Adam Gassensmith

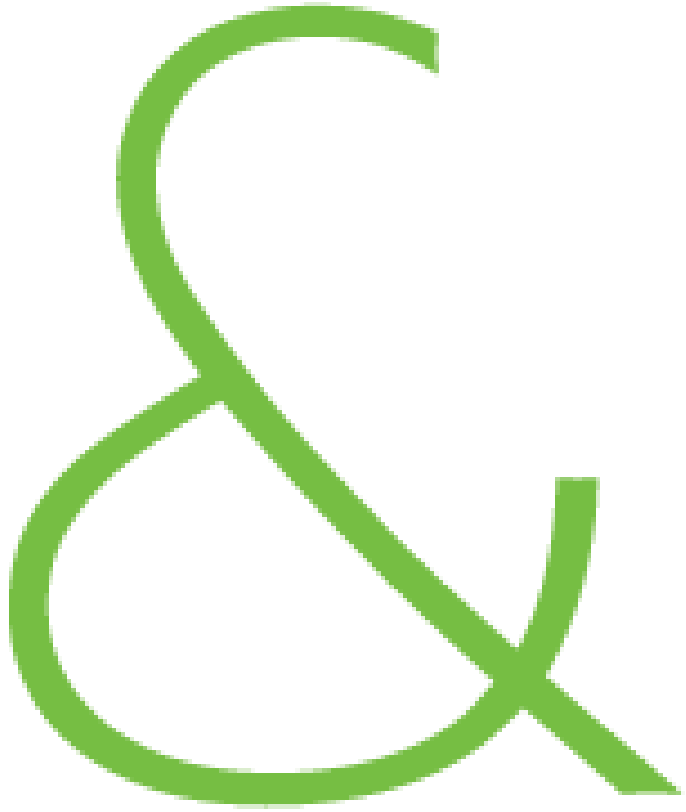
Manager of Client Engagement

peters & associates
simplify solve succeed

Catch the Bad Guys Red Handed!

Poll Question

Are you using a Security Information and Event Management (SIEM) solution today?

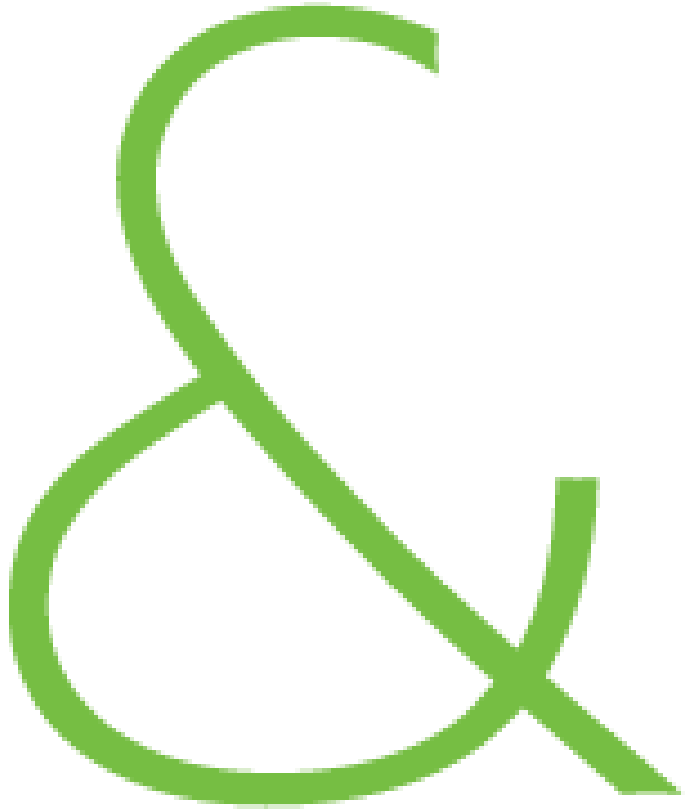


Agenda

A Framework for Cyber Security

Detecting Suspicious Activity

Simplifying Security Management

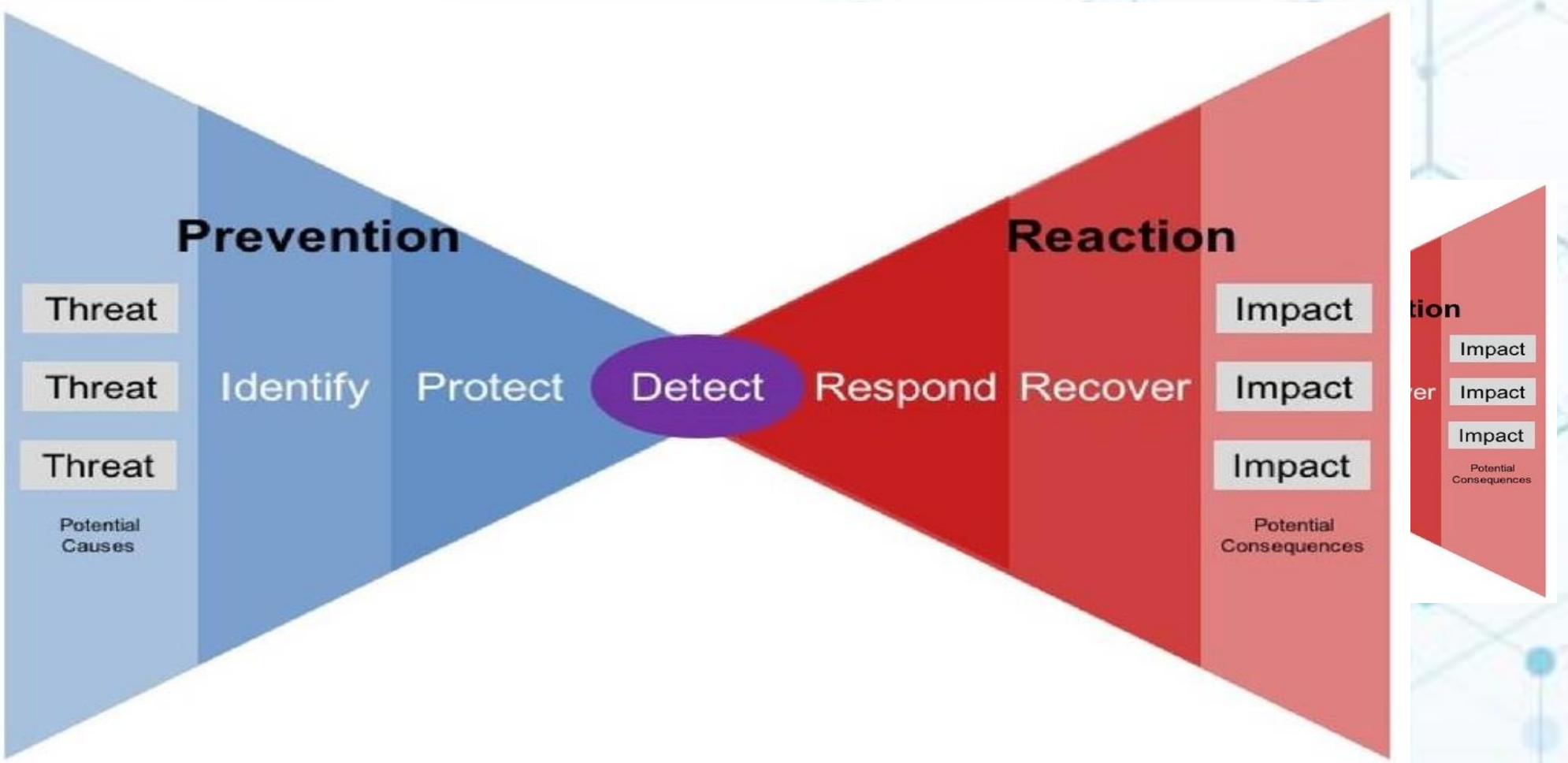


A Framework for Cyber Security

The 5
Cyber

Which
Impor

How A
Suspi



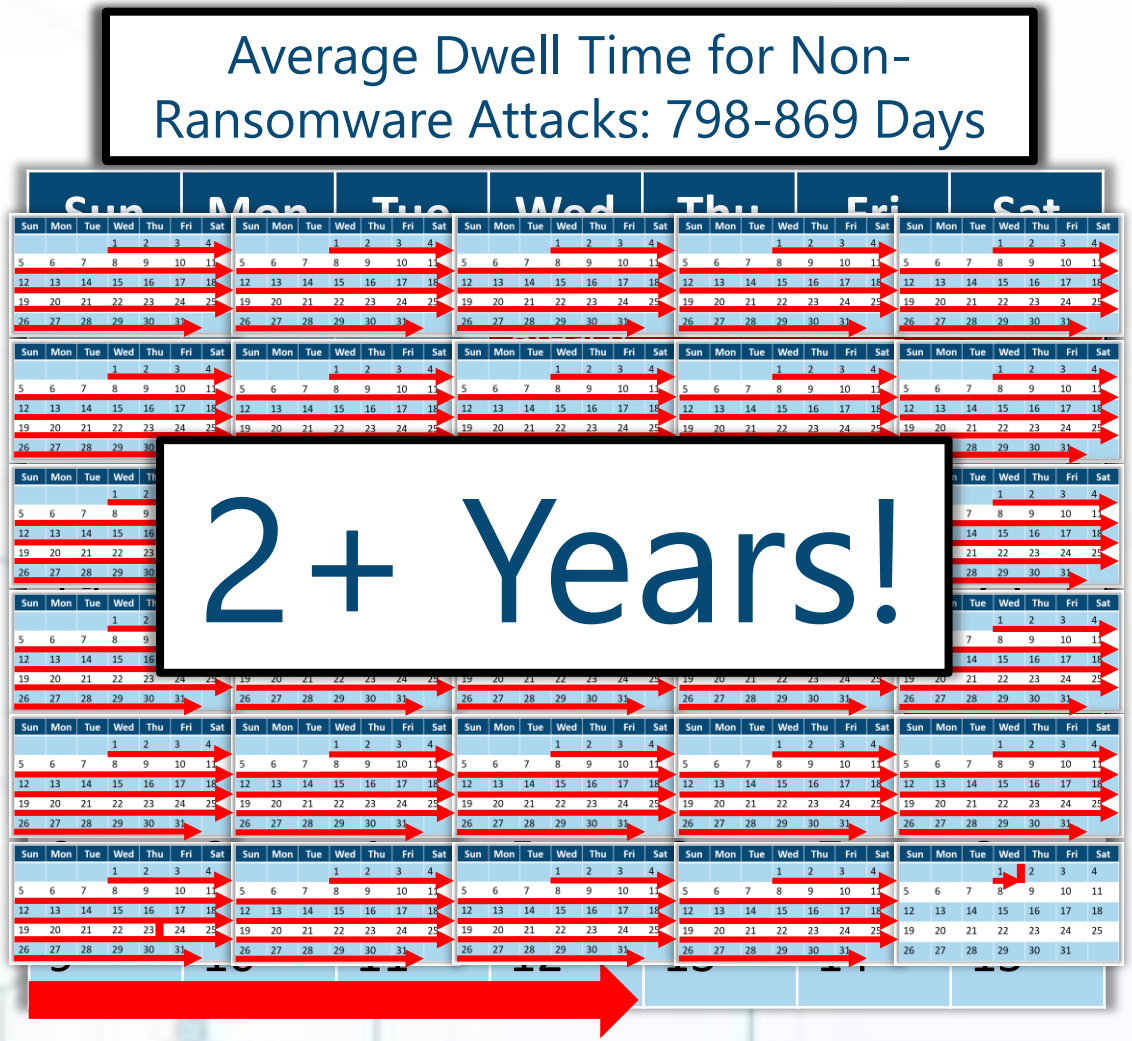
Introducing the Intrusion Kill Chain

Anatomy of a Cyber Attack

1. Exploit Compromise
2. Reconnaissance and Further Exploitation
3. Launch Attack

What is Dwell Time?

Average Dwell Time for Non-Ransomware Attacks: 798-869 Days



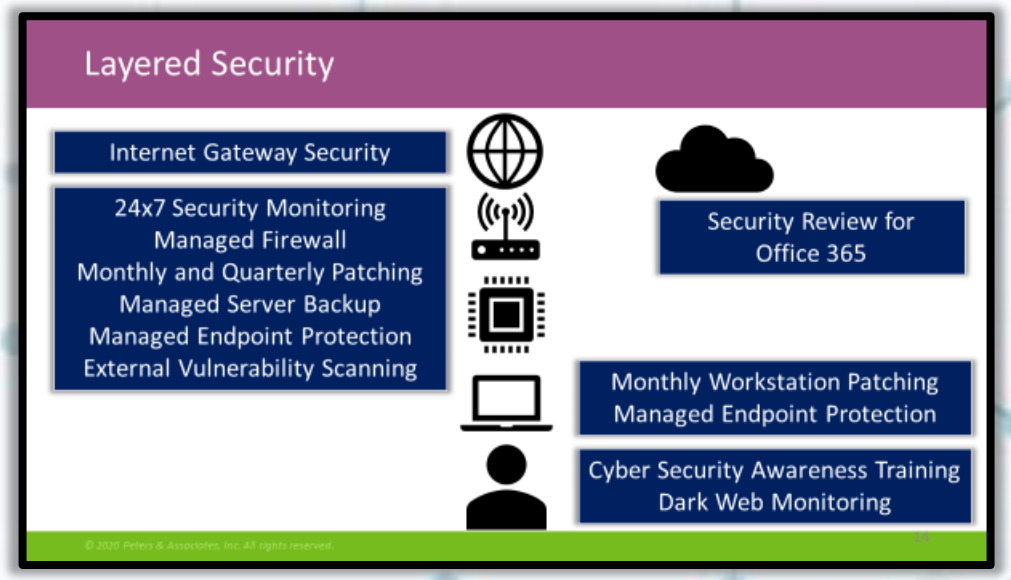
2+ Years!

Some Questions you Might be Asking&

Why didn't my traditional AV Solution stop this?!

What about this Next-Gen AV Solution?

But what about my other protection measures?

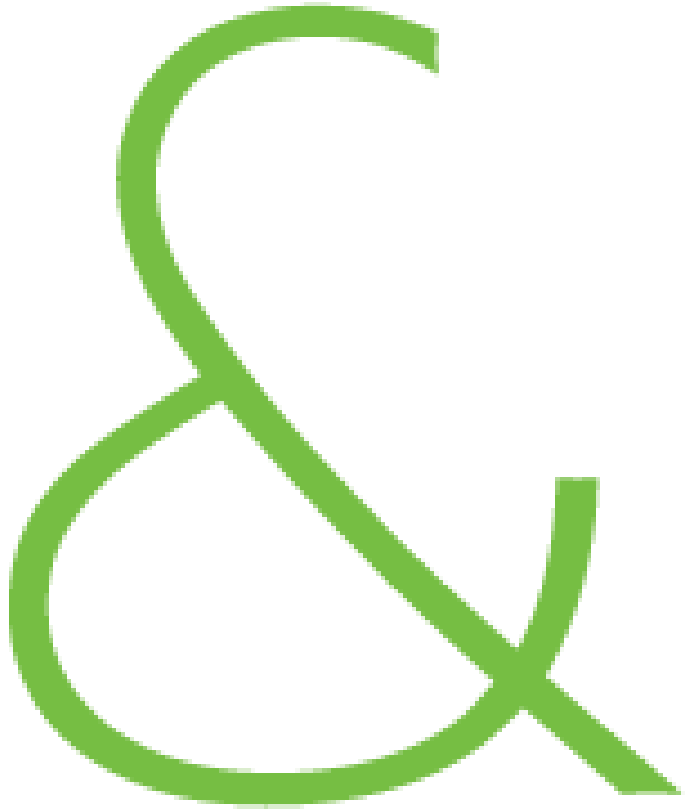


Agenda

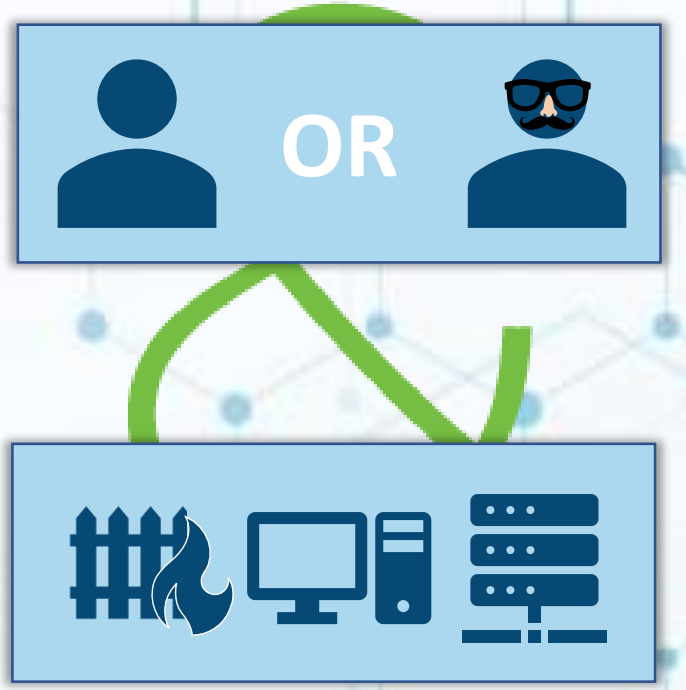
A Framework for Cyber Security

Detecting Suspicious Activity

Simplifying Security Management



Detecting Suspicious Behaviors

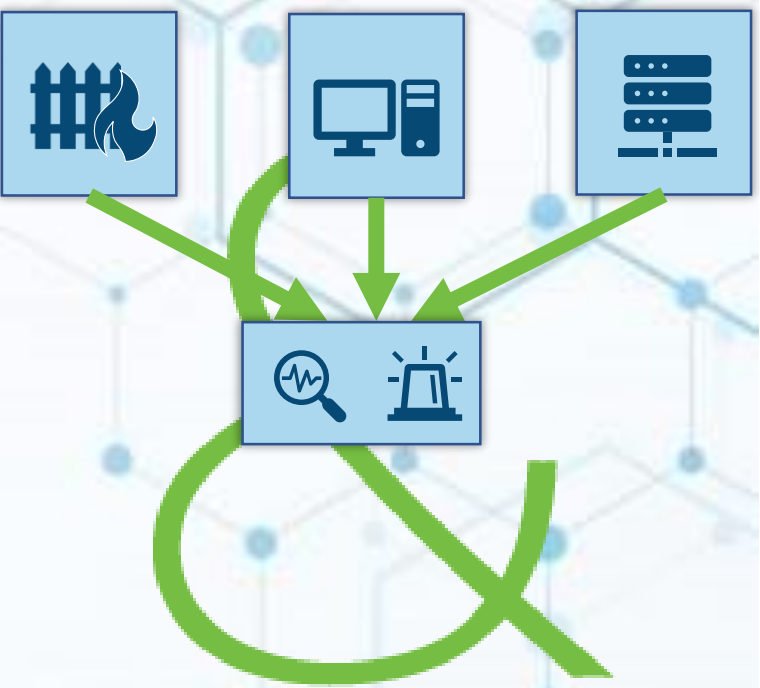


How do you sort out normal activity from authentic activity?

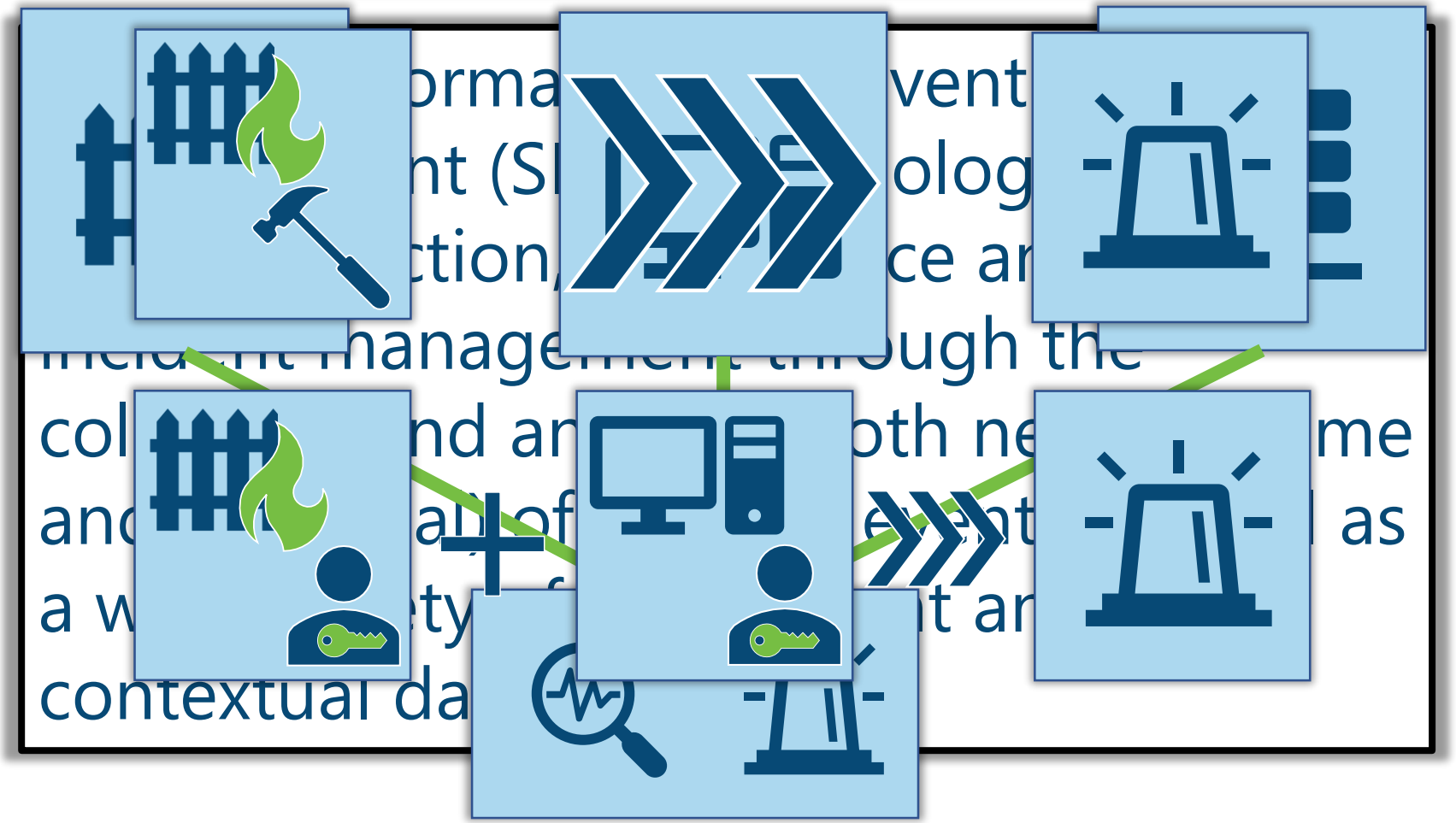
How do you collect information?

How is information correlated?

What is a SIEM?

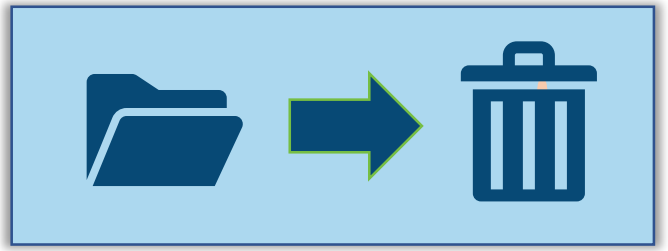


How does a SIEM work?

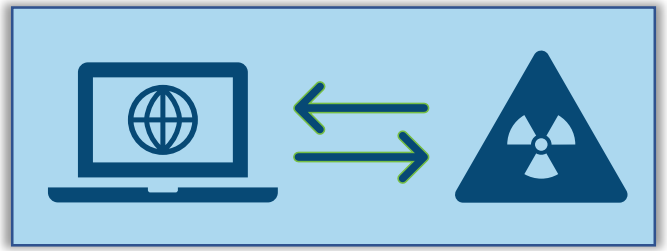


What about ransomware?

Mass File Deletion

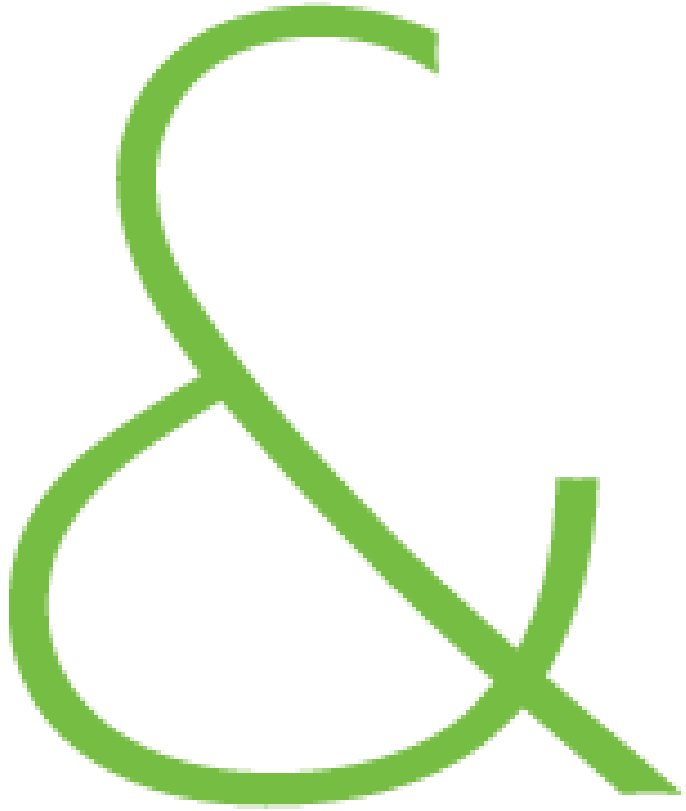


Traffic to Known Bad IPs



Poll Question

Which of the following regulatory standards does your organization adhere to?



Will a SIEM Make Me Compliant?

SIEMs help to achieve the following compliance and regulatory standards:

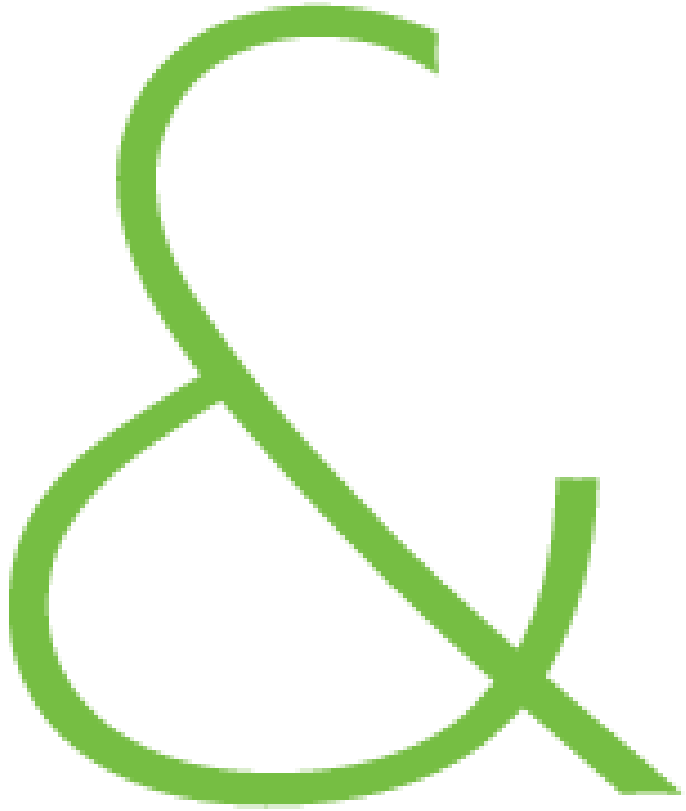
- PCI
- FERPA
- HIPAA
- FISMA
- DFARS

Agenda

A Framework for Cyber Security

Detecting Suspicious Activity

Simplifying Security Management



Simplifying Security Management

Responding to Threats

Managing the SIEM Platform

Completing the Security Picture

& Responding to Threats

PULSE Alarm

24x7 Security Monitoring, Alerting, and Response

…

Managing the SIEM Platform

PULSE Alarm

24x7 Security Monitoring, Alerting, and Response

Weekly Report Analysis for Suspicious Activity

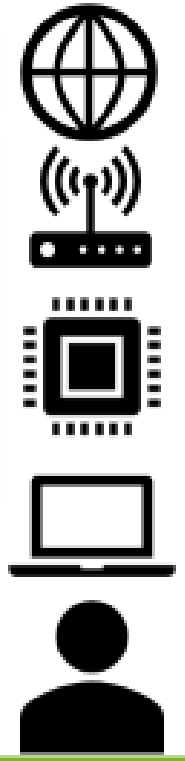
…

Completing the Security Picture

Layered Security

Internet Gateway Security

24x7 Security Monitoring
Managed Firewall
Monthly and Quarterly Patching
Managed Server Backup
Managed Endpoint Protection
External Vulnerability Scanning



Security Review for Office 365

Monthly Workstation Patching
Managed Endpoint Protection

Cyber Security Awareness Training
Dark Web Monitoring

PULSE Alarm

24x7 Security Monitoring, Alerting, and Response

Weekly Report Analysis for Suspicious Activity

Quarterly External Vulnerability Scan

What's Next?

Schedule a Free External Vulnerability Scan

Schedule a Security One-Day

Get Started with PULSE Alarm

Q&A

peters & associates

simplify solve succeed

Contact us:

Email us at:
info@peters.com

Call us at:
630.832.0075

Chat with us over coffee

peters & associates
simplify solve succeed

Thank You!

peters & associates
simplify solve succeed