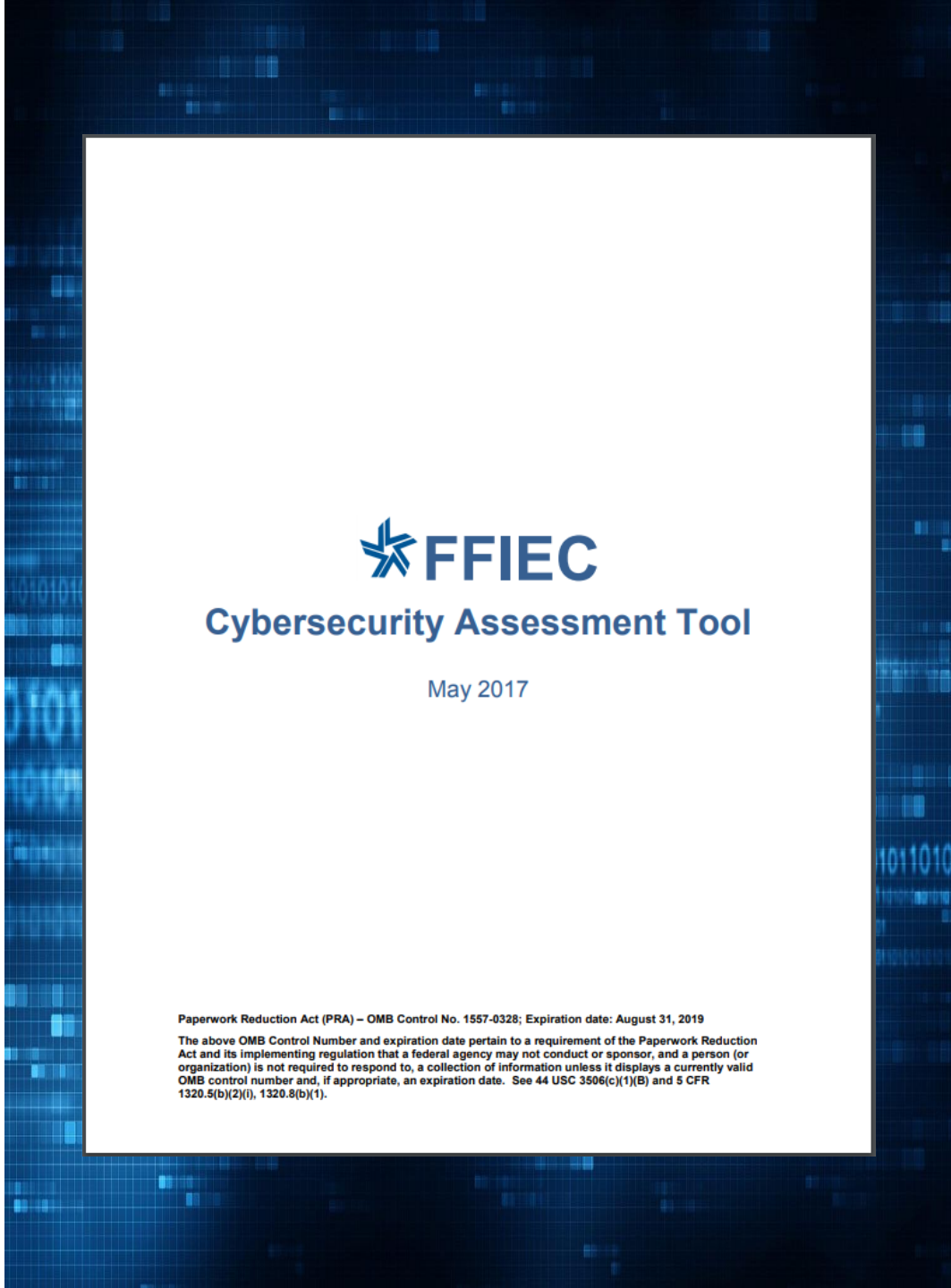
Logging practices are independently reviewed periodically to ensure appropriate **log management** (e.g., access controls, retention, and maintenance). (FFIEC Operations Booklet, page 29)

Threat Intelligence and Collaboration>Monitoring & Analyzing

Audit log records and other **security event logs** are reviewed and **retained** in a secure manner. (FFIEC Information Security Booklet, page 79)

Computer **event logs** are used for investigations once an event has occurred. (FFIEC Information Security Booklet, page 83)

Threat information is used to **monitor** threats and vulnerabilities. (FFIEC Information Security Booklet, page 83)



Why Now? Requirement? 2

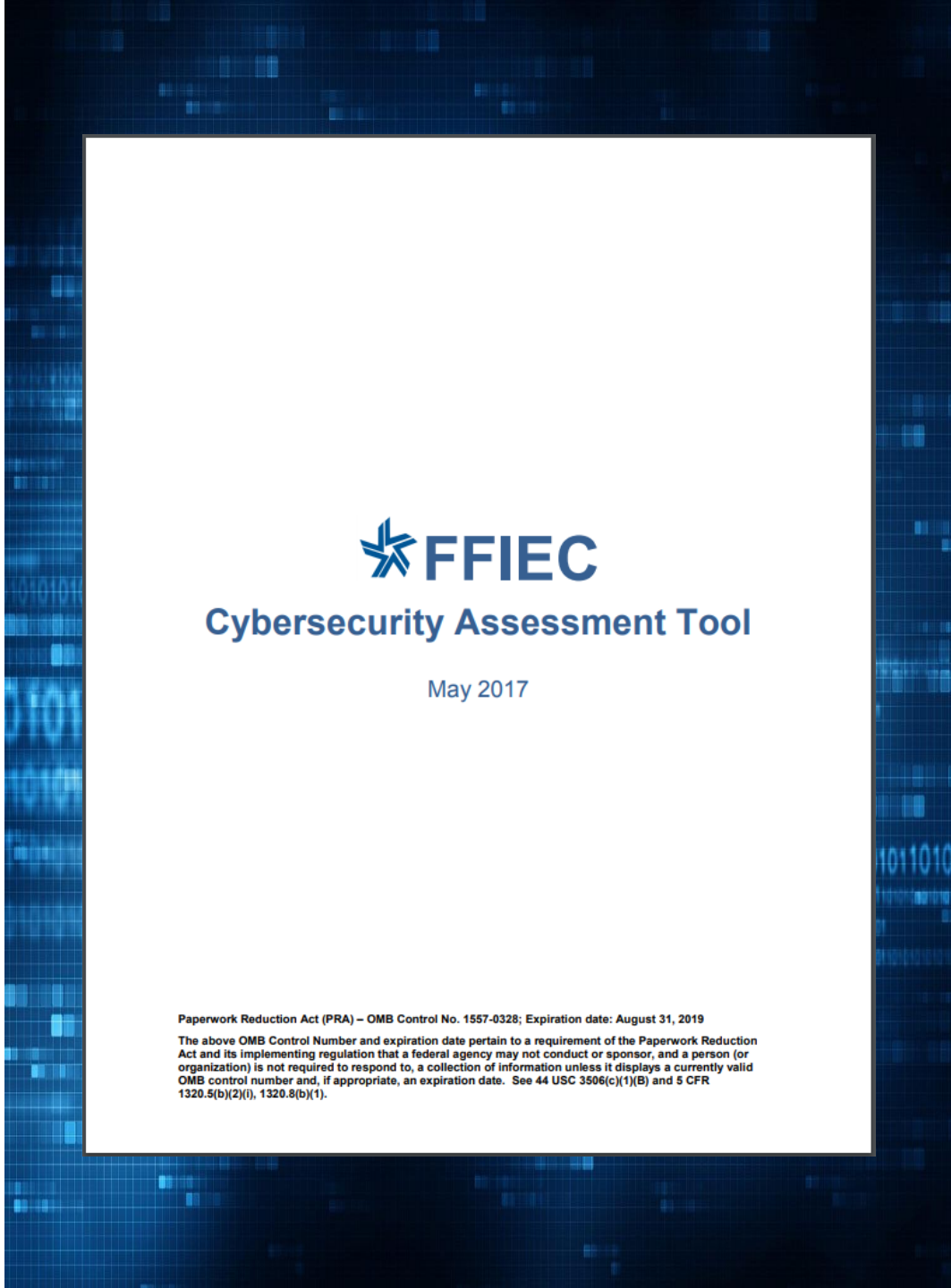
Cybersecurity Controls>Detective Controls> Anomalous Activity Detection

The institution is able to **detect** anomalous activities through **monitoring across the environment**. (FFIEC Information Security Booklet, page 32)

Logs of physical and/or logical access are reviewed following **events**. (FFIEC Information Security Booklet, page 73)

Access to critical systems by third parties is **monitored** for unauthorized or unusual activity. (FFIEC Outsourcing Booklet, page 26)

Elevated privileges are **monitored**. (FFIEC Information Security Booklet, page 19)



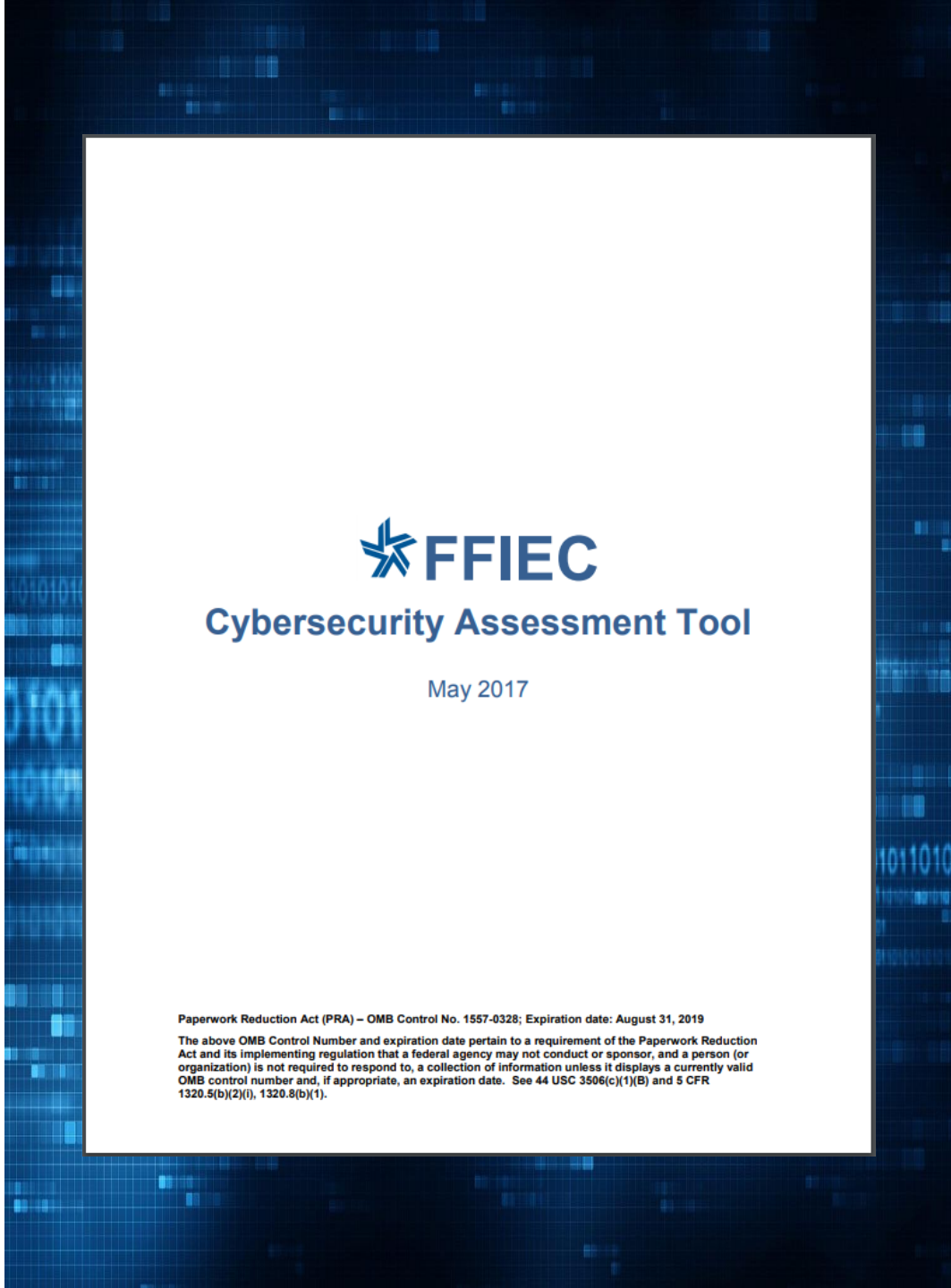
Why Now? Requirement? 3

Cybersecurity Controls>Detective Controls> Event Detection

A normal **network activity baseline** is established. (FFIEC Information Security Booklet, page 77)

Mechanisms (e.g., antivirus alerts, log event alerts) are in place to **alert** management to potential attacks. (FFIEC Information Security Booklet, page 78)

Processes are in place to **monitor** for the presence of unauthorized users, devices, connections, and software. (FFIEC Information Security Work Program, Objective II: M-9)



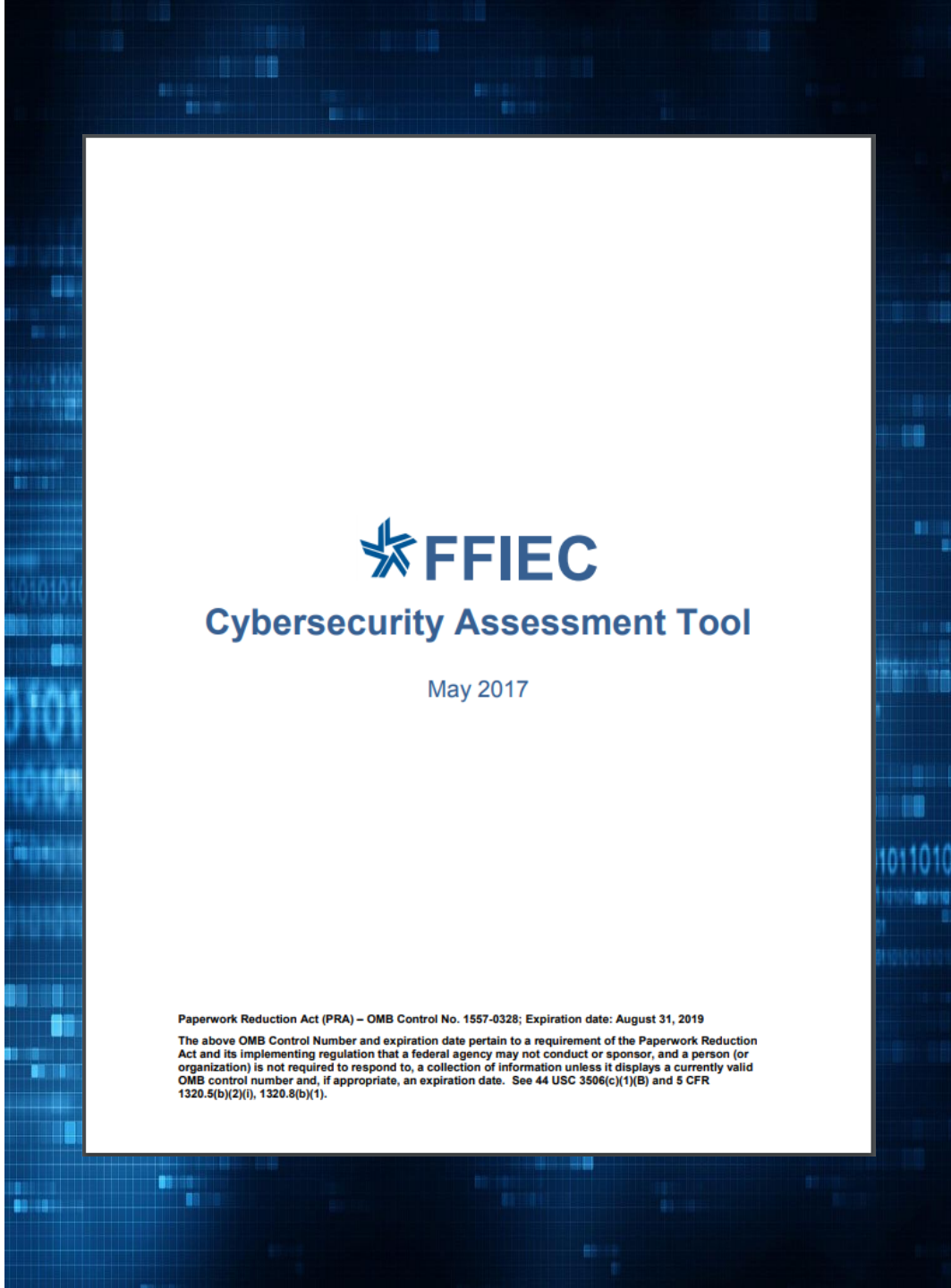
Why Now? Requirement? 4

Cyber Incident Management and Resilience>Detection, Response & Mitigation> Detection

Alert parameters are set for detecting information **security incidents** that prompt mitigating actions. (FFIEC Information Security Booklet, page 43)

System performance reports contain information that can be used as a risk indicator to **detect** information **security incidents**. (FFIEC Information Security Booklet, page 86)

Tools and processes are in place to **detect, alert**, and trigger the **incident** response program. (FFIEC Information Security Booklet, page 84)

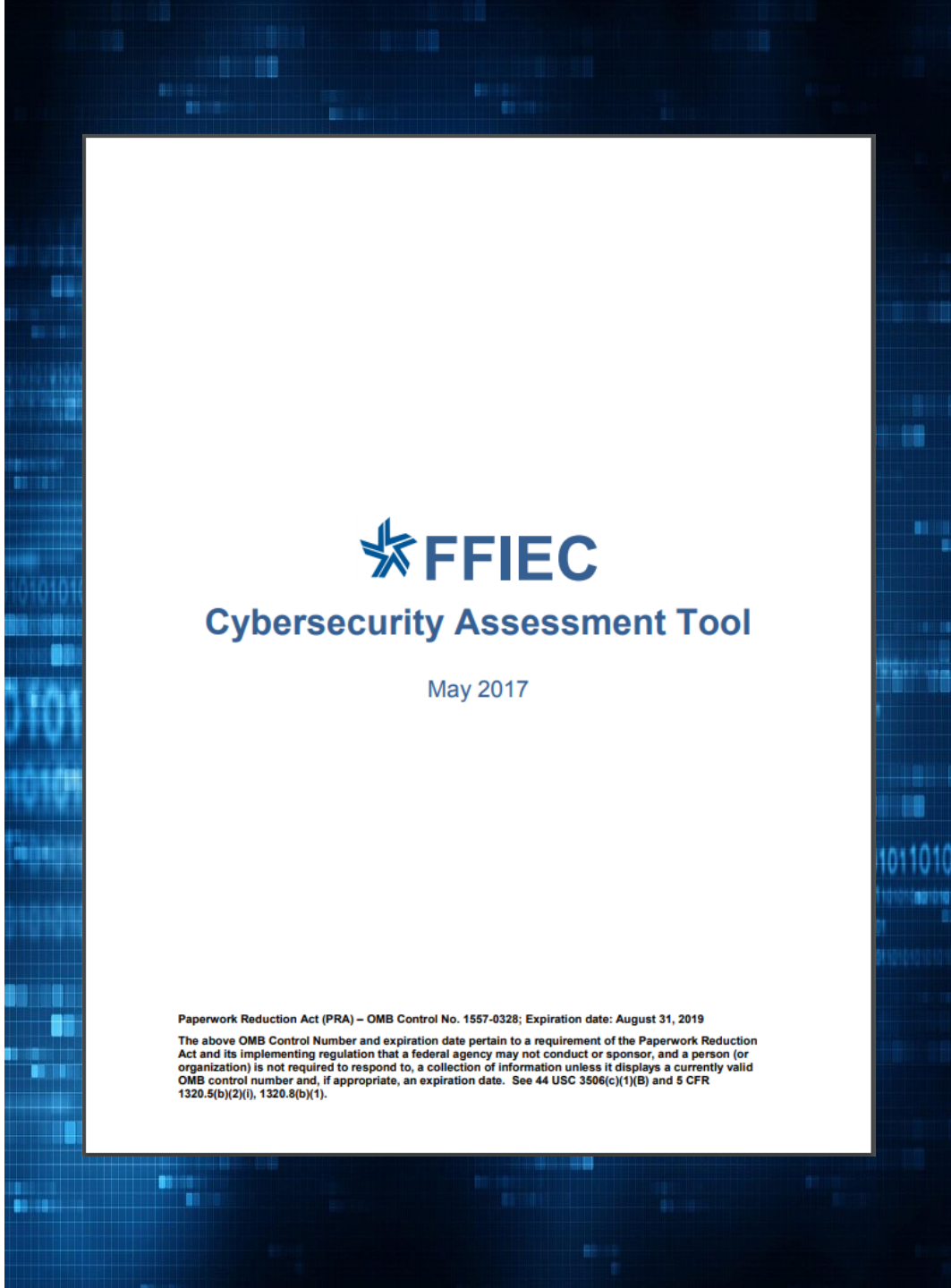


Why Now? Requirement? 5

A Peak Into Evolving

Cybersecurity Controls>Detective Controls>Detection, Response & Mitigation> Event Detection

A process is in place to **correlate event** information from multiple sources (e.g., network, application, or firewall).



Why Now? Requirement? 5

Summary

Log all events from everything, all the time.

Store and manage the logs centrally for a long time.

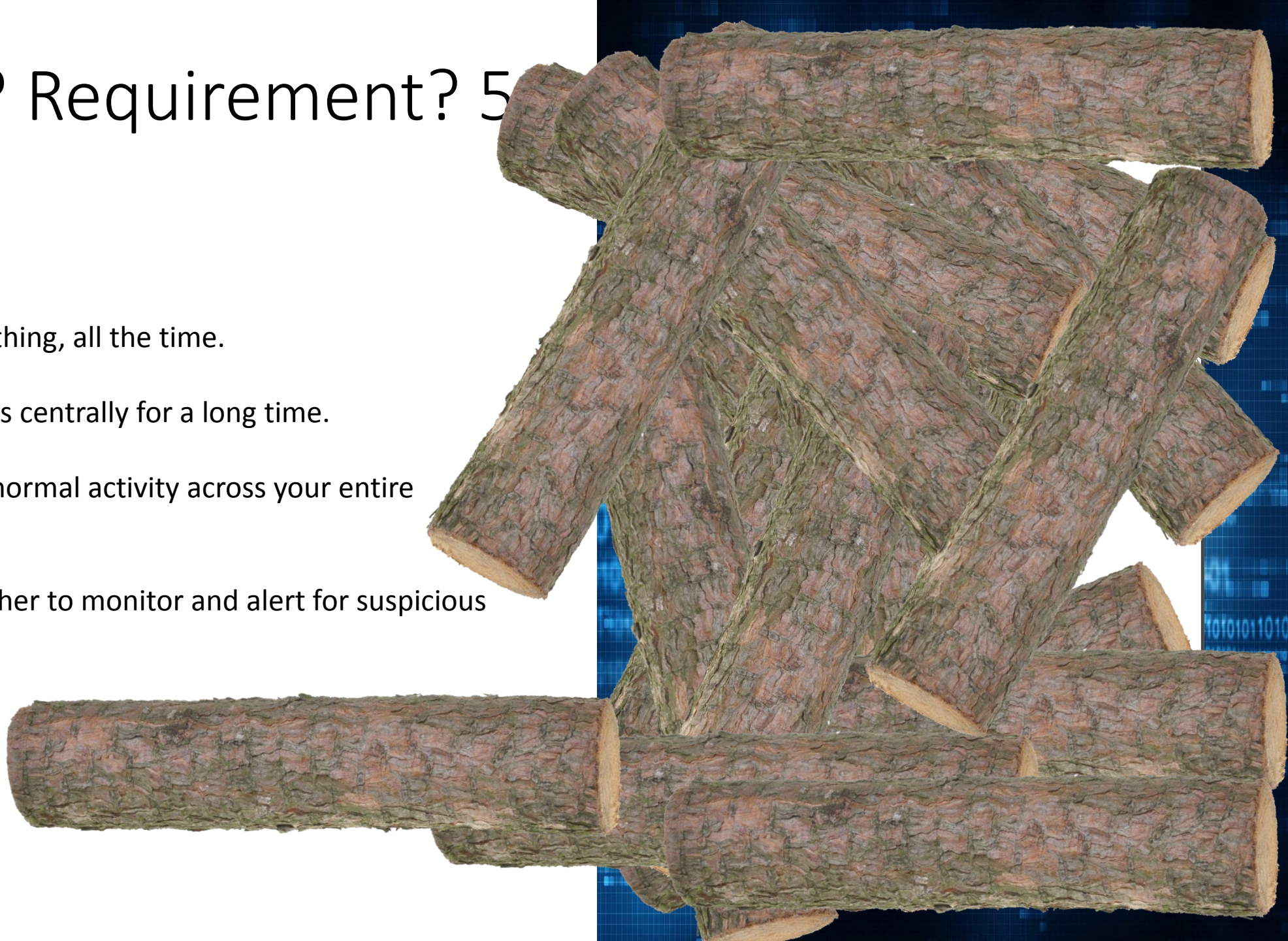
Use the logs to establish normal activity across your entire network.

Make the logs work together to monitor and alert for suspicious activity.

Rinse.

Repeat.

Perpetually.



How Many Logs?

Real Life Example

2 firewalls
19 switches
9 routers
30 servers
+ 4 VMware virtual hosts
1,000 events per second

60,000 events per minute

3,600,000 events per hour

Goals

Increase visibility

Increase security

Speed up and improve detection

Simplify response and investigation

Automate

Be more compliant

Lots to Consider

Agent vs. Agentless

Suite of capabilities – inclusive vs. modular

Existing product integration

Number of devices to monitor

Personnel resources

Deployment model

More Effective

The more devices/applications you monitor, the more logs you collect. The more logs you collect, the more visibility you have into your network.

But…

The more you more, the more you more.

And that’s Amore.

Plan Your Deployment

The deployment should be completed diligently in multiple phases.

1. Routers, switches, firewalls – network access points

2. Servers and server applications

3. Workstations and other endpoints

Plan Your Deployment cont.

The deployment should be completed diligently in multiple phases.

1. Asset inventory

2. Deploy HIDs to servers

3. Configure syslog's and apply plugins

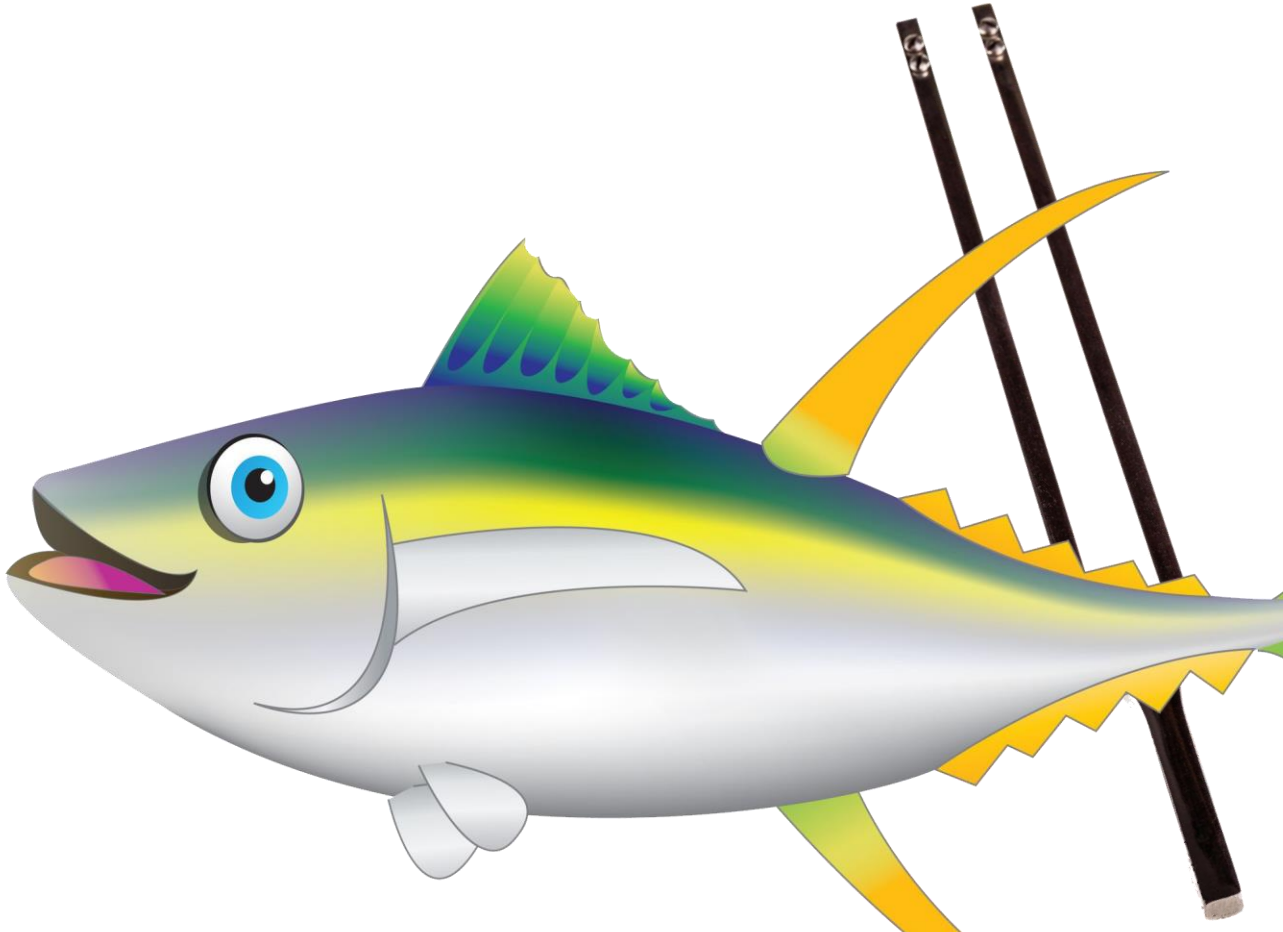
4. Vulnerability Scanning

5. Start in a read only, baselining mode with no alarms.

1. Implement
2. Observe

And then……

, Tune, Tune, Tune



After Tune, Tune, Tune, Tune

2 firewalls
19 switches
9 routers
30 servers
4 VMware virtual hosts
+ 110 Workstations

- Tuning

56 - 65 events per second

Features and Boxes You May Want to Check

1. Log and Event Management
2. Event Correlation
3. Reporting
4. Asset Discovery
5. IDS/IPS
    a. Network
    b. Host
6. File Integrity
7. Vulnerability Assessments
8. Incident Response
9. Active Directory Monitoring
10. Threat Information Feeds
11. Response/Remediation capabilities
12. Possible DLP – Data Loss Prevention

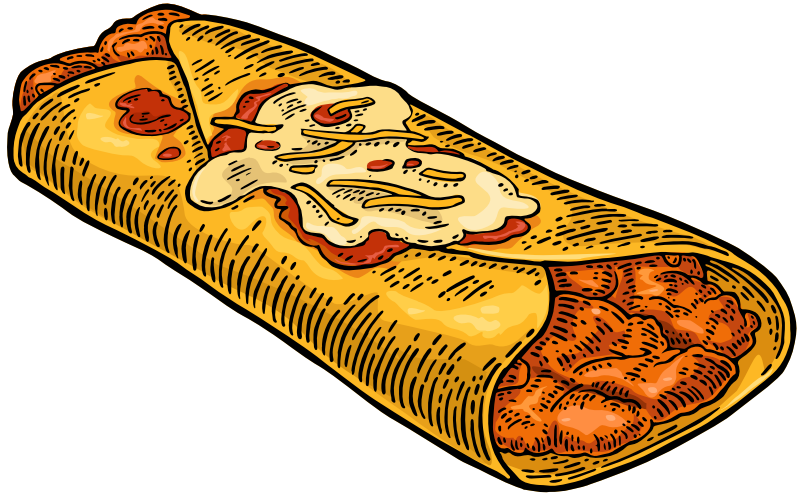
Going Forward - Developments and Features

UBA - User Behavior Analytics
Machine learning to understand how a user behaves in the system – normal/baseline
Identify and alert on deviation (risk/threat) – anomalous activity

UEBA – User and Entity Behavior Analytics
Think the same as above but with the machines, too.
More visibility.

SOAR or SOAPA
SOAR - Security Operations, Analytics and Reporting or
SOAPA - Security Operations and Analytics Platform Architecture

SIEM on the proverbial steroids with even more monitoring, UEBA, threat intelligence and response options. The whole …



Questions????

Sighs of relief?

THANK YOU

COMMUNITY BANC
CONSULTING, INC.
cbcohio.com

Full Service Information Security Program Consulting

One company for **ALL** technology related needs.

Hardware/Software Solution Implementation
Support/Maintenance/Monitoring

IT Compliance/InfoSec Program Management

Audit

Build your entire IT department with one hire.

paul@cbcohio.net
614.515.4617