Defining Security Assessment Techniques

Module Overview

Threat hunting

Vulnerability scans

Syslog/Security Information and Event Management (SIEM)

Security Orchestration, Automation and Response (SOAR)

Threat

Possible danger that can be used to exploit an existing vulnerability (via breach) with intent to cause harm to systems, networks or entire organizations

Threats can come from external or internal sources

Specific Types of Threats

- Physical Damage
- Natural Events
- Loss of Essential Services
- Compromise of Information
- Technical Failures
- Compromise of Functions

What is Cyber Threat Intelligence?

Gathering, Evaluating and Analyzing Data
Quickly gather information on what threats are being faced

Strategize Defense
Prevent the threat entirely or limit the damage caused

Understand all Details of a Threat
What tools are used, what was stolen, malware planted, methods of communication, etc.

Importance of Cyber Threat Intelligence

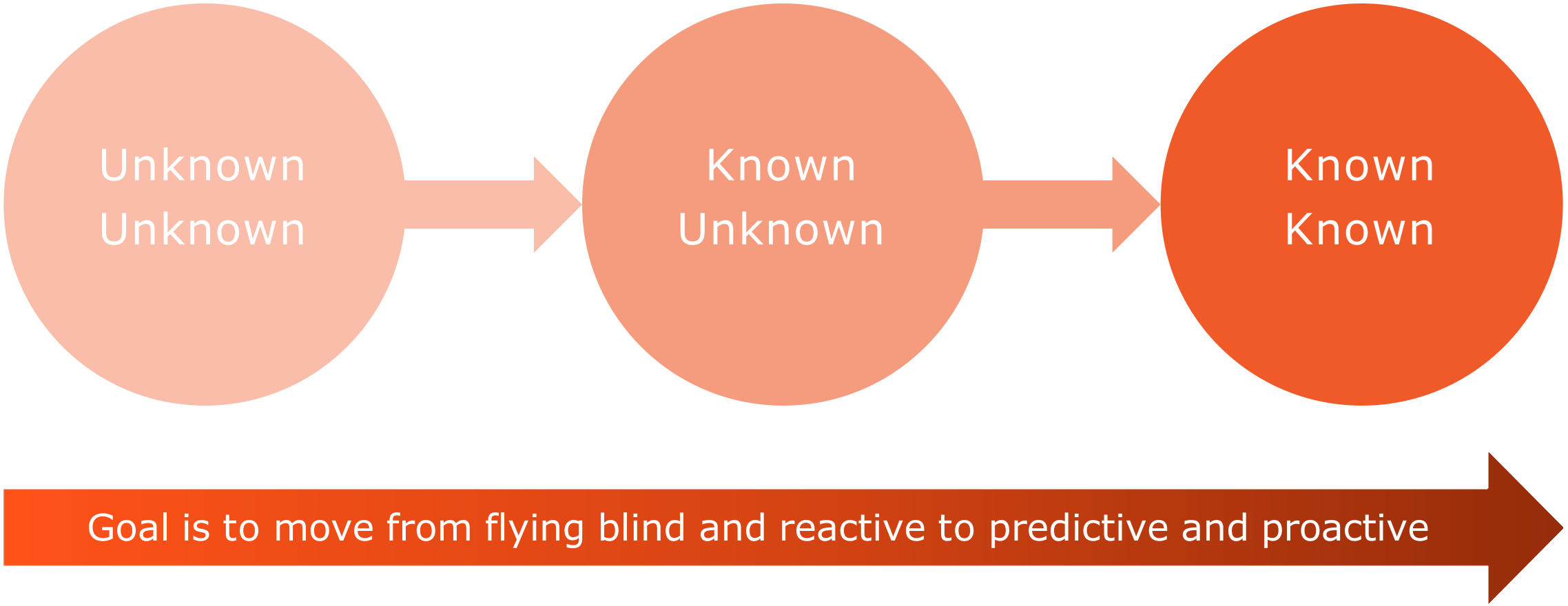
Protect Against Disruption to the Business

Continue to Do Business / Make Money

Retain Customer and Shareholder Confidence

Increase Profitability / Partner Value

Threat Intelligence Classifications



Strategic, Operational and Tactical Intelligence

Source: Cyber Threat Intelligence Responsibilities and Interrelationships (INSA, 2013)

Gathering and Correlating Information

Data in a vacuum, without context, is extremely difficult to interpret and understand exactly what data is valuable and what is noise

Forensics

Alerts

Logs

Feeds

Configs

Dark Web

TI Analyst

Gathering and Correlating Information

Data in a vacuum, without context, is extremely difficult to interpret and understand exactly what data is valuable and what is noise

Categorize TTPs and Enrich Alerts to track, target and deter/prevent attacks

Stages of Risk Management

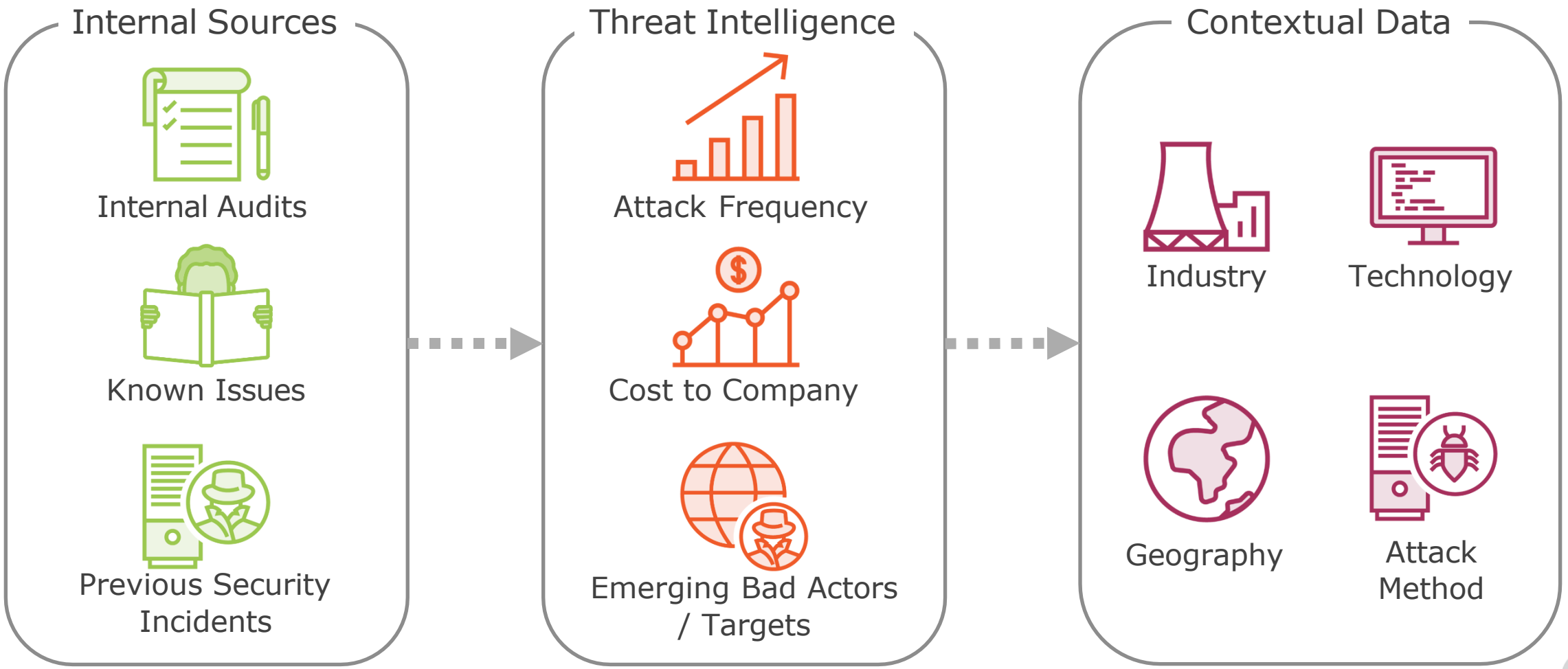
Assessing Requirements
Understanding the business and IT objectives and how security can meet those objectives

Aligning with Current Capabilities
Understand what's available today and what capabilities exist across people, process and technology

Creating Plans and Initiatives
Quantify existing gaps and develop plans to prioritize initiatives and fill the gaps

Creating Metrics and Monitoring Progress
Develop metrics to track progress and ensure programs are meeting business requirements

Risk Management Data Sources



Vulnerability Scanning

Vulnerability scanning is different from penetration testing

- Should be performed in tandem with pen testing
- Non-intrusive and can be performed with credentials or without credentials depending on risk tolerance

Always obtain consent prior to beginning any type of vulnerability scan or pen test

- Make sure that you're operating with the proper permissions
- Document the process and keep authorization forms readily available

False Positive

No system is perfect and can occasionally generate false positives

- Identify a vulnerability that doesn't actually exist
- Results must be verified and audited for completeness and accuracy

False Positives

Controls should be routinely audited and reviewed

- False positives are events that aren't really incidents
- Anomalies that deviate from normal behavior
  - Review to ensure policies are set up properly
  - False positives can create excess work or minimize attention when real incidents occur

False Negatives

False negatives are the opposite of false positives

- You had an incident but failed to recognize it
  - Controls set up improperly
  - Operator error

Type I, II, III Errors

- Type I – False positives
- Type II – False negatives
- Type III – You arrive at the right conclusion for the wrong reasons

Intrusive vs. Non-Intrusive

Intrusive testing can disrupt normal operations or have a greater impact of reducing system responsiveness

Non-intrusive simply identifies vulnerabilities and reports findings for later review and possible remediation

Passively Test Security Controls

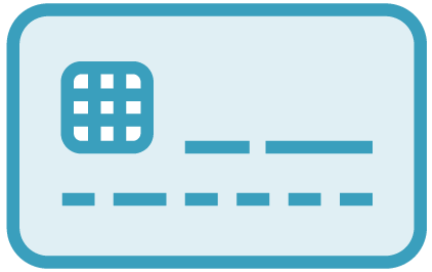
Vulnerability scanning is by nature a passive test

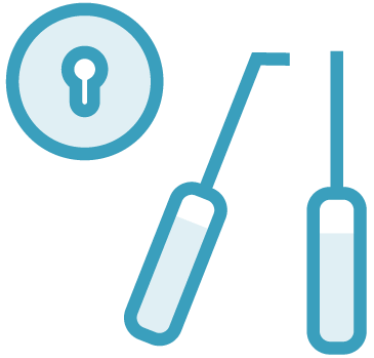
- No disruption to the business
- Observes and reports on findings
- Does not take down systems, applications or services

Credentialed vs. Non-Credentialed

Scans and tests can be run with network/system credentials or without

- Credentialed access has easier access and less impact on tested systems as well as more accurate results
- Non-credentialed access requires more resources as a system may try to brute-force access or try multiple things to gain access





Credentialed vs. Non-Credentialed

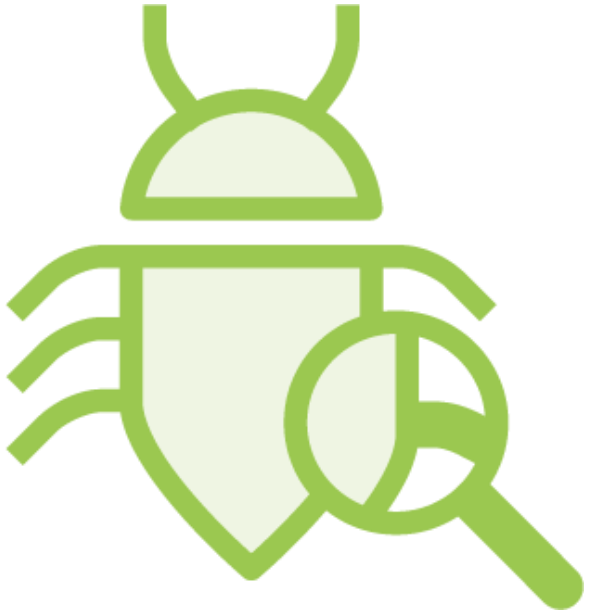
Attackers typically start out with non-credentialed access

- They normally don't know much about the networks they're attacking

Attackers try to gain privileged account access

- Gain administrator or root access
- Providing much more detail about the network and associated systems

Identify Vulnerability



Scanners will report on the various vulnerabilities found

- Missing patches
- Security misconfigurations
- Known exploits

Identify Lack of Security Controls

- Often times it’s more than just the security control is misconfigured or missing a patch
  - The security control itself might be missing
  - Anti-virus programs
  - Missing patches
- Review logs
- Interview personnel

Identify Common Misconfigurations

Nessus, Metasploit and other similar programs can identify security misconfigurations

Review logs and perform audits of key assets

- Open ports
- Weak passwords
- Active default accounts and passwords
- Sensitive data leakage
- Audit against security baseline to identify unauthorized changes

Things to Remember

Obtain Consent

- Very important to have consent in writing
- Vulnerability scanning or pen testing without consent can be considered an attack and grounds for dismissal

Review company guidelines and "rules of engagement"

Identify and assess tester's skills and background

- Verify and obtain references when possible
- Tester could potentially have access to sensitive corporate data

CVE / CVSS

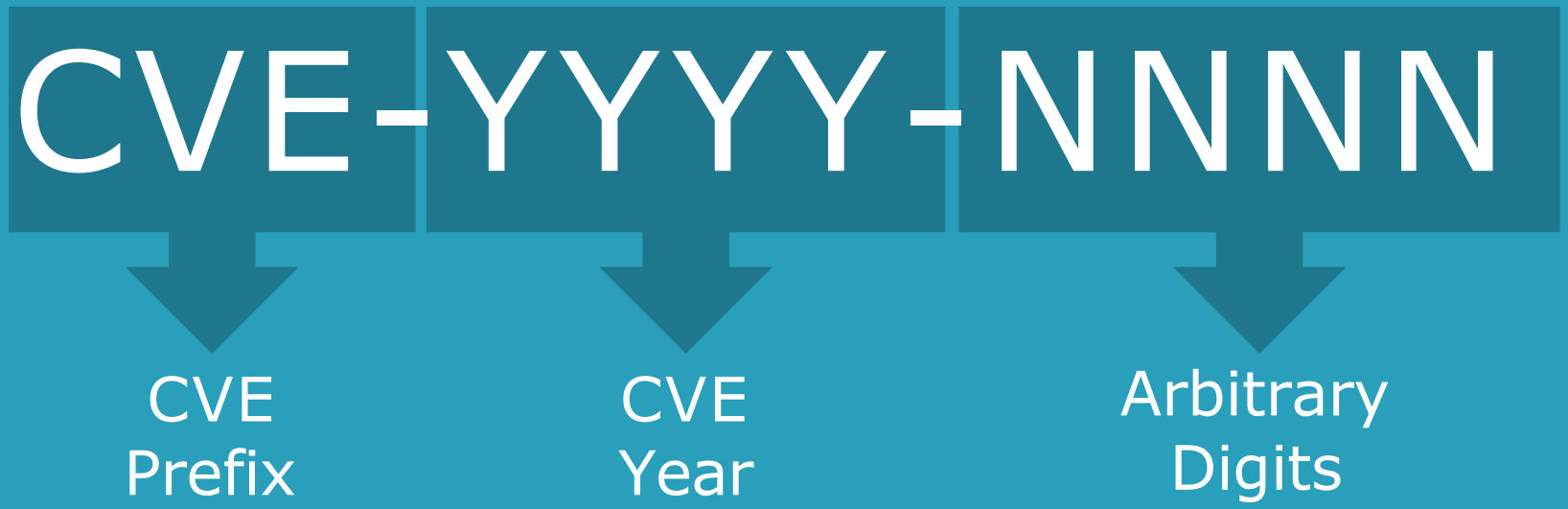
Common Vulnerabilities and Exposures (CVE)

- Reference for publicly known information security vulnerabilities
- Maintained by the Mitre Corporation

Common Vulnerability Scoring System (CVSS)

- Open framework for communicating the characteristics and severity of software vulnerabilities

CVE-YYYY-NNNN


CVE-YYYY-NNNN
CVE
Prefix
CVE
Year
Arbitrary
Digits

Search Results

There are **0** CVE entries that match your search.

Name	Description

BACK TO TOP

SEARCH CVE USING KEYWORDS: windows Submit

You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

Search Results

There are **8318** CVE entries that match your search.

Name	Description
CVE-2020-9858	A dynamic library loading issue was addressed with improved path searching. This issue is fixed in Windows Migration Assistant 2.2.0.0 (v. 1A11). Running the installer in an untrusted directory may result in arbitrary code execution.
CVE-2020-9850	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A remote attacker may be able to cause arbitrary code execution.
CVE-2020-9843	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to a cross site scripting attack.
CVE-2020-9807	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-9806	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-9805	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to universal cross site scripting.

Printer-Friendly View

CVE-ID	
CVE-2020-9326	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

BeyondTrust Privilege Management for Windows and Mac (aka PMWM; formerly Avecto Defendpoint) 5.1 through 5.5 before 5.5 SR1 mishandles command-line arguments with PowerShell .ps1 file extensions present, leading to a DefendpointService.exe crash.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://www.beyondtrust.com/support/changelog/privilege-management-for-windows-5-5-sr1

Assigning CNA

MITRE Corporation

Date Entry Created

20200220	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20200220)

CVE Formatting

CVE-2020-9326 Detail

Current Description

BeyondTrust Privilege Management for Windows and Mac (aka PMWM; formerly Avecto Defendpoint) 5.1 through 5.5 before 5.5 SR1 mishandles command-line arguments with PowerShell .ps1 file extensions present, leading to a DefendpointService.exe crash.

+View Analysis Description

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

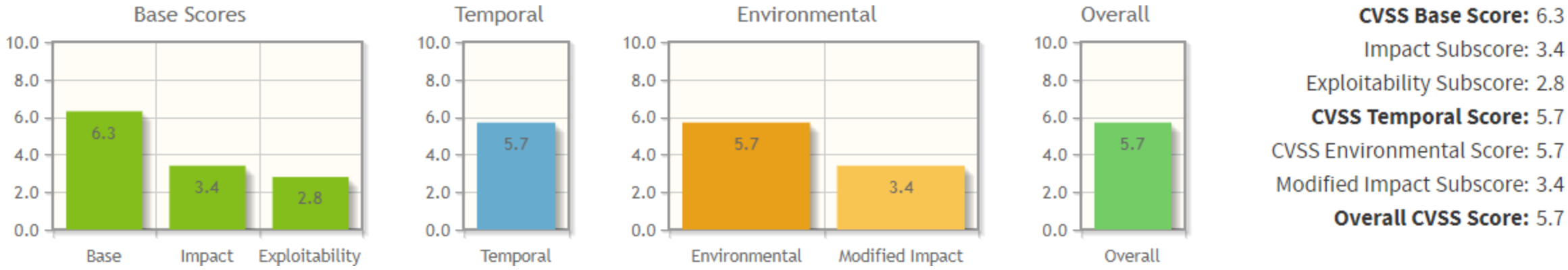
Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Source: https://nvd.nist.gov/vuln/detail/CVE-2020-9326

CVSS

CVSS is maintained by Forum of Incident Response and Security Teams (FIRST) and is used to assess the principal characteristics of a vulnerability and produce a numerical score reflecting its severity (scale of 1-10).

The numerical score can then be translated into low, medium, high to help organizations properly assess vulnerabilities and prioritize resources to manage and mitigate.



Source: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

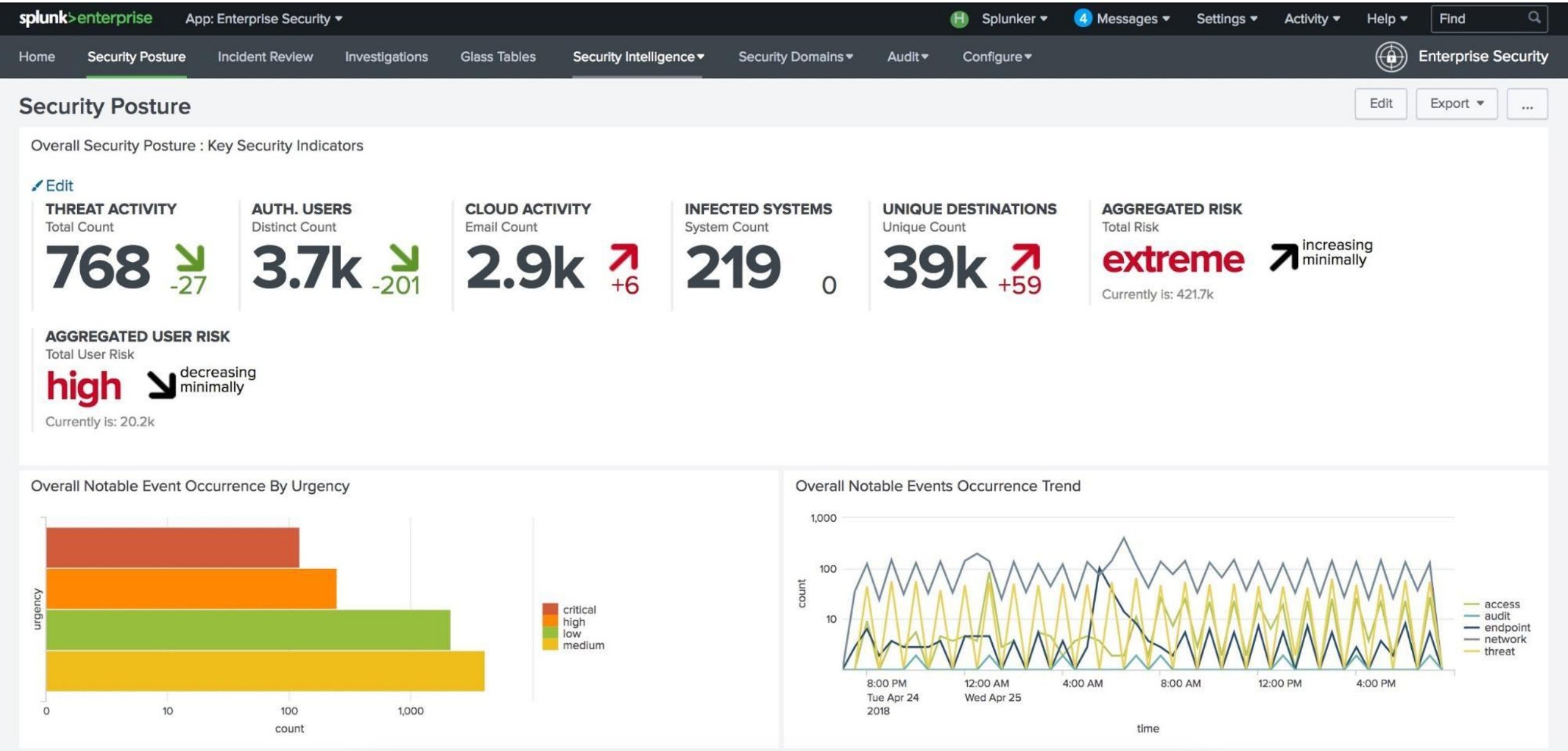
Security Information and Event Management (SIEM)

SIEM are software suites that provide the following:

- Collects data
- Aggregates the data
- Analyzes normalized data for anomalies, threats and trends
- Investigates alerts, identifies breaches and takes action
- Remediates discovered vulnerabilities
- Reports on risk and compliance

Source: Gartner (February 2020)

SIEM Dashboard

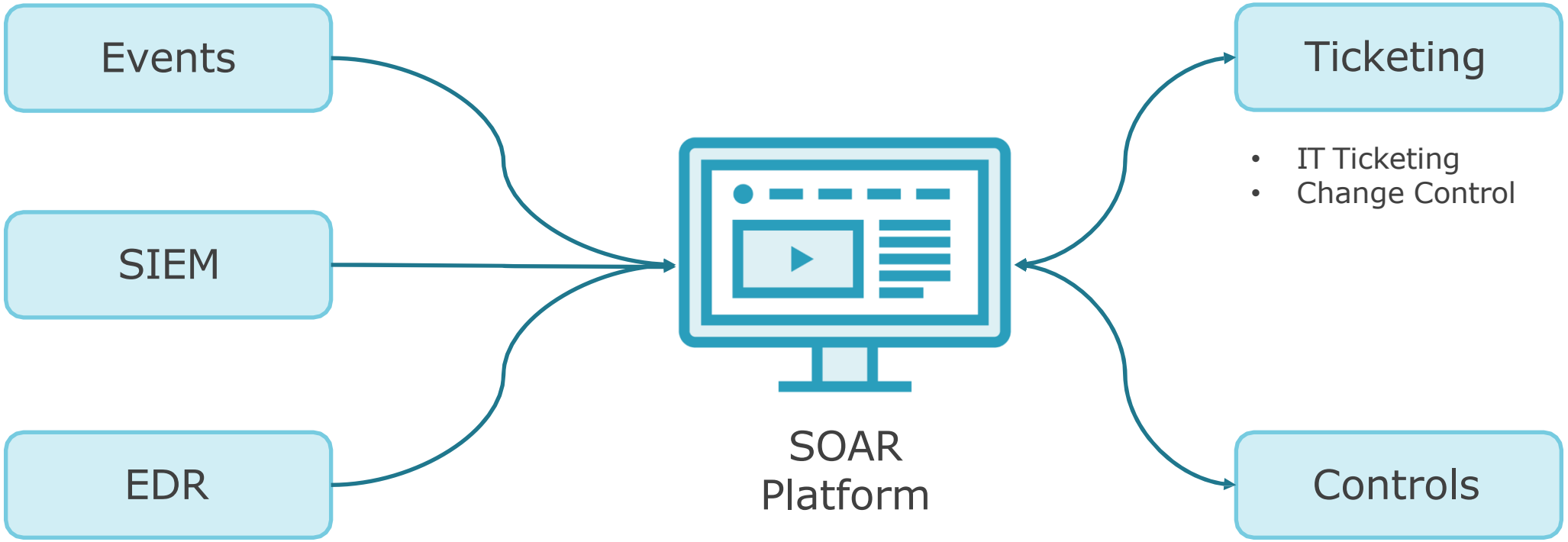


SOAR

Security Orchestration, Automation and Response

- Complements SIEM
- Aggregates all tools within a SOC and provides automated playbooks
  - Ticket creation, case management, etc.
  - Integrations with 3rd party products

SOAR



EDR = Endpoint Detection and Response

Module Review

Threat hunting

Vulnerability scans

Syslog/Security Information and Event Management (SIEM)

Security Orchestration, Automation and Response (SOAR)