ASMGi ONEteam

ARCTIC WOLF

Managing Cyber Risk

Don't be careless about your exposure to cyber-attacks!

March 25, 2021

Managing Cyber Risk – Don’t be careless about your exposure to cyber-attacks!

Dmitriy Sandler
Director of Presales Engineering
Arctic Wolf

Steve Roesing
President, CEO
ASMGi

ARCTIC WOLF

ASMGi
ONEteam

Upcoming ASMGi Cyber Security Webinar with Arctic Wolf

Don't Let Your Cloud Security Fall Behind

presented by ASMGi and Arctic Wolf Networks
live webinar, ***April 8 at 1PM ET***

*Reply "**YES**" in the Question Box and we will preregister you for this webinar*

Agenda

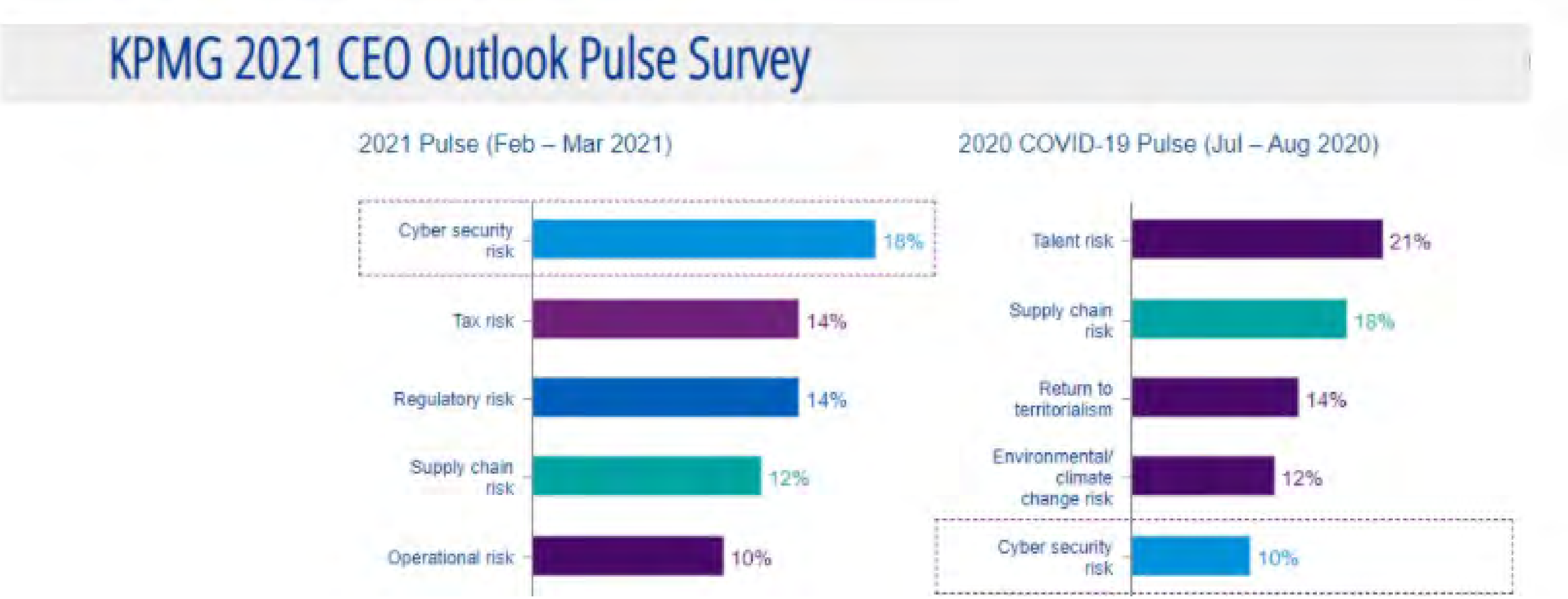
- *Why is Cyber Risk so Important?*
- *How do we Lower Cyber Risk?*
- *Key Benefits*
- *Q & A*

CYBER SECURITY SOLUTIONS

Why is Managing Cyber Risk so Important?

Why is Managing Cyber Risk so Important?

KPMG: Cyber Security Risk Is Now No. 1 Threat To Growth



KPMG 2021 CEO Outlook Pulse Survey

Why is Managing Cyber Risk so Important?

ASMGi ONEteam

ARCTIC WOLF

We're all moving workloads to the Cloud – misconfigurations should be a huge concern! Is anyone checking your Cloud configurations?

2017

Equifax Announces Cybersecurity Incident Involving Consumer Information

Flaw was known by vulnerability management tools, but the patch was never installed.

2019

Hackers Gain Access to 100 Million Capital One Credit Card Applications and Accounts

Misconfiguration in cloud service went unnoticed despite availability of monitoring products.

June 2020

Control Systems Targeted Shutting Down Production In Honda Breach

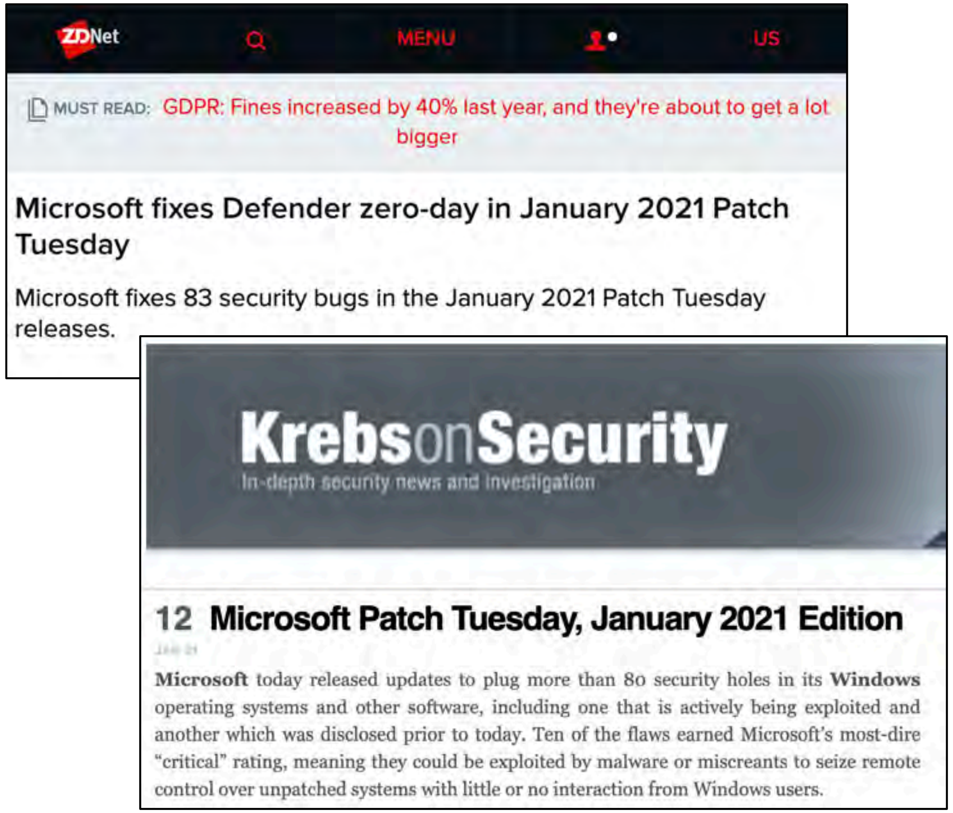
Attack focused on control systems, in the production line

Knowing about vulnerabilities does not lower your risk. Remediating them does!

All connected devices are targets! Make sure you are identifying all your connected devices and their vulnerabilities!

Microsoft Patch Tuesday, January 2021

High-profile vulnerabilities always lead to the same questions



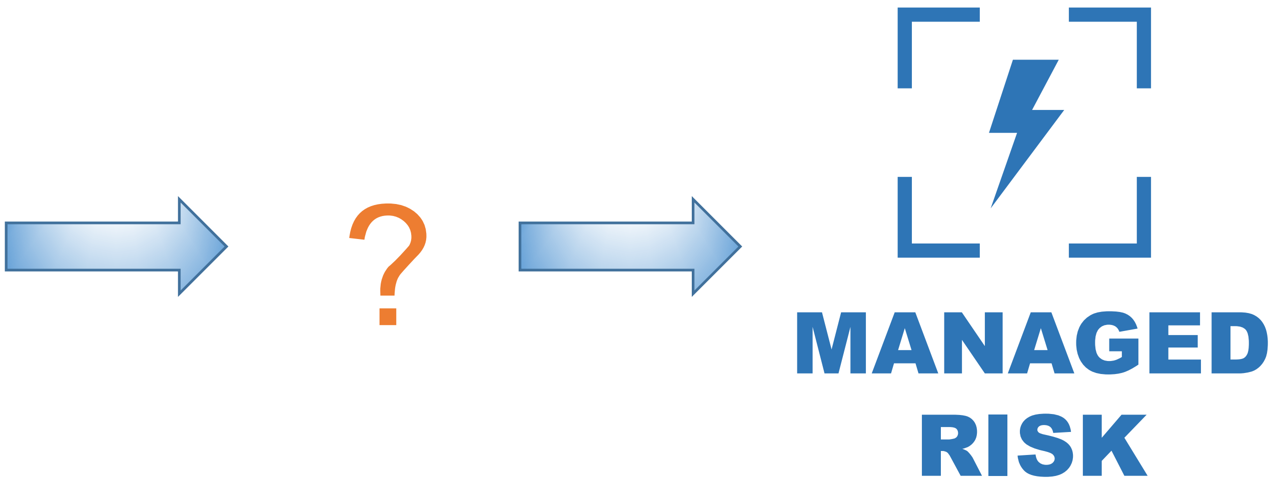
MUST READ: GDPR: Fines increased by 40% last year, and they're about to get a lot bigger

Microsoft fixes Defender zero-day in January 2021 Patch Tuesday

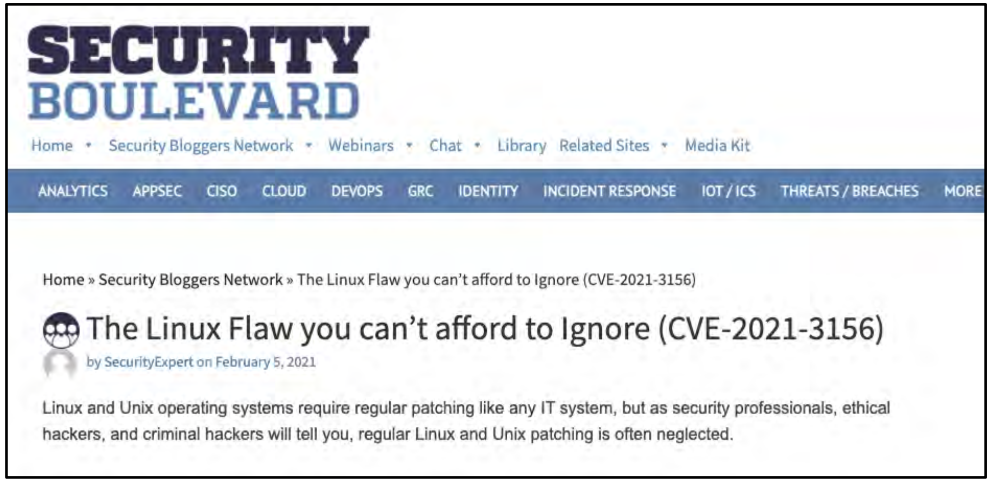
Microsoft fixes 83 security bugs in the January 2021 Patch Tuesday releases.

12 Microsoft Patch Tuesday, January 2021 Edition

Microsoft today released updates to plug more than 80 security holes in its **Windows** operating systems and other software, including one that is actively being exploited and another which was disclosed prior to today. Ten of the flaws earned Microsoft's most-dire "critical" rating, meaning they could be exploited by malware or miscreants to seize remote control over unpatched systems with little or no interaction from Windows users.



Another flaw you can't ignore...


SECURITY BOULEVARD
Home • Security Bloggers Network • Webinars • Chat • Library Related Sites • Media Kit
ANALYTICS APPSEC CISO CLOUD DEVOPS GRC IDENTITY INCIDENT RESPONSE IOT / ICS THREATS / BREACHES MORE

Home » Security Bloggers Network » The Linux Flaw you can't afford to Ignore (CVE-2021-3156)

The Linux Flaw you can't afford to Ignore (CVE-2021-3156)

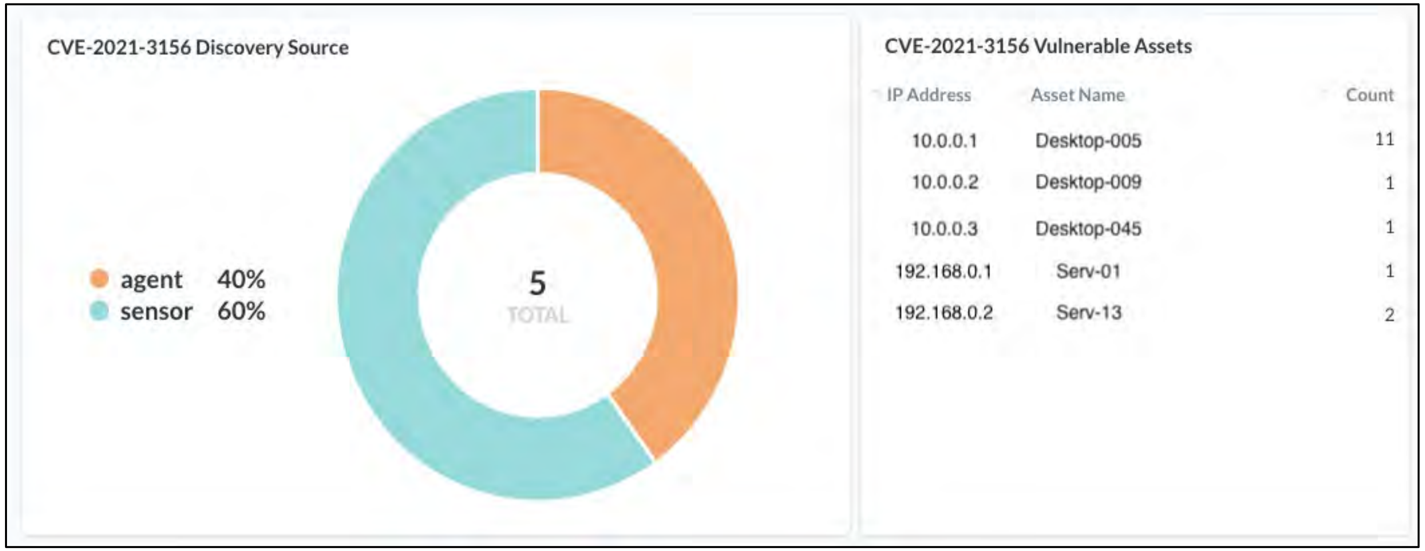
by SecurityExpert on February 5, 2021

Linux and Unix operating systems require regular patching like any IT system, but as security professionals, ethical hackers, and criminal hackers will tell you, regular Linux and Unix patching is often neglected.

MANAGED RISK

High-profile vulnerabilities always lead to the same question:

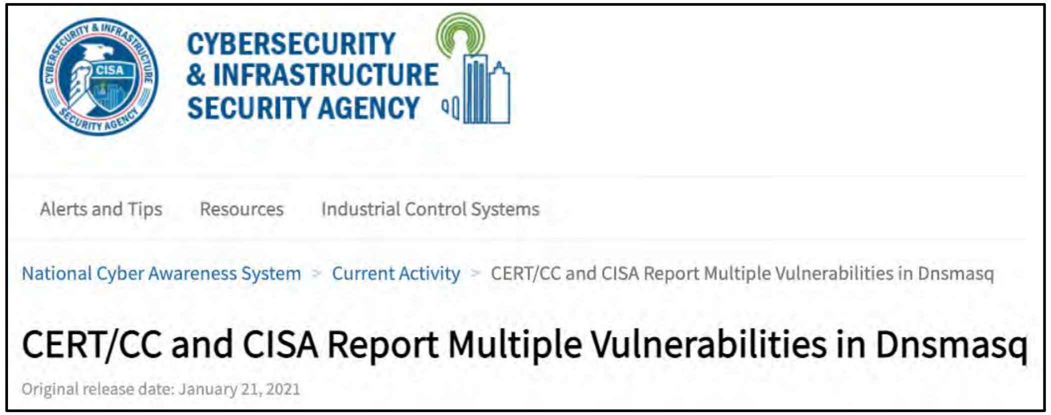
What's our exposure to this?



CVE-2021-3156 Vulnerable Assets

IP Address	Asset Name	Count
10.0.0.1	Desktop-005	11
10.0.0.2	Desktop-009	1
10.0.0.3	Desktop-045	1
192.168.0.1	Serv-01	1
192.168.0.2	Serv-13	2

Another flaw you can't ignore...



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Current Activity > CERT/CC and CISA Report Multiple Vulnerabilities in Dnsmasq

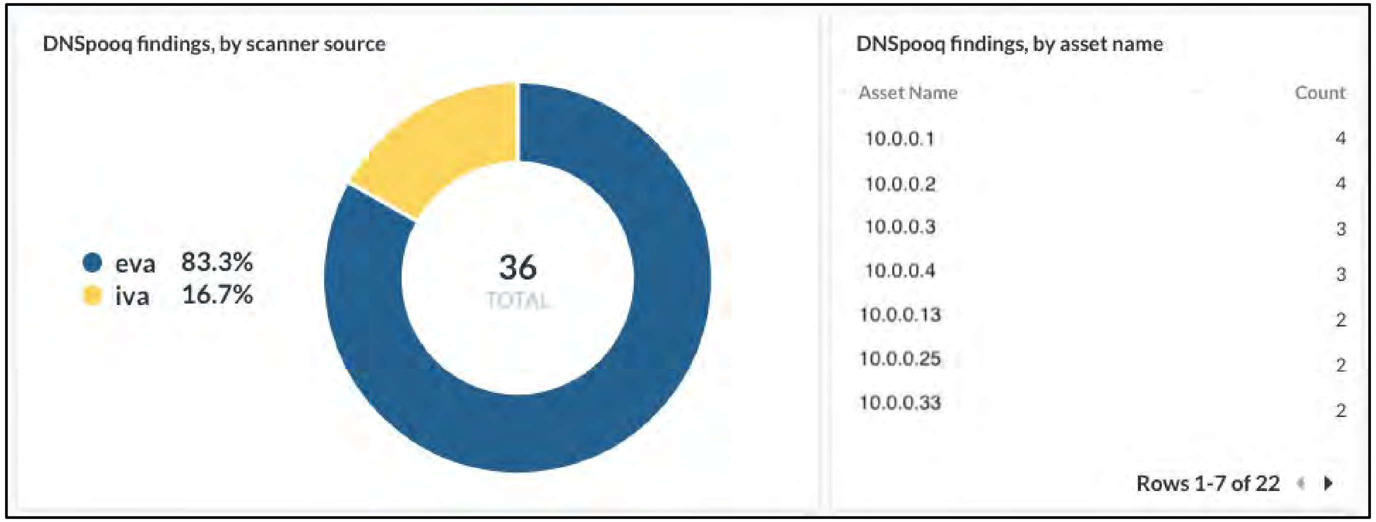
CERT/CC and CISA Report Multiple Vulnerabilities in Dnsmasq

Original release date: January 21, 2021

MANAGED RISK

High-profile vulnerabilities always lead to the same question:

What's our exposure to this?



DNSpooq findings, by scanner source

DNSpooq findings, by asset name

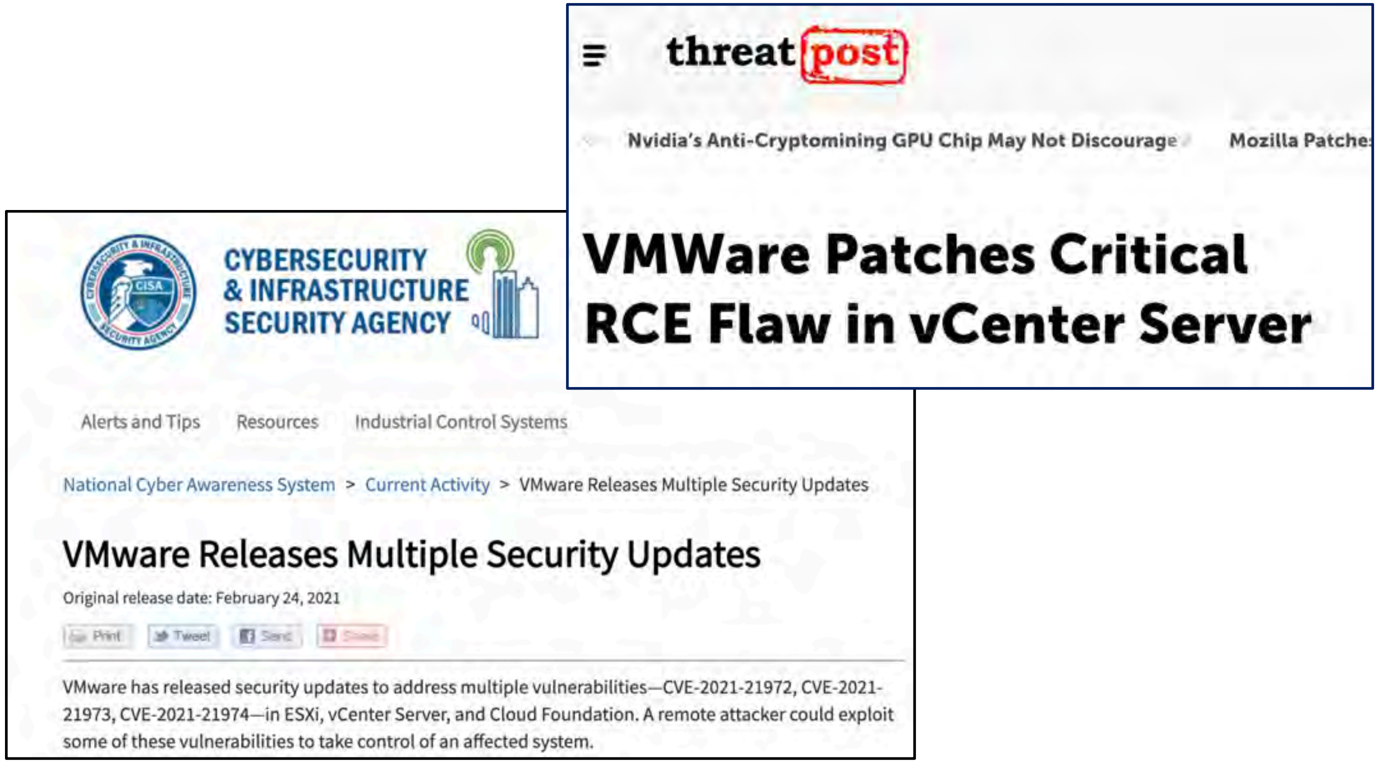
Asset Name	Count
10.0.0.1	4
10.0.0.2	4
10.0.0.3	3
10.0.0.4	3
10.0.0.13	2
10.0.0.25	2
10.0.0.33	2

Rows 1-7 of 22

What’s our exposure to this?

ASMGi ONEteam

ARCTIC WOLF



threatpost

Nvidia’s Anti-Cryptomining GPU Chip May Not Discourage Mozilla Patche

VMWare Patches Critical RCE Flaw in vCenter Server

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Current Activity > VMware Releases Multiple Security Updates

VMware Releases Multiple Security Updates

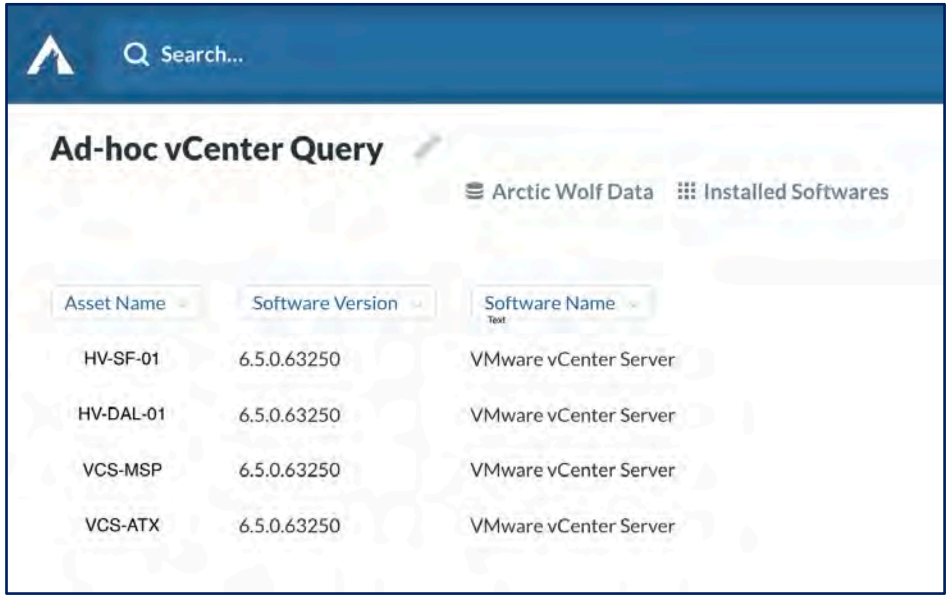
Original release date: February 24, 2021

VMware has released security updates to address multiple vulnerabilities—CVE-2021-21972, CVE-2021-21973, CVE-2021-21974—in ESXi, vCenter Server, and Cloud Foundation. A remote attacker could exploit some of these vulnerabilities to take control of an affected system.

High-profile vulnerabilities always lead to the same question.

Managed Risk helps you answer, quickly.

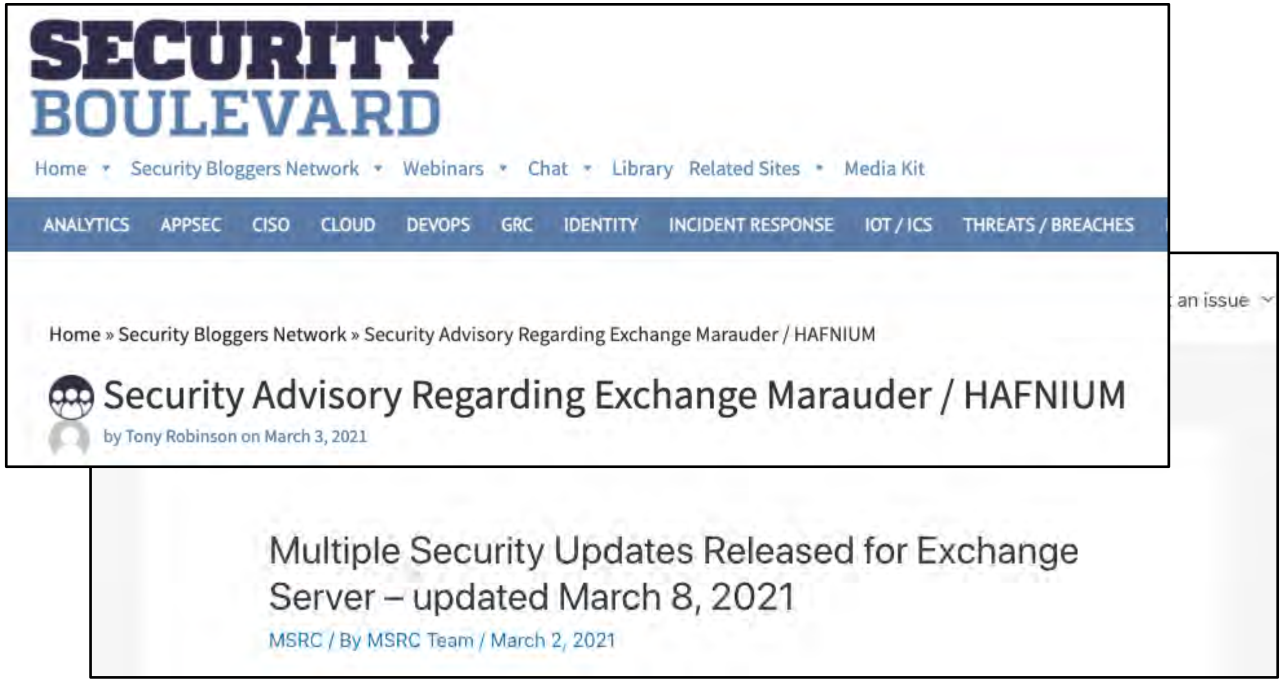
MANAGED RISK



Ad-hoc vCenter Query

Asset Name	Software Version	Software Name
HV-SF-01	6.5.0.63250	VMware vCenter Server
HV-DAL-01	6.5.0.63250	VMware vCenter Server
VCS-MSP	6.5.0.63250	VMware vCenter Server
VCS-ATX	6.5.0.63250	VMware vCenter Server

What's our exposure to this?



SECURITY BOULEVARD

Home • Security Bloggers Network • Webinars • Chat • Library Related Sites • Media Kit
ANALYTICS APPSEC CISO CLOUD DEVOPS GRC IDENTITY INCIDENT RESPONSE IOT / ICS THREATS / BREACHES
an issue

Home » Security Bloggers Network » Security Advisory Regarding Exchange Marauder / HAFNIUM

Security Advisory Regarding Exchange Marauder / HAFNIUM

by Tony Robinson on March 3, 2021

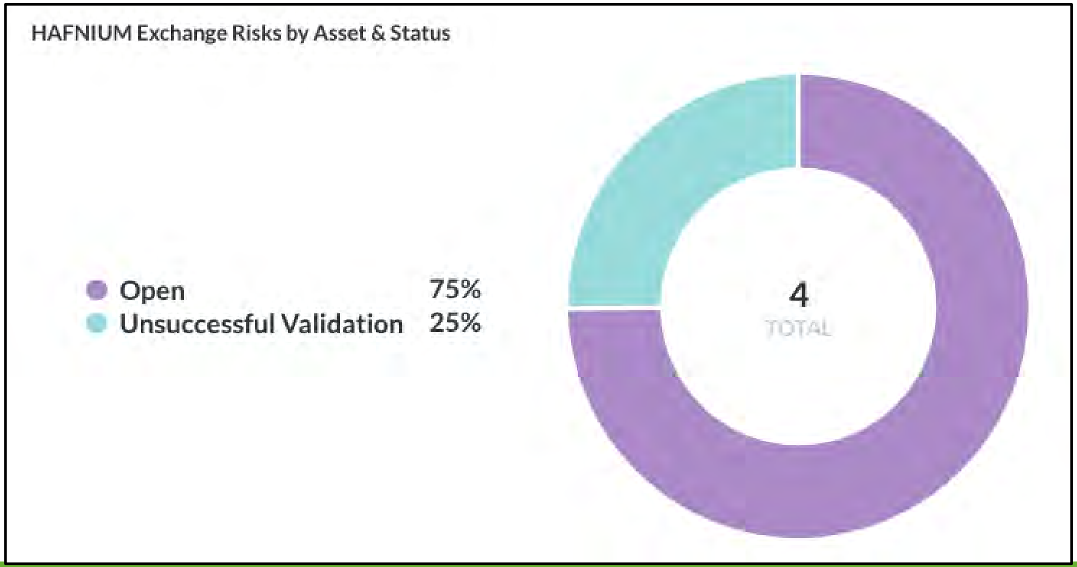
Multiple Security Updates Released for Exchange Server – updated March 8, 2021

MSRC / By MSRC Team / March 2, 2021

MANAGED RISK

High-profile vulnerabilities always lead to the same question.

Managed Risk helps you answer, quickly.



HAFNIUM Exchange Risks by Asset & Status

CYBER SECURITY SOLUTIONS

How do we lower Cyber Risk?

CYBER SECURITY SOLUTIONS

RISK = Likelihood x Impact

We Lower "Likelihood" by:

- Remediating Vulnerabilities makes "Likelihood = 0" and prevents an attack.
- Identifying Vulnerabilities continuously and across all modes, Account Takeovers, External, Network-based, Host-based helps reduce Likelihood, and if the Vulnerabilities are remediated, makes "Likelihood = 0".

We Lower "Impact" by:

- Identifying intruders quickly to reduce the Impact of an incident. The longer an intruder spends on your network (dwell time), the larger the Impact. If the intruder is detected quickly, Impact may even be eliminated completely.
- Containment of the incident reduces the Impact of an incident. We contain incidents both manually and using automation.
- Structured, rehearsed Incident Response Program (including table-top exercises)

What is ONEteam MDR/MSOC *plus*?

ONEteam
MDR/MSOC *plus*

=

ARCTIC WOLF + ASMGi

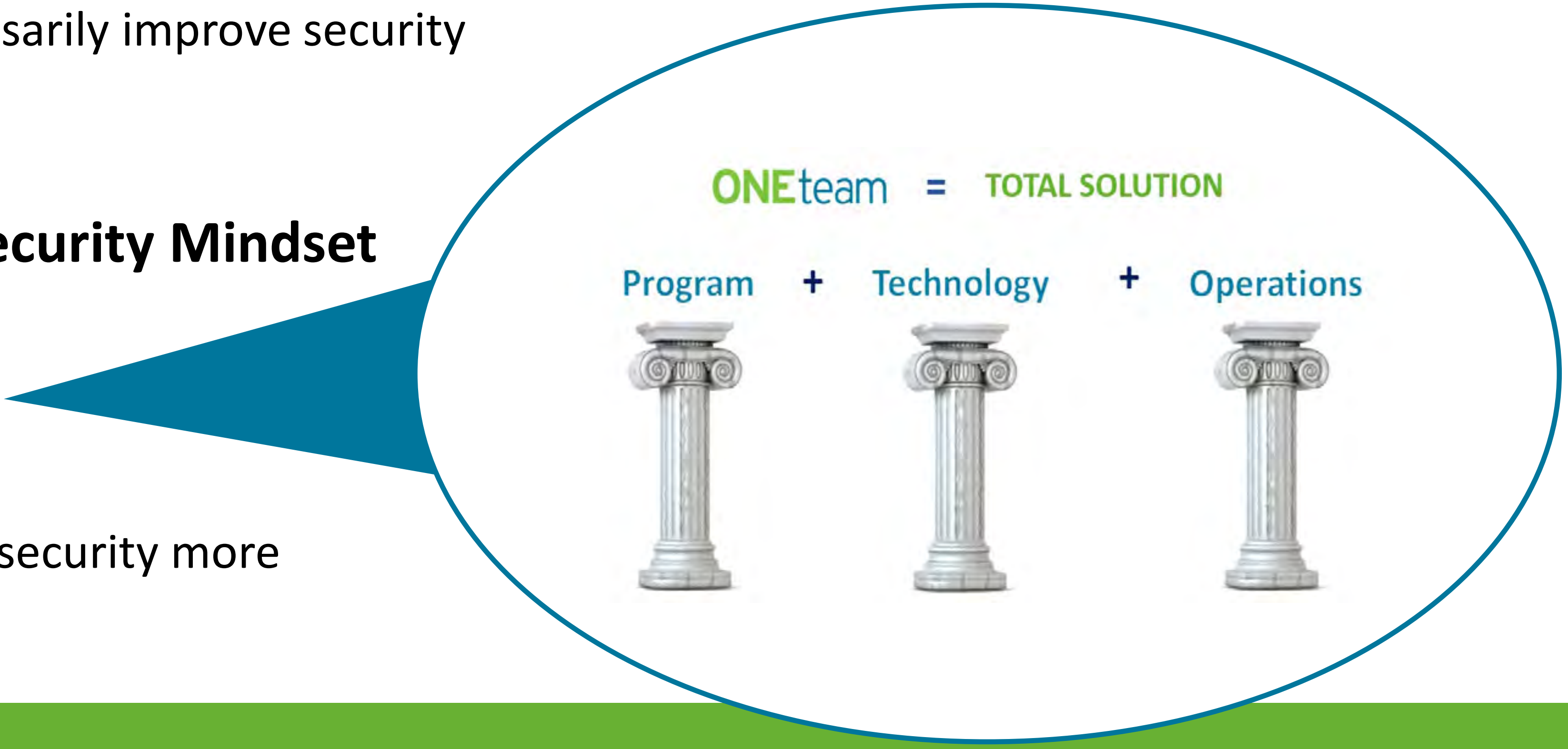
Cyber Security – ONEteam Principles

The Old Way: Point-Solution Mindset

- Reactive
- Focus on Individual Controls
- Fragmented and inefficient
- Spend a lot and not necessarily improve security

The New Way: Holistic Security Mindset

- Proactive
- Focus on Total Solutions
- Gap-Based & Risk-Based
- Spend less and improve security more


ONEteam = TOTAL SOLUTION

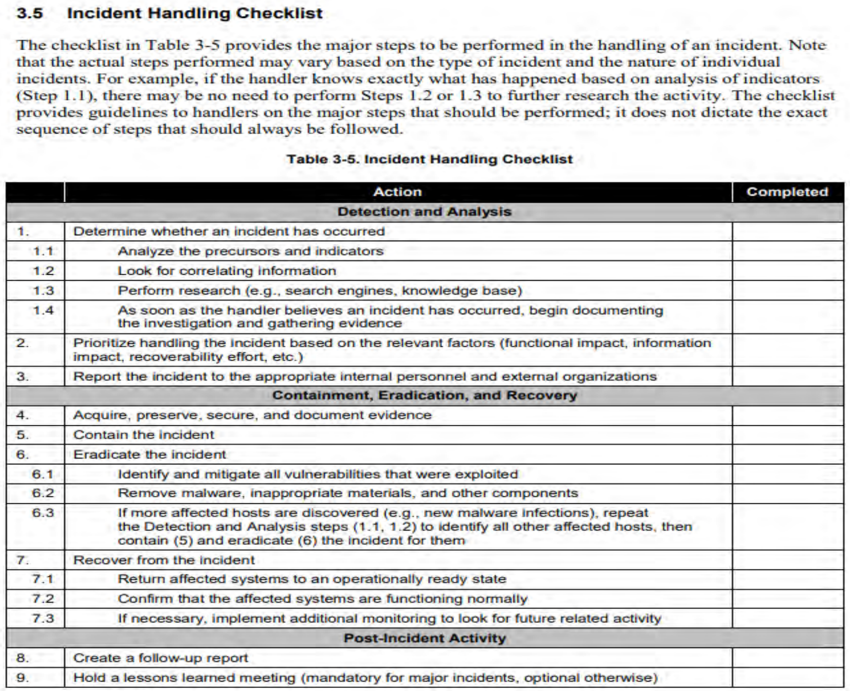
Program + Technology + Operations

TOTAL SOLUTION:

ASMGi ONEteam | ARCTIC WOLF

ONEteam
MDR/MSOC *plus*

- ◆ Security Operations Centers (SOCs)
- ◆ Managed Detect and Response
- ◆ Managed Risk Services
- ◆ Managed Cloud Monitoring
- ◆ Cyber Incident Response / Forensics
- ◆ Vulnerability Management and Remediation



3.5 Incident Handling Checklist

The checklist in Table 3-5 provides the major steps to be performed in the handling of an incident. Note that the actual steps performed may vary based on the type of incident and the nature of individual incidents. For example, if the handler knows exactly what has happened based on analysis of indicators (Step 1.1), there may be no need to perform Steps 1.2 or 1.3 to further research the activity. The checklist provides guidelines to handlers on the major steps that should be performed; it does not dictate the exact sequence of steps that should always be followed.

Table 3-5. Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Key

- Arctic Wolf + ASMGi
- ASMGi

The Complete Cybersecurity Operations Platform

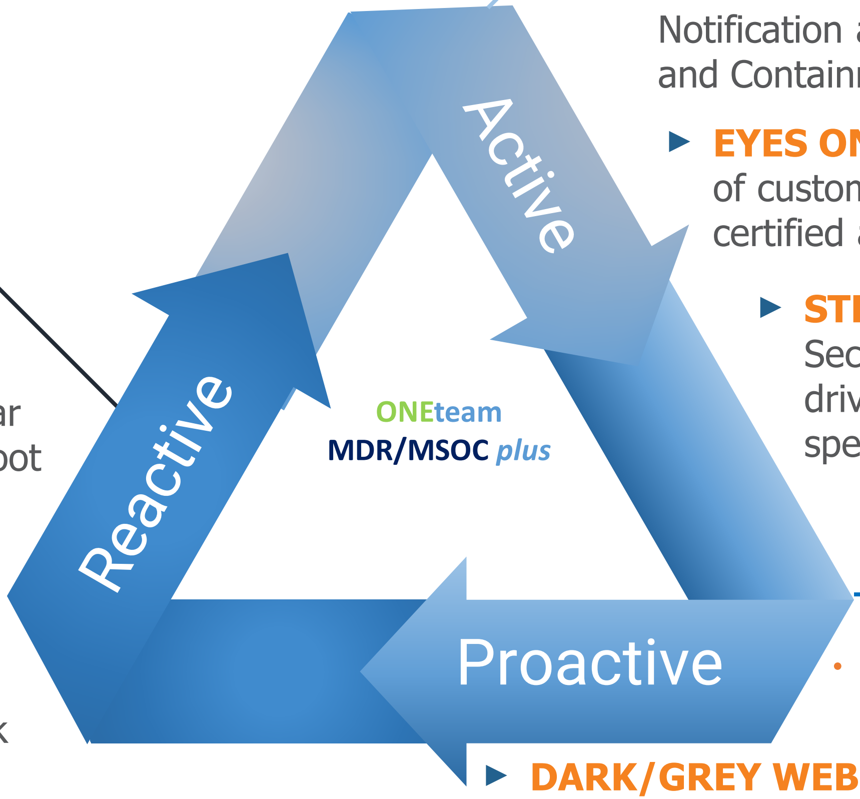
Security Operations

ASMGi ONEteam

ARCTIC WOLF

Managed Detection & Response

- **PROACTIVELY** provides IDS, Dark Web Scanning, and Endpoint Intelligence
- **REMEDIATION** Including detailed steps, War Room Assistance, Required Reporting, and Root Cause Analysis Detail
- **ACTIVE** monitoring of Cloud assets and resources for misconfigurations and vulnerabilities
- **ACTIVE** scanning of customer entire network environment to achieve and maintain broad visibility of assets agent or agentless



- **DETECTION** of in process attacks providing: Notification and Escalation, GEOIP Information, and Containment
- **EYES ON GLASS** 24/7/365 Human monitoring of customer environments by experienced, certified and skilled security experts
- **STRATEGIC** 2 Person, Named Concierge Security Team providing Security guidance, driving continuous improvement tailored to the specific needs of each organization.

Managed Risk

- **PREVENTION** of known attacks before they occur by limiting known attack surfaces
- **DARK/GREY WEB SCANNING** for customer accounts that may have been compromised
- **CONTINUOUS** vulnerability scanning of networks and endpoints
- **RISK QUANTIFICATION** from external and internal networks assets, regardless of Arctic Wolf Agent installation capability
- **REMEDIATION PRIORITIZATION** Detailed correlation of risks

SOC 2 TYPE 2

CERTIFIED ISO 27001 CERTIFIED

NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover

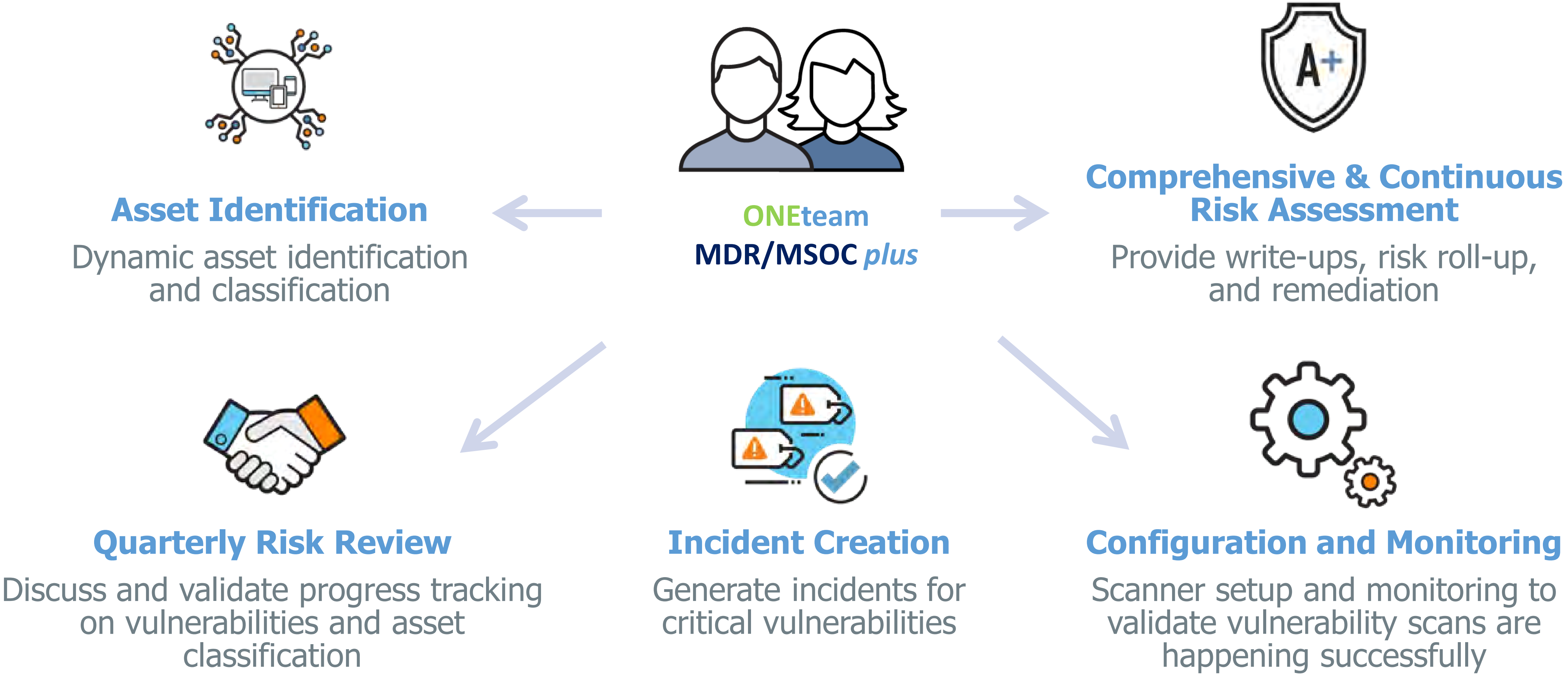
Cybersecurity Maturity Model Certification — DFARS — NIST 800-171 Compliance

GDPR READY

ASMGi ONEteam

ARCTIC WOLF

Managed Risk Services



ONEteam
MDR/MSOC *plus*

Asset Identification

Dynamic asset identification and classification

Comprehensive & Continuous Risk Assessment

Provide write-ups, risk roll-up, and remediation

Quarterly Risk Review

Discuss and validate progress tracking on vulnerabilities and asset classification

Incident Creation

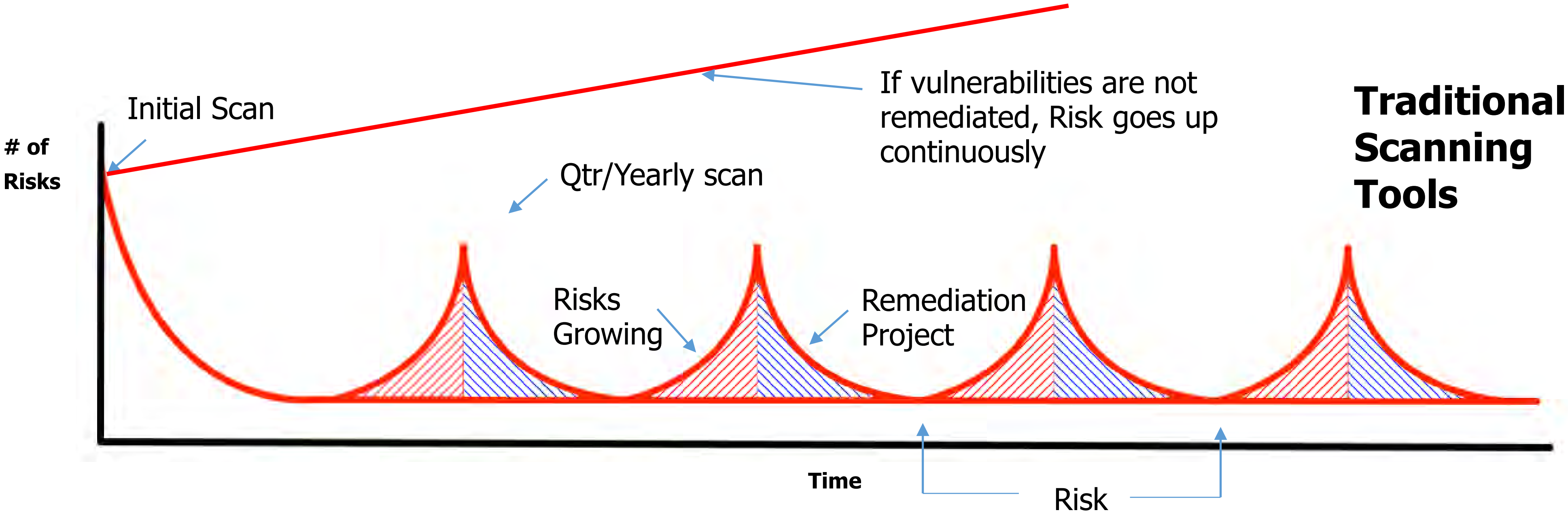
Generate incidents for critical vulnerabilities

Configuration and Monitoring

Scanner setup and monitoring to validate vulnerability scans are happening successfully

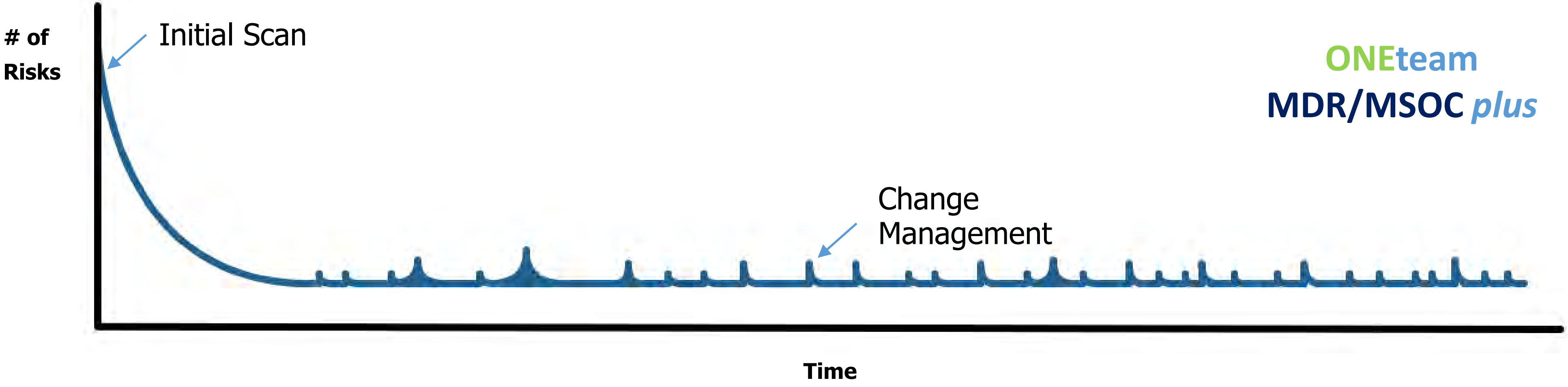
Continuous Cyber Risk Assessment

Point In Time Scans



Traditional Scanning Tools

Continuous Scans

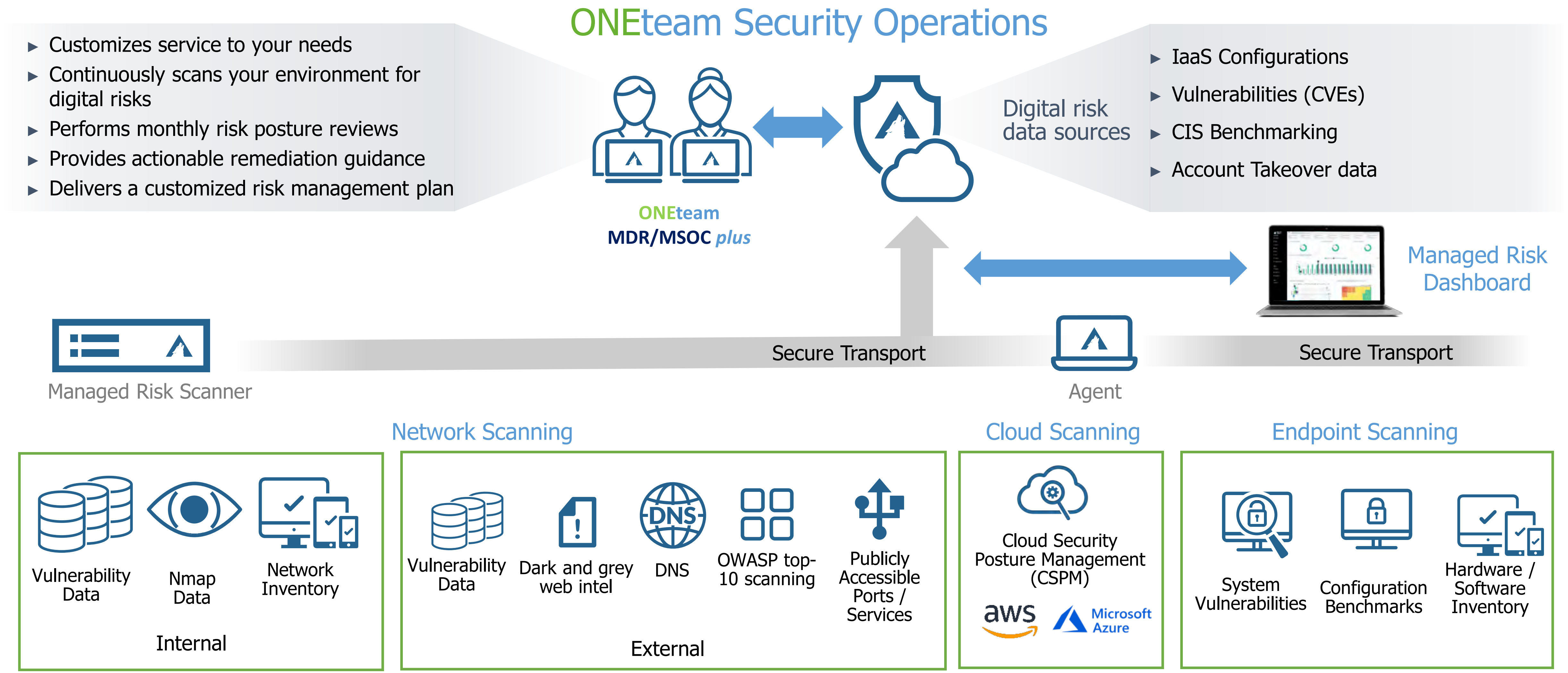


ONEteam
MDR/MSOC *plus*

ASMGi ONEteam

ARCTIC WOLF

Managed Risk Architecture



ONEteam Security Operations

- Customizes service to your needs
- Continuously scans your environment for digital risks
- Performs monthly risk posture reviews
- Provides actionable remediation guidance
- Delivers a customized risk management plan

Digital risk data sources

- IaaS Configurations
- Vulnerabilities (CVEs)
- CIS Benchmarking
- Account Takeover data

Network Scanning

Internal: Vulnerability Data; Nmap Data; Network Inventory

External: Vulnerability Data; Dark and grey web intel; DNS; OWASP top-10 scanning; Publicly Accessible Ports / Services

Cloud Scanning

Cloud Security Posture Management (CSPM)

Endpoint Scanning

System Vulnerabilities; Configuration Benchmarks; Hardware / Software Inventory

Managed Risk - Features

Analytics and Reporting

- Risk roll-up of internal + external vulnerabilities
- Risk prioritization and workflow integration
- Managed Risk Dashboard
- Executive reporting snapshots
- Custom reporting for analytics and alerts

Host-Based Vulnerability Assessment

- Arctic Wolf Agent for Windows Server/workstation, MacOS, Linux
- Proactive risk monitoring
- Audit reporting, asset categorization
- Security Controls Benchmarking

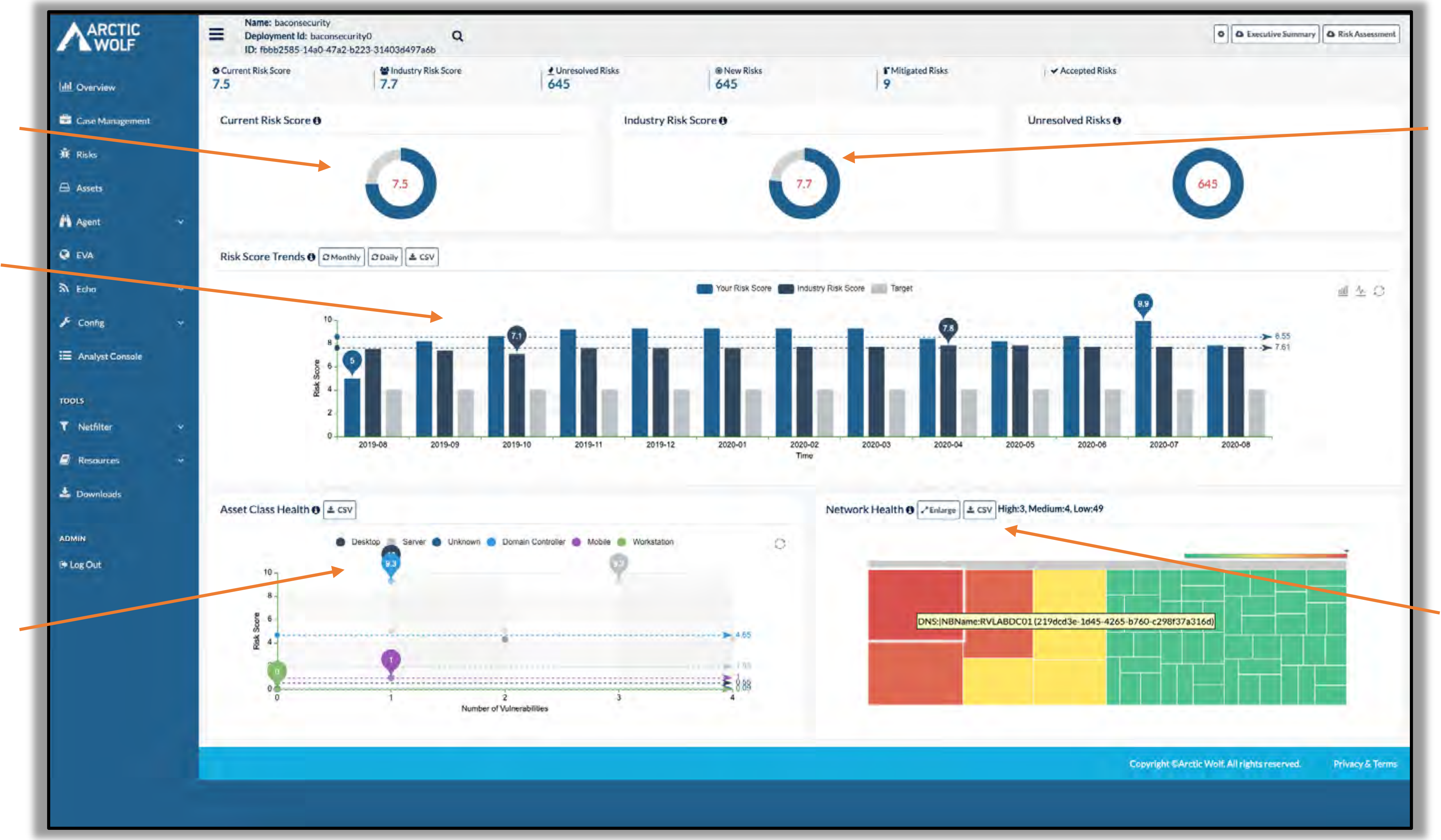
External Vulnerability Assessment

- Asset discovery based on root domains & IP addresses
- Automatic IP, domain, sub-domain detection
- Continuous external vulnerability scanning
- Account Takeover Risk Detection
- OWASP top-10 scanning
- Cloud Security Posture Management (CSPM)

Internal Vulnerability Assessment

- Dynamic asset discovery and credential scanning
- Asset inventory, categorization, notes, and tags
- Asset mapping - IP, DNS, Netbios history
- Continuous internal vulnerability scanning
- Scanning schedules with blacklisting capability

Managed Risk Dashboard



Name: baconsecurity
Deployment Id: baconsecurity0
ID: fbbb2585-14a0-47a2-b223-31403d497a6b

Current Risk Score	Industry Risk Score	Unresolved Risks	New Risks	Mitigated Risks	Accepted Risks
7.5	7.7	645	645	9	

Network Health High:3, Medium:4, Low:49

DNS:|NBName:RVLABDC01 (219dcd3e-1d45-4265-b760-c298f37a316d)

Copyright ©Arctic Wolf. All rights reserved.

Current Risk Score

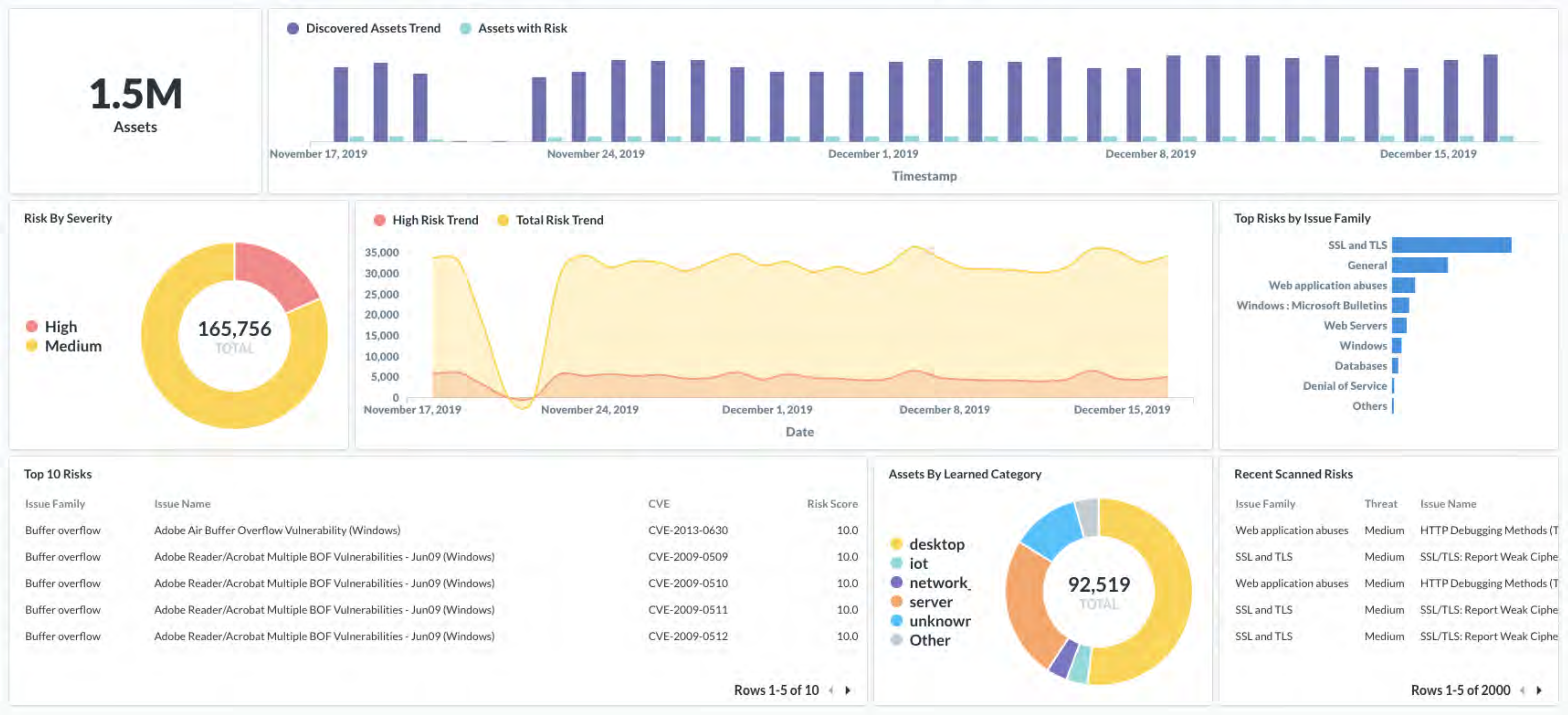
Risk Score Trends

Asset Class Health

Industry Risk Score

Network Health Heatmap

Quarterly Reports



Top 10 Risks

Issue Family	Issue Name	CVE	Risk Score
Buffer overflow	Adobe Air Buffer Overflow Vulnerability (Windows)	CVE-2013-0630	10.0
Buffer overflow	Adobe Reader/Acrobat Multiple BOF Vulnerabilities - Jun09 (Windows)	CVE-2009-0509	10.0
Buffer overflow	Adobe Reader/Acrobat Multiple BOF Vulnerabilities - Jun09 (Windows)	CVE-2009-0510	10.0
Buffer overflow	Adobe Reader/Acrobat Multiple BOF Vulnerabilities - Jun09 (Windows)	CVE-2009-0511	10.0
Buffer overflow	Adobe Reader/Acrobat Multiple BOF Vulnerabilities - Jun09 (Windows)	CVE-2009-0512	10.0

Rows 1-5 of 10

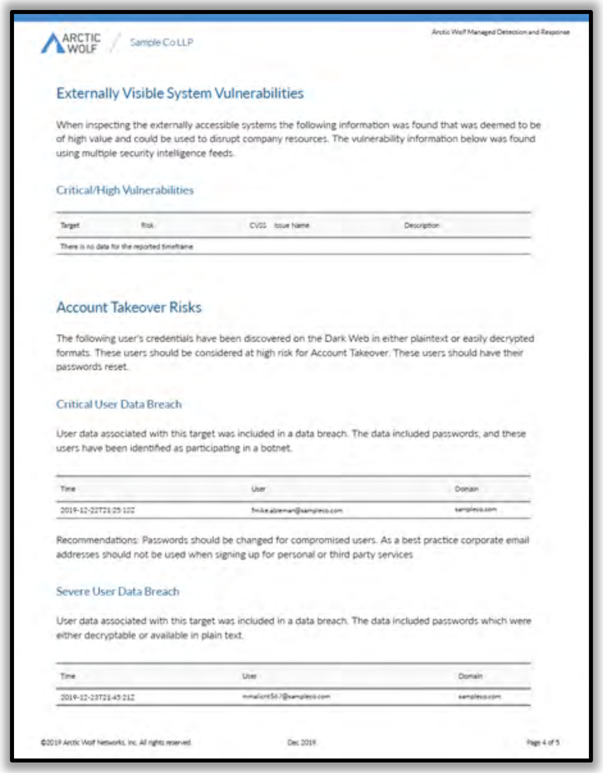
Recent Scanned Risks

Issue Family	Threat	Issue Name
Web application abuses	Medium	HTTP Debugging Methods (T
SSL and TLS	Medium	SSL/TLS: Report Weak Ciphe
Web application abuses	Medium	HTTP Debugging Methods (T
SSL and TLS	Medium	SSL/TLS: Report Weak Ciphe
SSL and TLS	Medium	SSL/TLS: Report Weak Ciphe

Rows 1-5 of 2000

Account Takeover Risk Detection

We continuously scan your environment against one of the world's largest repositories of third-party data breach information recovered from dark and grey web sources. This insight is used to produce observations and alert on potential account takeover situations at the scale of your business.



ARCTIC WOLF / Sample Co LLP

Arctic Wolf Managed Detection and Response

Externally Visible System Vulnerabilities

When inspecting the externally accessible systems the following information was found that was deemed to be of high value and could be used to disrupt company resources. The vulnerability information below was found using multiple security intelligence feeds.

Critical/High Vulnerabilities

Target	Risk	CVSS	Issue Name	Description
There is no data for the reported timeframe				

Account Takeover Risks

The following user's credentials have been discovered on the Dark Web in either plaintext or easily decrypted formats. These users should be considered at high risk for Account Takeover. These users should have their passwords reset.

Critical User Data Breach

User data associated with this target was included in a data breach. The data included passwords, and these users have been identified as participating in a botnet.

Time	User	Domain
2019-12-22T21:25:12Z	fmike.ableman@sampleco.com	sampleco.com

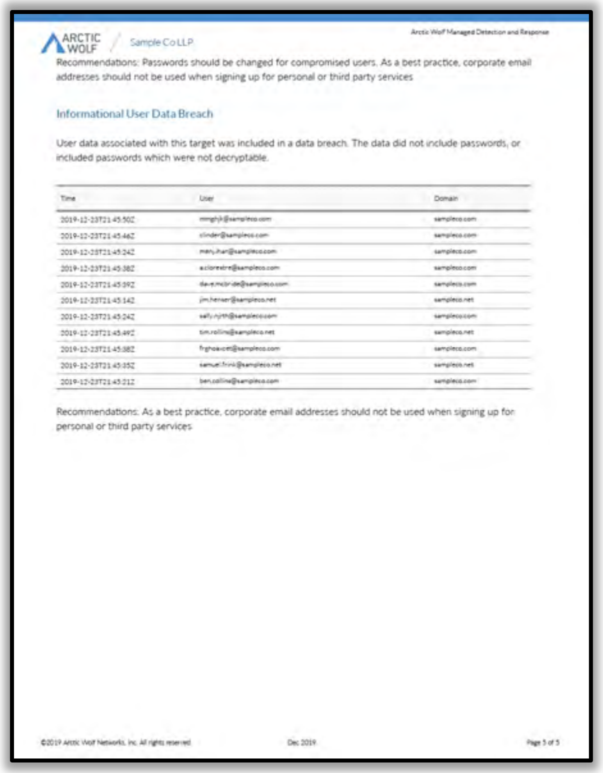
Recommendations: Passwords should be changed for compromised users. As a best practice corporate email addresses should not be used when signing up for personal or third party services

Severe User Data Breach

User data associated with this target was included in a data breach. The data included passwords which were either decryptable or available in plain text.

Time	User	Domain
2019-12-23T21:45:21Z	mmaliont567@sampleco.com	sampleco.com

©2019 Arctic Wolf Networks, Inc. All rights reserved. Dec 2019 Page 4 of 5



ARCTIC WOLF / Sample Co LLP

Arctic Wolf Managed Detection and Response

Recommendations: Passwords should be changed for compromised users. As a best practice, corporate email addresses should not be used when signing up for personal or third party services

Informational User Data Breach

User data associated with this target was included in a data breach. The data did not include passwords, or included passwords which were not decryptable.

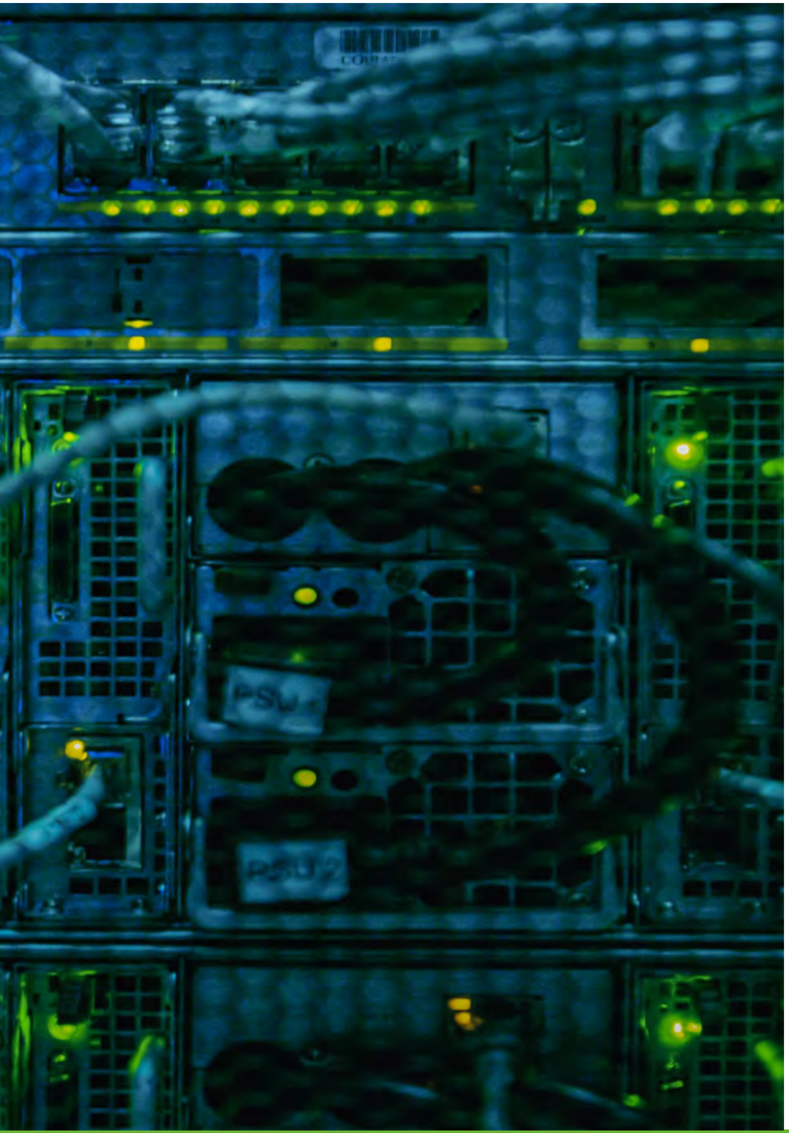
Time	User	Domain
2019-12-23T21:45:50Z	mmghjk@sampleco.com	sampleco.com
2019-12-23T21:45:46Z	clinder@sampleco.com	sampleco.com
2019-12-23T21:45:24Z	mery.ihar@sampleco.com	sampleco.com
2019-12-23T21:45:38Z	a.clorestre@sampleco.com	sampleco.com
2019-12-23T21:45:39Z	dave.mcbride@sampleco.com	sampleco.com
2019-12-23T21:45:14Z	jim.henser@sampleco.net	sampleco.net
2019-12-23T21:45:24Z	sally.njrth@sampleco.com	sampleco.com
2019-12-23T21:45:49Z	tim.rollins@sampleco.net	sampleco.net
2019-12-23T21:45:38Z	frghoacett@sampleco.com	sampleco.com
2019-12-23T21:45:35Z	samuel.frink@sampleco.net	sampleco.net
2019-12-23T21:45:21Z	ben.collins@sampleco.com	sampleco.com

Recommendations: As a best practice, corporate email addresses should not be used when signing up for personal or third party services

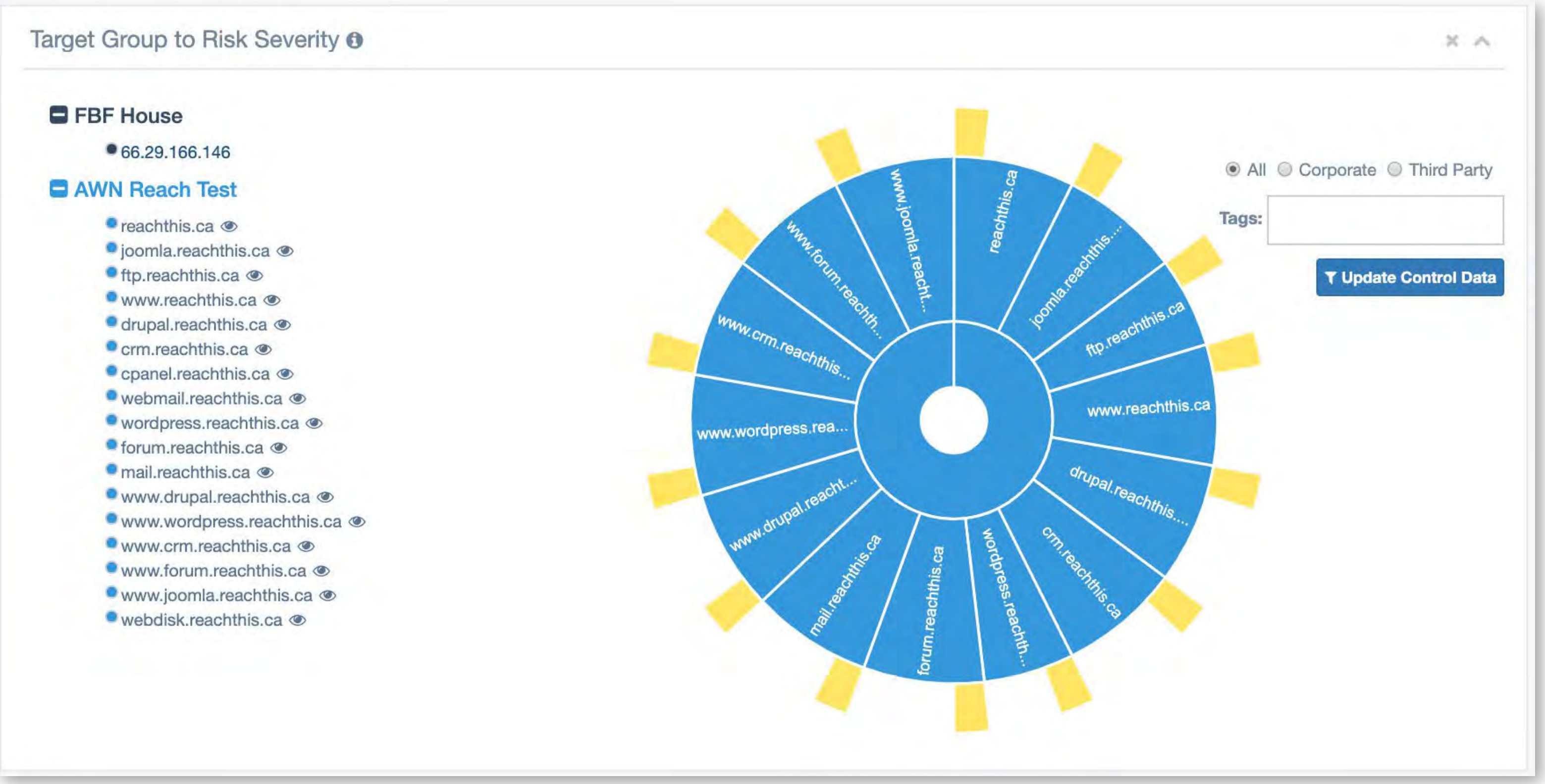
©2019 Arctic Wolf Networks, Inc. All rights reserved. Dec 2019 Page 5 of 5

Example of data breach information and additional context provided by Arctic Wolf

External Vulnerability Assessment



External Vulnerability Assessment continuously scans internet-facing servers and web applications to understand your company's digital footprint and quantify risk to your business.



Target Group to Risk Severity

- FBF House
  - 66.29.166.146
- AWN Reach Test
  - reachthis.ca
  - joomla.reachthis.ca
  - ftp.reachthis.ca
  - www.reachthis.ca
  - drupal.reachthis.ca
  - crm.reachthis.ca
  - cpanel.reachthis.ca
  - webmail.reachthis.ca
  - wordpress.reachthis.ca
  - forum.reachthis.ca
  - mail.reachthis.ca
  - www.drupal.reachthis.ca
  - www.wordpress.reachthis.ca
  - www.crm.reachthis.ca
  - www.forum.reachthis.ca
  - www.joomla.reachthis.ca
  - webdisk.reachthis.ca

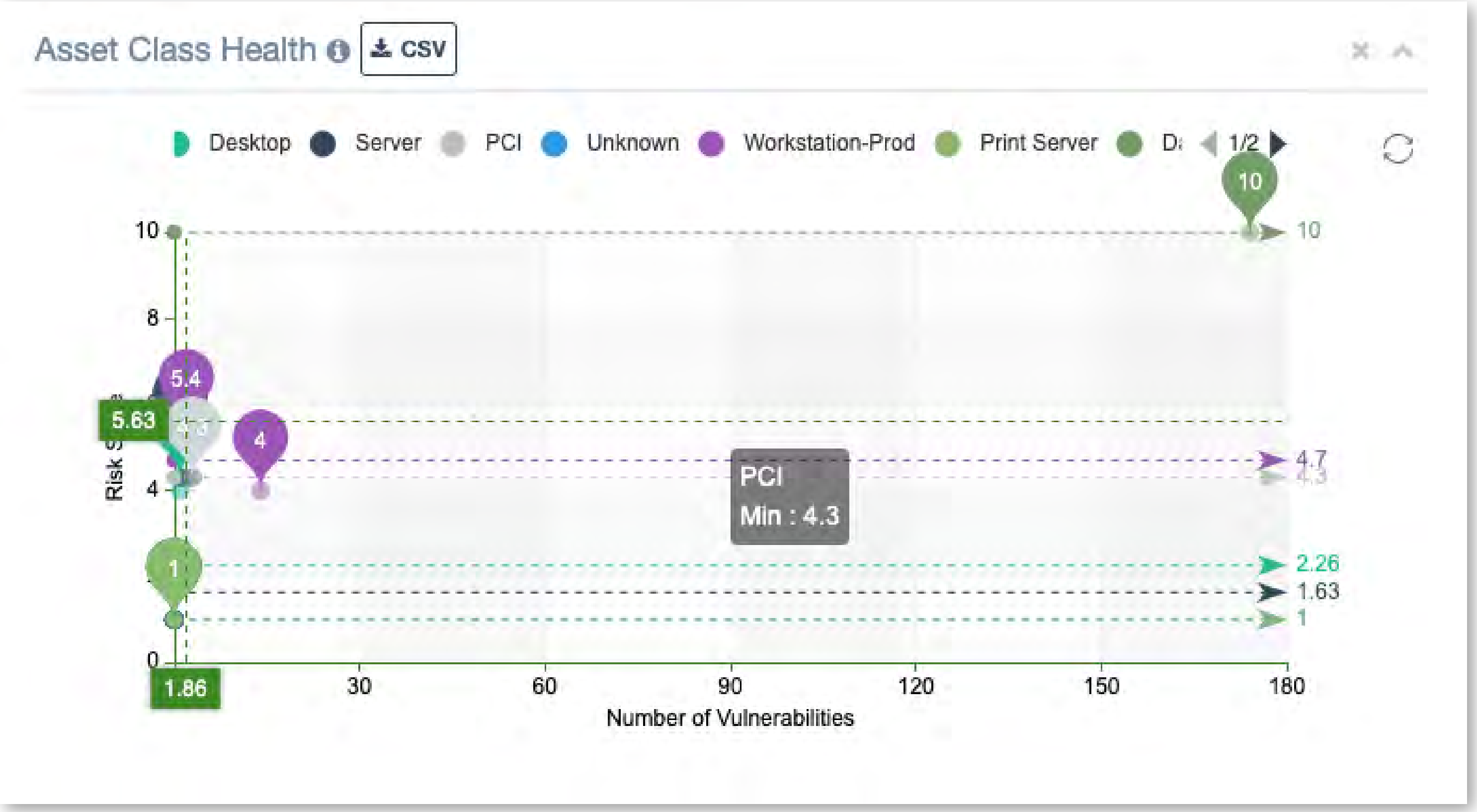
● All ○ Corporate ○ Third Party

Tags:

Sample output from External Vulnerability Assessment in Managed Risk Dashboard

Network Vulnerability Assessment

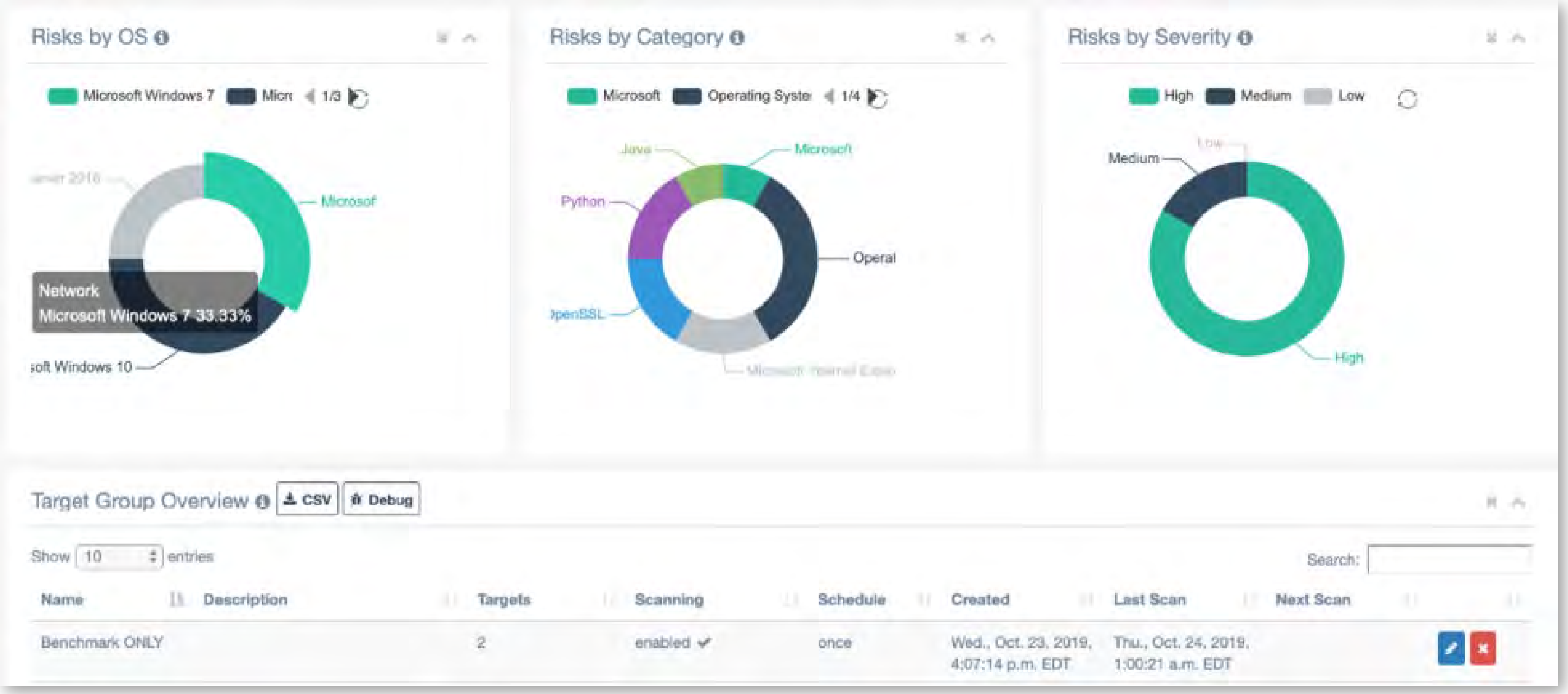
Internal Vulnerability Assessment continuously scans all your internal IP-connected devices. Your Concierge Security Team catalogues core infrastructure, equipment, and personal devices to help you understand your company's digital footprint and quantify the risk/exposure to your business.



Sample output from Internal Vulnerability Assessment in Managed Risk Dashboard

Host-based Vulnerability Assessment

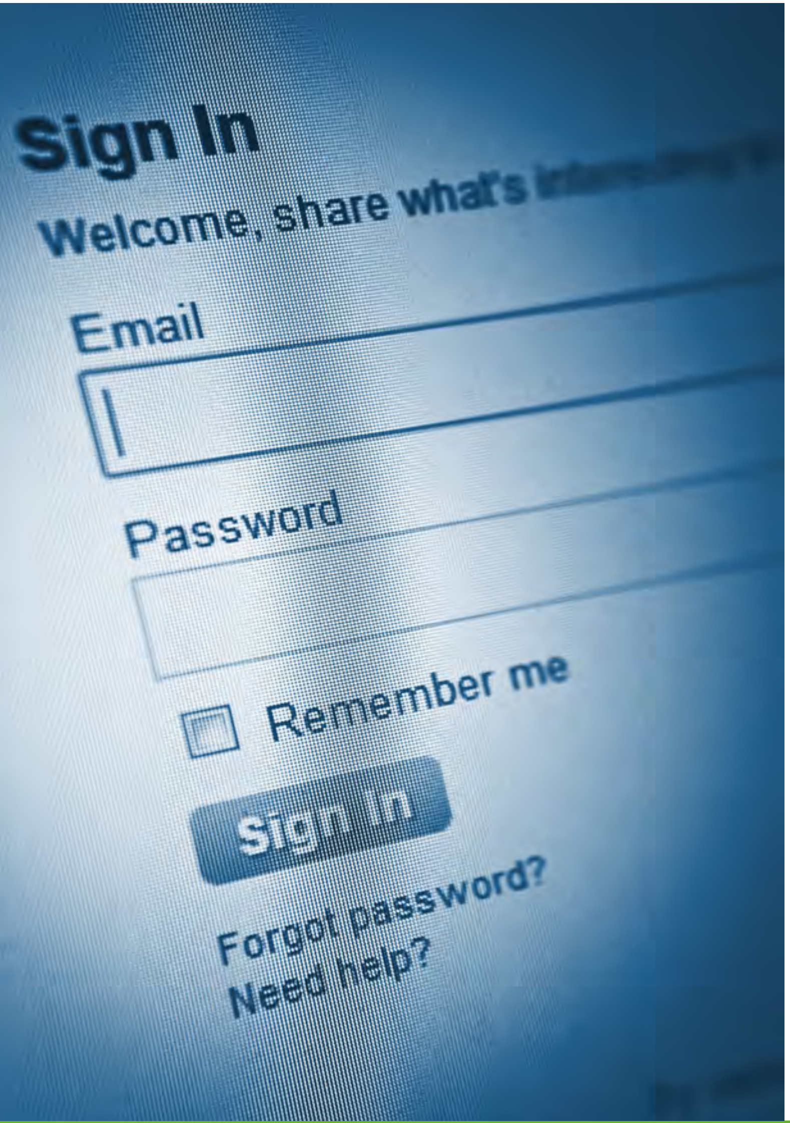
Host-Based Vulnerability Assessment extends visibility to endpoints such as Windows, MacOS, and Linux-based systems to reveal threats, system misconfigurations, and user behavior that put your organization at risk.



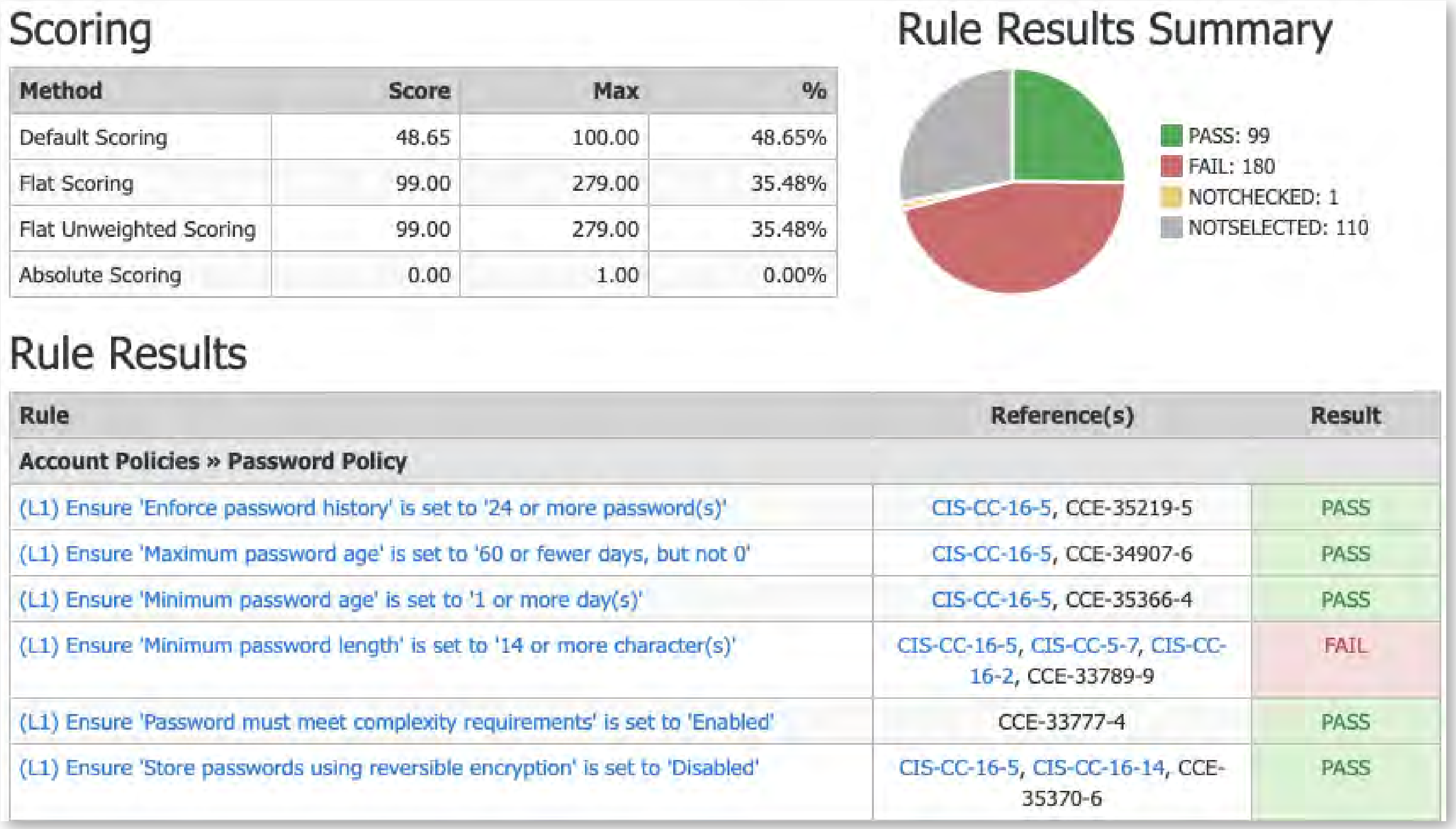
Name	Description	Targets	Scanning	Schedule	Created	Last Scan	Next Scan
Benchmark ONLY		2	enabled ✓	once	Wed., Oct. 23, 2019, 4:07:14 p.m. EDT	Thu., Oct. 24, 2019, 1:00:21 a.m. EDT	

Sample output from Host-based Vulnerability Assessment in Managed Risk Dashboard

Security Controls Benchmarking



Provides enhanced scanning coverage that goes beyond simple vulnerability assessment to scan endpoints for gaps in security posture against globally-accepted configuration standards.



Scoring

Method	Score	Max	%
Default Scoring	48.65	100.00	48.65%
Flat Scoring	99.00	279.00	35.48%
Flat Unweighted Scoring	99.00	279.00	35.48%
Absolute Scoring	0.00	1.00	0.00%

Rule Results Summary

- 🟩 PASS: 99
- 🟥 FAIL: 180
- 🟨 NOTCHECKED: 1
- ▨ NOTSELECTED: 110

Rule Results

Rule	Reference(s)	Result
Account Policies » Password Policy		
(L1) Ensure 'Enforce password history' is set to '24 or more password(s)'	CIS-CC-16-5, CCE-35219-5	PASS
(L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'	CIS-CC-16-5, CCE-34907-6	PASS
(L1) Ensure 'Minimum password age' is set to '1 or more day(s)'	CIS-CC-16-5, CCE-35366-4	PASS
(L1) Ensure 'Minimum password length' is set to '14 or more character(s)'	CIS-CC-16-5, CIS-CC-5-7, CIS-CC-16-2, CCE-33789-9	FAIL
(L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'	CCE-33777-4	PASS
(L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	CIS-CC-16-5, CIS-CC-16-14, CCE-35370-6	PASS

Sample output from Security Controls Benchmarking report in Managed Risk Dashboard

Managed Risk - Benefits

Program Benefits

- Monthly risk reviews
- Quarterly risk roll-up and progress tracking
- Tickets and alerts from your security operations experts
- Classification and organization of assets and risks
- Sensor configuration and monitoring
- Actionable remediation and guidance
- Customized risk-based vulnerability management plan

Solution Benefits

- Complete visibility and quantified risk analytics across endpoints, networks (internal and external), and cloud environments
- Risk prioritization based on severity, latest exploits and business impact
- Remediation with automated trouble ticketing
- Account Takeover Risk reporting
- Configuration benchmarking

Upcoming ASMGi Cyber Security Webinar with Arctic Wolf

Don't Let Your Cloud Security Fall Behind

presented by ASMGi and Arctic Wolf Networks
live webinar, ***April 8 at 1PM ET***

*Reply “**YES**” in the Question Box and we will preregister you for this webinar*

ASMGi ONEteam

ARCTIC WOLF

Q & A

ASMGi
ONEteam

ARCTIC
WOLF

For more information:

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Email: sales@asmgi.com

www.asmgi.com