SBE SMALL BUSINESS EXPO

An Inc. 5000 Company

DARKSTACK7

www.darkstack7.com

Cyber Security for Small Businesses (Top 10 Best Practices)

Joshua R Nicholson
Cyber Security Expert
Founder & Chief Mentor

(@nicholsonj7111) / Twitter
Joshua.r.Nicholson@darkstack7.com

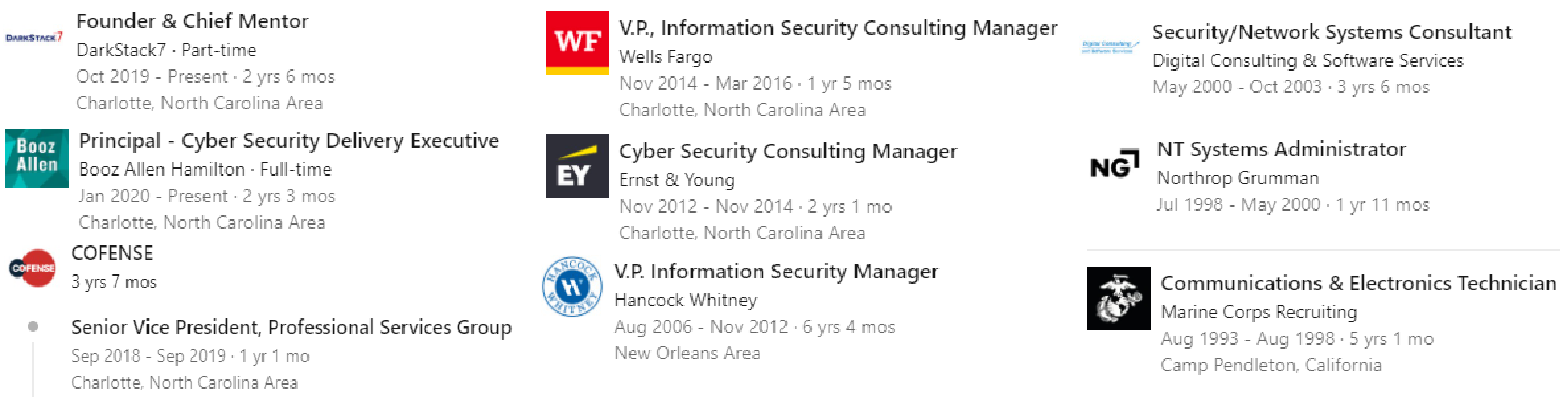
Joshua.r.Nicholson@darkstack7.com

Biography

22 Years of cyber security experience leading Incident Response and Security Engineering teams (SVP / Functional CISO)

- ➢ Leader in Booz Allen Hamilton (Managed Services) Cyber Defense team
- ➢ Cyber Fusion Center (CFC) Build Lead - focused on the identification and integration of cutting-edged cyber security toolsets and automation systems
- ➢ SOC Leader for a multi-billion global U.S. biopharmaceutical company
- ➢ Executive Leader responsible for Service Delivery and Professional Services functions within our Managed Threat Services division for all customers
- ➢ Led and mentored a team of 76 security team members and 12 contractors operating in 6 countries and 10 time zones

Background / Bio



Founder & Chief Mentor
DarkStack7 · Part-time
Oct 2019 - Present · 2 yrs 6 mos
Charlotte, North Carolina Area

Principal - Cyber Security Delivery Executive
Booz Allen Hamilton · Full-time
Jan 2020 - Present · 2 yrs 3 mos
Charlotte, North Carolina Area

COFENSE
3 yrs 7 mos

Senior Vice President, Professional Services Group
Sep 2018 - Sep 2019 · 1 yr 1 mo
Charlotte, North Carolina Area

V.P., Information Security Consulting Manager
Wells Fargo
Nov 2014 - Mar 2016 · 1 yr 5 mos
Charlotte, North Carolina Area

Cyber Security Consulting Manager
Ernst & Young
Nov 2012 - Nov 2014 · 2 yrs 1 mo
Charlotte, North Carolina Area

V.P. Information Security Manager
Hancock Whitney
Aug 2006 - Nov 2012 · 6 yrs 4 mos
New Orleans Area

Security/Network Systems Consultant
Digital Consulting & Software Services
May 2000 - Oct 2003 · 3 yrs 6 mos

NT Systems Administrator
Northrop Grumman
Jul 1998 - May 2000 · 1 yr 11 mos

Communications & Electronics Technician
Marine Corps Recruiting
Aug 1993 - Aug 1998 · 5 yrs 1 mo
Camp Pendleton, California

Joshua.r.Nicholson@darkstack7.com

Background / Bio

Led and mentored a team of 76 security team members and 12 contractors operating in 6 countries and 10 time zones with an enterprise customer base of 465

Biography

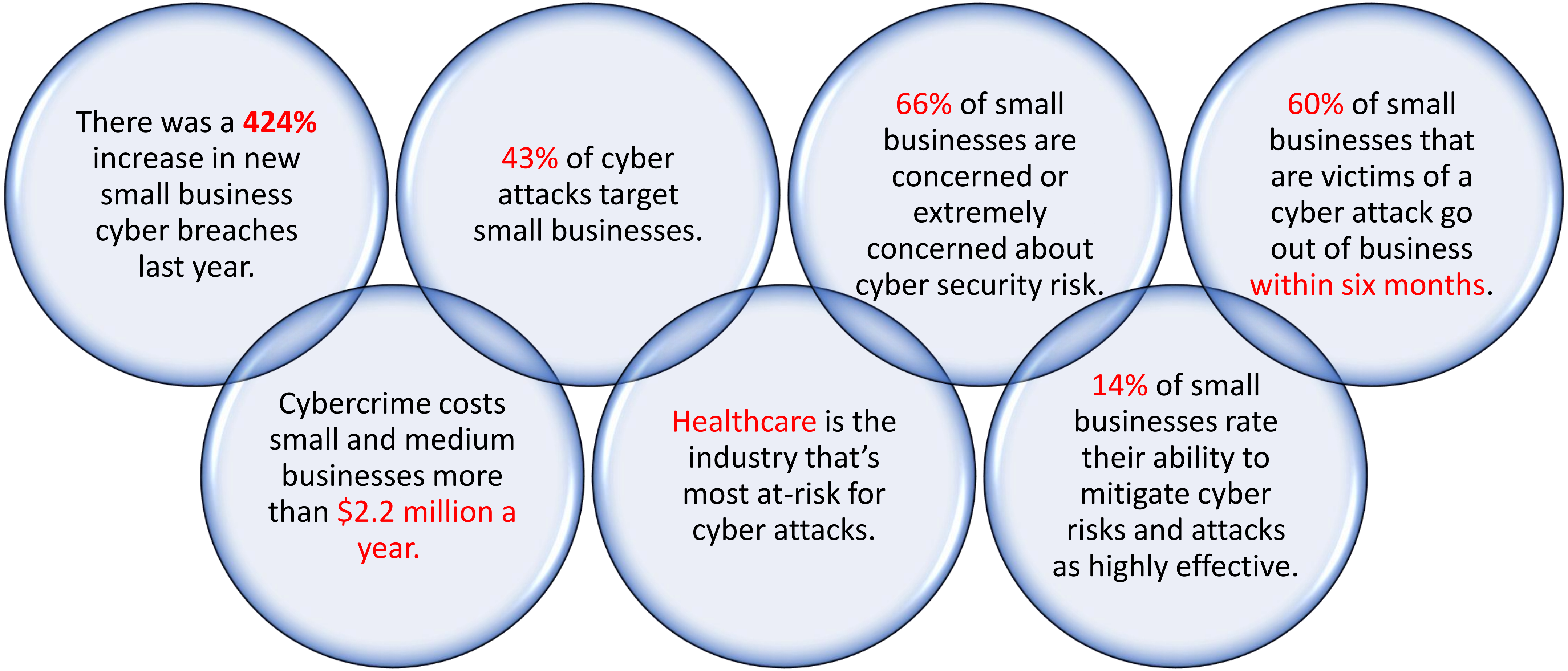
22 Years of cyber security experience leading Incident Response and Security Engineering teams (SVP / Functional CISO)

Global Execution

Cybersecurity Workshop for Managers
Information Security Department

*Broad experience working internationally in over **23 countries (e.g., U.K., EU, Middle East, Asia, Australia)** to maintain and build strong customer relationships with key foreign executives leading on services sales pursuits*

Small Business Threats



There was a **424%** increase in new small business cyber breaches last year.

43% of cyber attacks target small businesses.

66% of small businesses are concerned or extremely concerned about cyber security risk.

60% of small businesses that are victims of a cyber attack go out of business within six months.

Cybercrime costs small and medium businesses more than $2.2 million a year.

Healthcare is the industry that’s most at-risk for cyber attacks.

14% of small businesses rate their ability to mitigate cyber risks and attacks as highly effective.

30 Surprising Small Business Cyber Security Statistics (2021) - Fundera Ledger

Objectives - Outcomes | Enterprise Cybersecurity | Small Business focus | Tech Guidance | Action Plan

Small Business Cyber Security

Objectives

- Expose you to the world of enterprise cybersecurity
- Provide you with understanding of basic security controls
- Present practices that have the greatest impact to risk reduction

Methodology

- Distill advanced cyber security principles into focused and discrete actions you can take
- Focus on best practices for organization with little to no dedicated security staff
- Focus on most impactful areas of risk

Structure

- Enterprise Cyber Fusion Center (CFC) overview and Operating Model
- Highlight low hanging hygiene issues
- Multi-dimensional approach to due diligence
- NIST Cyber Security framework

Outcomes

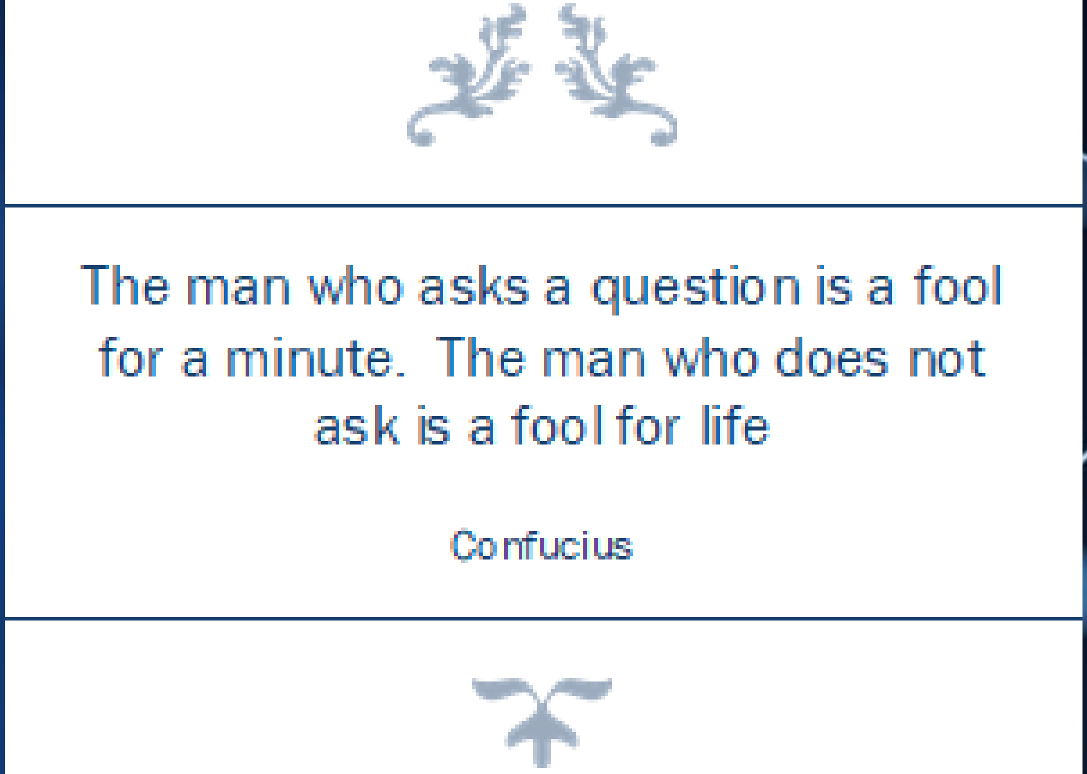
✓ Increase your understanding of the threats and vectors

✓ Empower you with actionable tactics

Admin Controls

Hardening guidance

Threat Protection

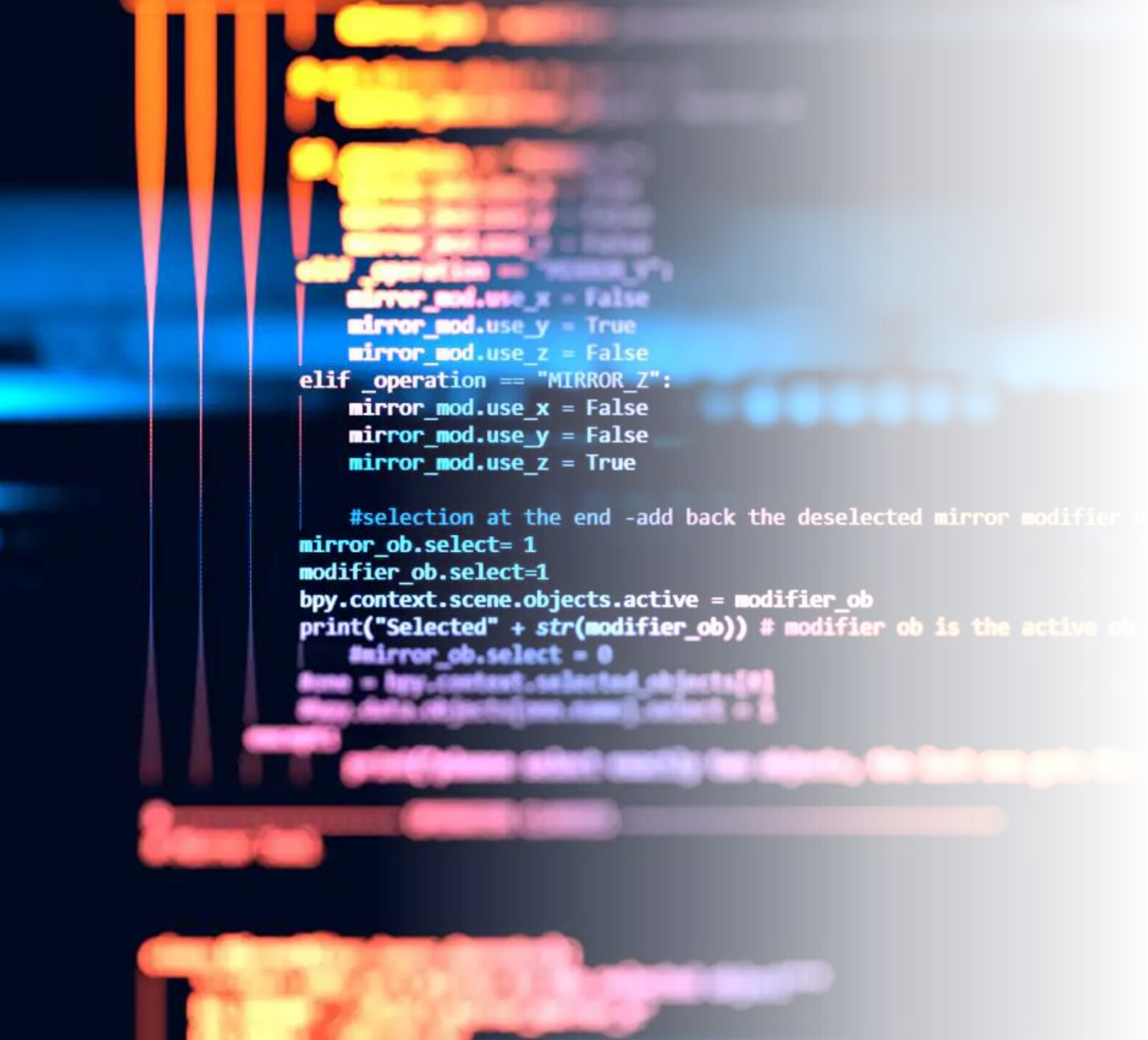


The man who asks a question is a fool for a minute. The man who does not ask is a fool for life

Confucius

Luck favors the prepared

Artificial Intelligence is no match for natural stupidity!



```
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

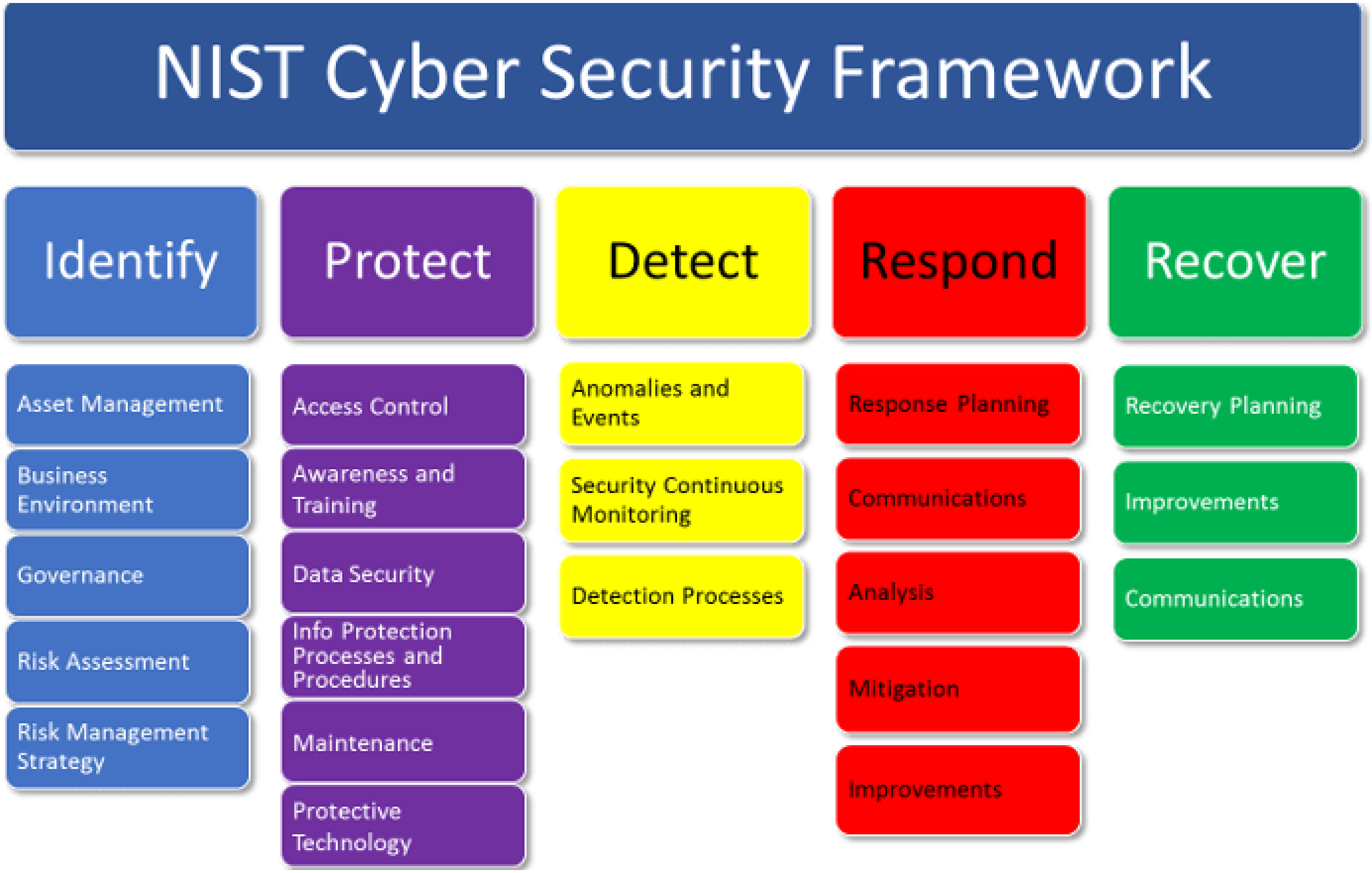
Enterprise Cyber Security

- NIST Cyber Security Framework
- Attacker Kill chain
- MITRE ATT&CK Matrix
- Risk Assessment & Prioritization
- Cyber Fusion Center (CFC)
  - **Operating Model**
  - **Attack Surface Reduction**
  - **CFC Run Books**
  - **3rd party cyber risks**

Understanding through frameworks

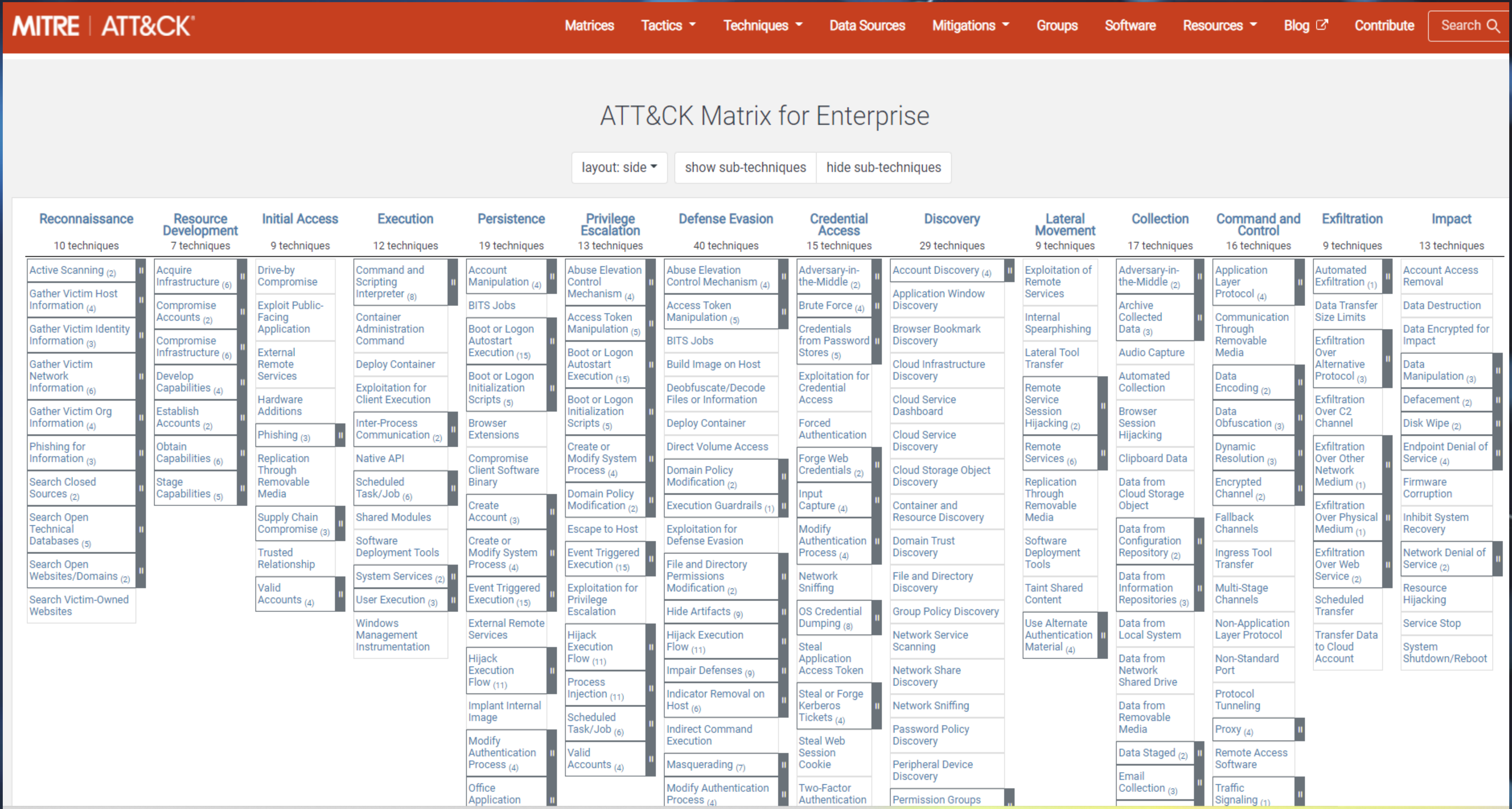
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The framework "provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes"



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			



ATT&CK Matrix for Enterprise

Reconnaissance
10 techniques

- Active Scanning (2)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (2)
- Search Victim-Owned Websites

Resource Development
7 techniques

- Acquire Infrastructure (6)
- Compromise Accounts (2)
- Compromise Infrastructure (6)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)
- Stage Capabilities (5)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
12 techniques

- Command and Scripting Interpreter (8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (2)
- Native API
- Scheduled Task/Job (6)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (4)
- BITS Jobs
- Boot or Logon Autostart Execution (15)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (11)
- Implant Internal Image
- Modify Authentication Process (4)
- Office Application

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (15)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Escape to Host
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (11)
- Process Injection (11)
- Scheduled Task/Job (6)
- Valid Accounts (4)

Defense Evasion
40 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (9)
- Hijack Execution Flow (11)
- Impair Defenses (9)
- Indicator Removal on Host (6)
- Indirect Command Execution
- Masquerading (7)
- Modify Authentication Process (4)

Credential Access
15 techniques

- Adversary-in-the-Middle (2)
- Brute Force (4)
- Credentials from Password Stores (5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Modify Authentication Process (4)
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Two-Factor Authentication

Discovery
29 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques

- Adversary-in-the-Middle (2)
- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (2)
- Data from Information Repositories (3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)

Command and Control
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (1)

Exfiltration
9 techniques

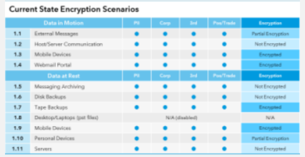
- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Assess Current State

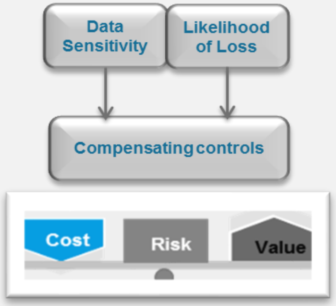
- Define & Assess detective and protective controls
- Evaluate people, process, technology weaknesses



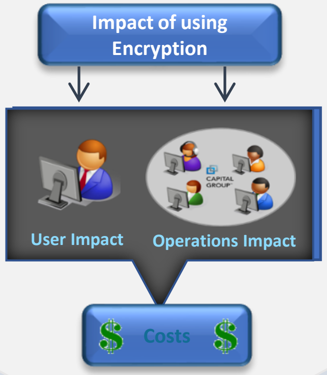
Current State Encryption Scenarios

Data in Motion		PII	Corp	3rd	Pos/Trade	Encryption
1.1	External Messages	●	●	●	●	Partial Encryption
1.2	Host/Server Communication	●	●	●	●	Not Encrypted
1.3	Mobile Devices	●	●	●	●	Encrypted
1.4	Webmail Portal	●	●	●	●	Encrypted
Data at Rest		**PII**	**Corp**	**3rd**	**Pos/Trade**	**Encryption**
1.5	Messaging Archiving	●	●	●	●	Not Encrypted
1.6	Disk Backups	●	●	●	●	Not Encrypted
1.7	Tape Backups	●	●	●	●	Encrypted
1.8	Desktop/Laptops (pst files)	N/A (disabled)				N/A
1.9	Mobile Devices	●	●	●	●	Encrypted
1.10	Personal Devices	●	●	●	●	Partial Encryption
1.11	Servers	●	●	●	●	Not Encrypted

Analyze and Prioritize

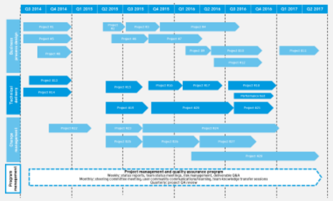


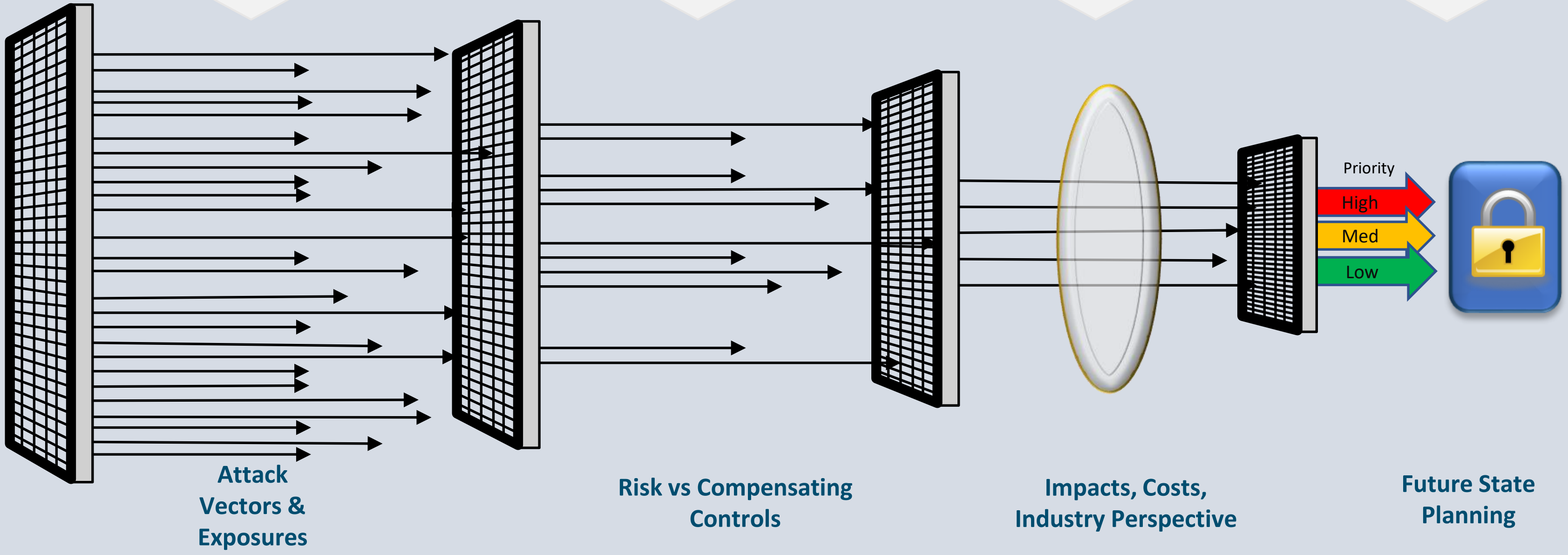
Develop Strategy



Roadmap

- Gap Analysis
- Prioritization
- Risk Transferal




Priority
High
Med
Low
Attack Vectors & Exposures
Risk vs Compensating Controls
Impacts, Costs, Industry Perspective
Future State Planning

Security Operations Center (SOC)

Cyber Threat Intelligence (CTI)

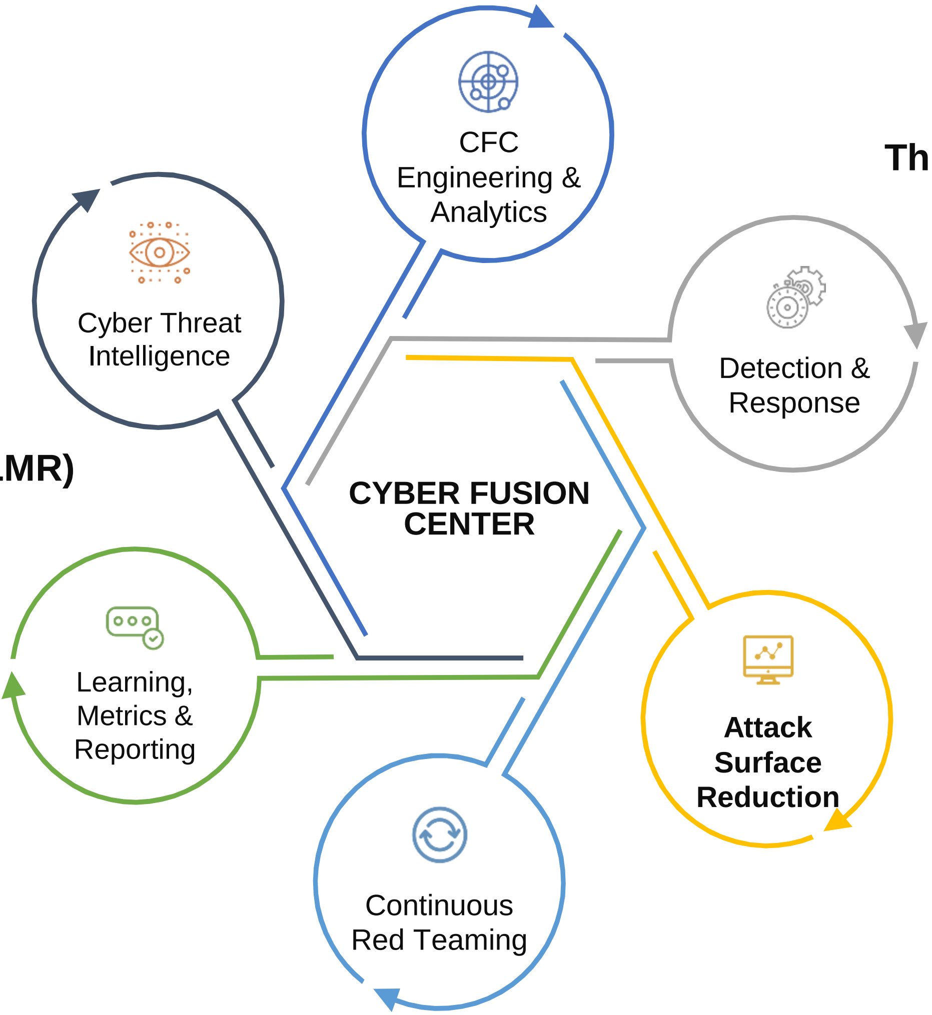
Collect and analyze data on cyber threat landscape to drive informed, risk-based decision-making. Conduct hunt activities.

Learning, Metrics & Reporting (LMR)

Define metrics and develop reports. Collaborate and communicate with internal and external audiences.

Continuous Red Teaming (CRT)

Execute threat-based scenarios and incorporate lessons learned into capabilities.



Threat Detection Operations (TDO)

Identify, onboard, and maintain visibility of security tools, develop threat-centric content, and perform data analytics.

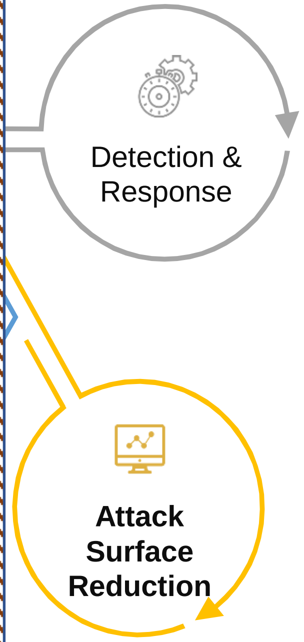
Incident Detection & Response (IR)

Provide security event monitoring, triage analysis, incident handling, remediation actions, and forensic support.

Attack Surface Reduction (ASR)

- **Manage remediation strategy for vulnerabilities**
- **Insights into high value systems**
- **Identify risk mitigation opportunities via monitoring.**

ASR exists as one of the key pillars of the CFC, continuing the loop on how information is distributed, shared, and actioned upon in a fully mature Security Operations Center (SOC)



Threat Detection Operations (TDO)

Identify, onboard, and maintain visibility of security tools, develop threat-centric content, and perform data analytics.

Incident Detection & Response (IR)

Provide security event monitoring, triage analysis, incident handling, remediation actions, and forensic support.

Attack Surface Reduction (ASR)

- **Manage remediation strategy for vulnerabilities**
- **Insights into high value systems**
- **Identify risk mitigation opportunities via monitoring.**

CFC Operating Model

Remediation & Handling done by On-Site CFC Resources

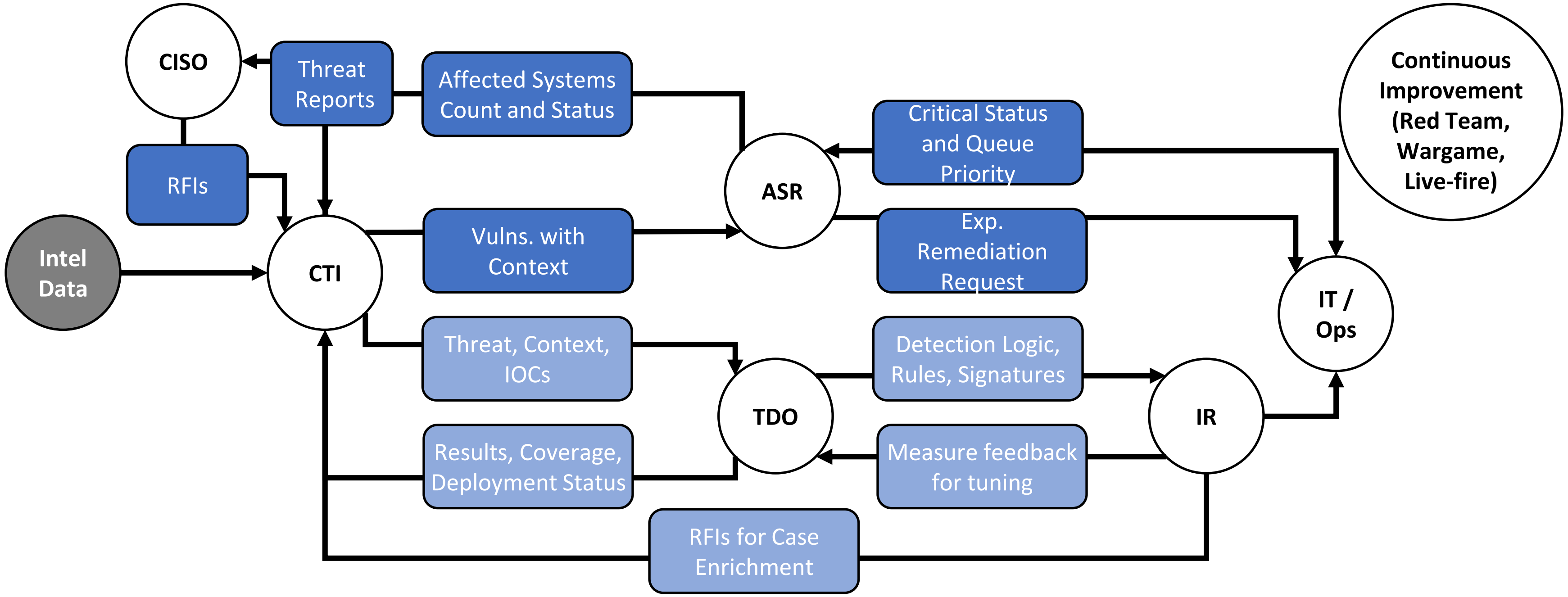
	Cyber Threat Intelligence	Threat Defense Operations	Incident Response		Attack Surface Reduction		Red Team	Learning, Metrics & Resolution
Core Functions	Data Feed / IOC Management	Content Development	Event Analysis	Triage Analysis	Vulnerability Analysis	GPS ASR	Red Teaming	Resolution
	Technical Intel	Control Engineers	Incident Handlers	Threat Remediation	Vulnerability Scanning	Remediation	War Gaming	CFC Metrics
	Strategic Intel	Hunt	Digital Forensics	Major Incident Crisis Action Plan			Penetration Testing	Process Improvement
Inputs/ Outputs	Analyst vetted IOCs	Alert / Detection Logic	SIEM	Host Forensics	Findings	Celebrity Vuln. Tracking	Findings	Resolution Tracking
	Actionable Intel Reports	Hunt Analytics / Findings	Case Management	Playbooks	Asset Management	Prioritize Remediation	Cyber Sims/LFX	Third Party Scoring
	Threat Intel Platform (TIP)	Control / Security Tool Updates	Investigations				Tabletop Exercises	Dashboards
Key Objectives	Actionable Intelligence	Adaptive Cyber Defense	Threat/Risk-Prioritized Response		Critical Vuln. Tracking	Reduced Attack Surface	Cyber Readiness	Continuous Improvement
Supporting Functions	SOAR (Automation and Orchestration) Security Engineering – Existing Tool Functionality / New Tool Integration							
	Other Stakeholder Functions - IdAM, Network Security, Infrastructure, Messaging, etc.							
	3rd Party Operational Support Teams							

Legend

Off-Site CFC	On-Site CFC	Future Capability	Service Providers

Intelligence is collected from CTI and IT Operations to profile the infrastructure, determine threat exposure, and make risk-informed decisions on remediation

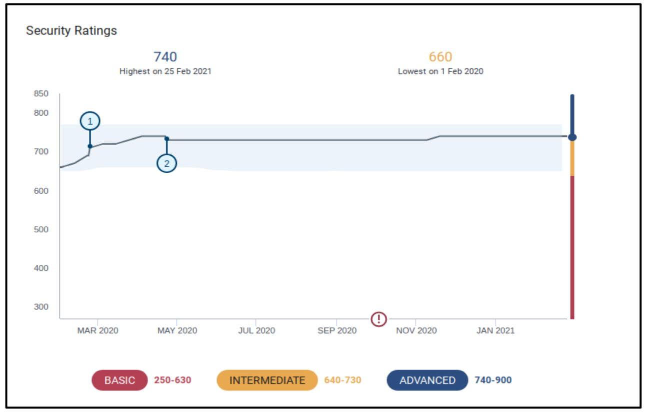
Threat Intel Drives Proactive Cyber Security Measures


CISO
Threat Reports
Affected Systems Count and Status
RFIs
Intel Data
CTI
Vulns. with Context
ASR
Critical Status and Queue Priority
Exp. Remediation Request
Continuous Improvement (Red Team, Wargame, Live-fire)
IT / Ops
Threat, Context, IOCs
TDO
Detection Logic, Rules, Signatures
IR
Results, Coverage, Deployment Status
Measure feedback for tuning
RFIs for Case Enrichment

Sample from CFC Playbook

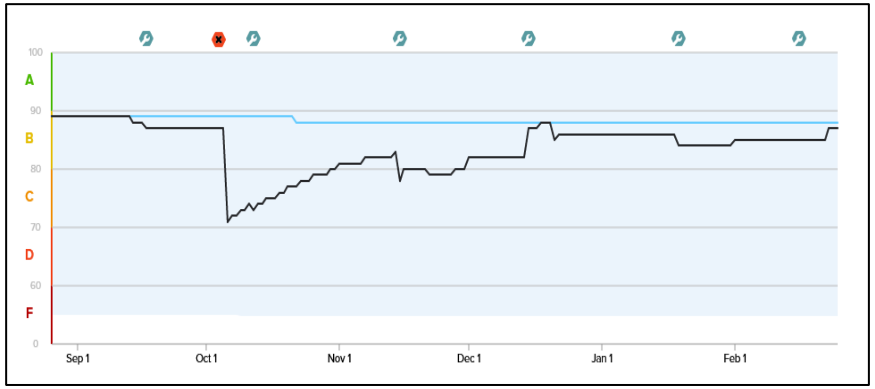
		CTI	TDO	ASR
Vulnerability Intel Received	“New Vulnerability Discovered in SolarWinds Orion”	▪ **IDENTIFY** latest TTPs relevant to client sector	▪ **CONDUCT** retrospective searching for IOCs ▪ **EXECUTE** Hunt sweeps (low counts, *new*, *changes*)	▪ **ASSESS** for org. exposure ▪ **EXPEDITE** patching – issue CSIRT as necessary ▪ **MONITOR** remediation effort

BITSIGHT



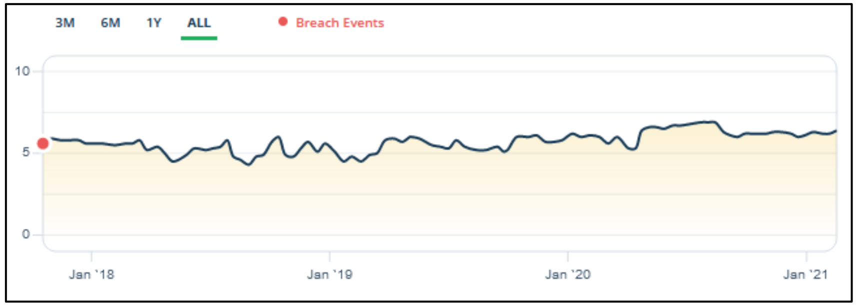
660 -> 740

SecurityScorecard



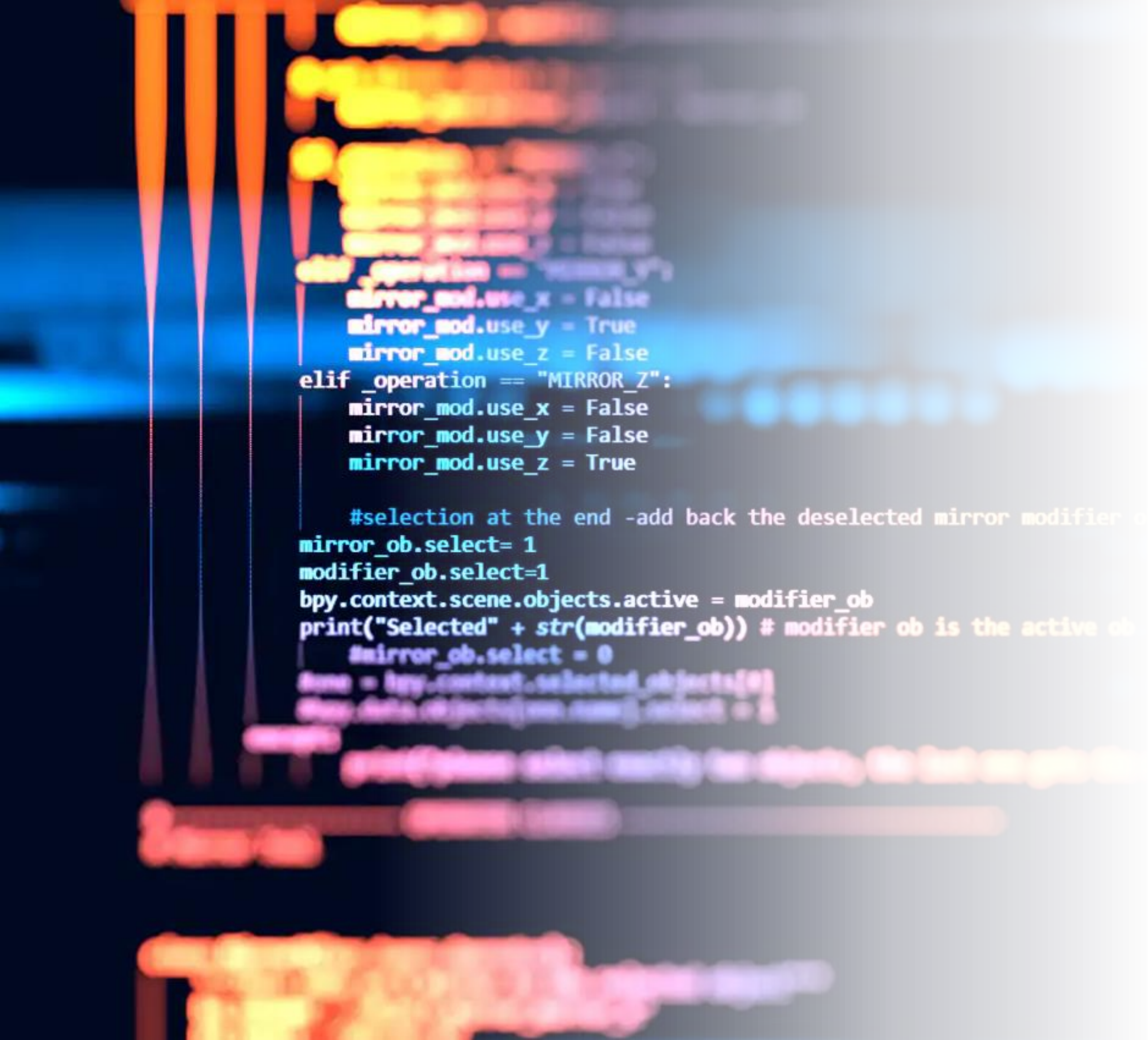
89 -> 87 *

riskrecon™



5.8 -> 6.4

- 3rd party platforms identify findings that indicate security risks to our business. These findings are prioritized based on severity and system owners are contacted and requested to remediate based on SLAs in the 3rd party SOP.



```
elif _operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active
    #mirror_ob.select = 0
```

Small Business Focus

- Have the right philosophy
- Core Pillars
- Malware Threats
- Ransomware Attacks
- Privileged Access Management
- Password Management
- Attack Surface Reduction
- Threat Protection
- Strategy & Action Plan

Core Pillars

Balance Cyber Interests and Support Business Strategy

How to enable the business while representing cyber up to senior management

Administrative Controls

Common sense approach to acceptable usage policies and

Computer Hardening

Common sense practices and configurations that reduces your attack surface thus lowering risk

Attack Surface Reduction (ASR)

Threat Protection

Technical security analysis and defense through solutions and tools in "Defense in Depth" methodology

Approach Considerations

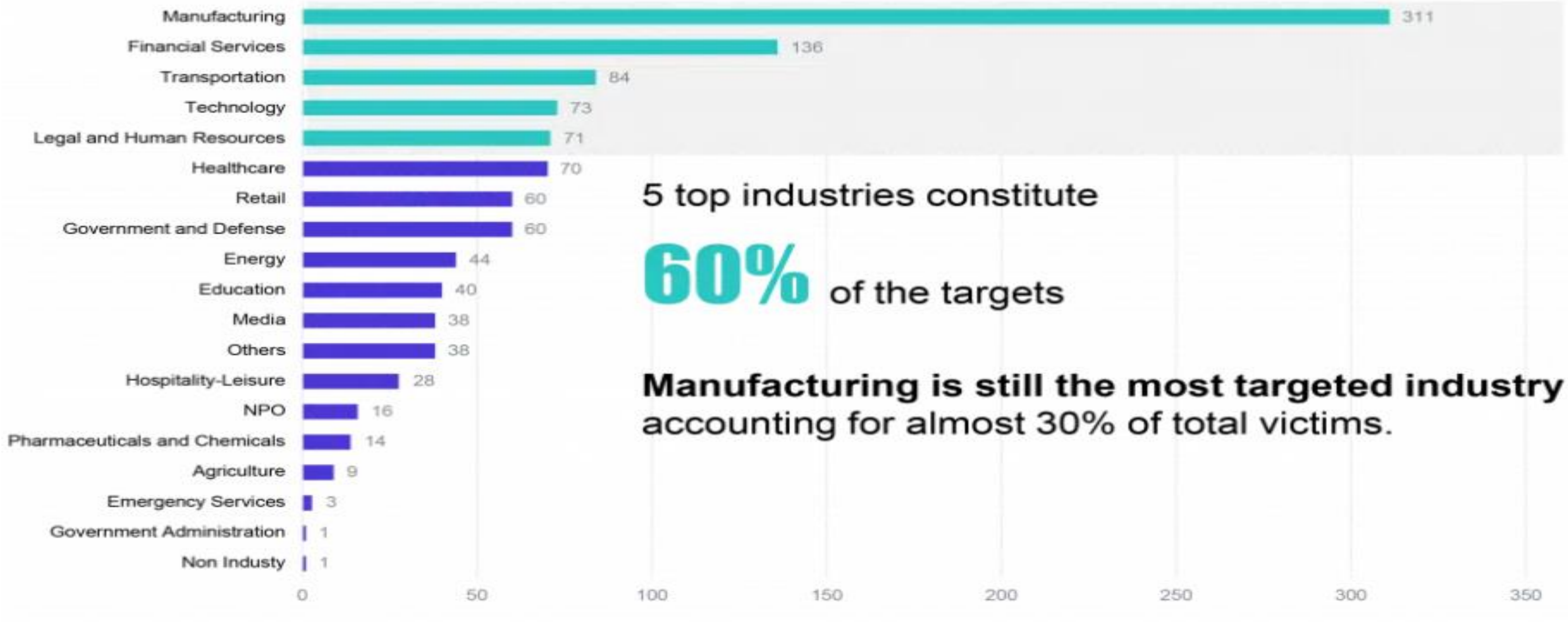
People

Process

Technology

Threat Intelligence

https://www.cognyte.com/blog/ransomware_2021/

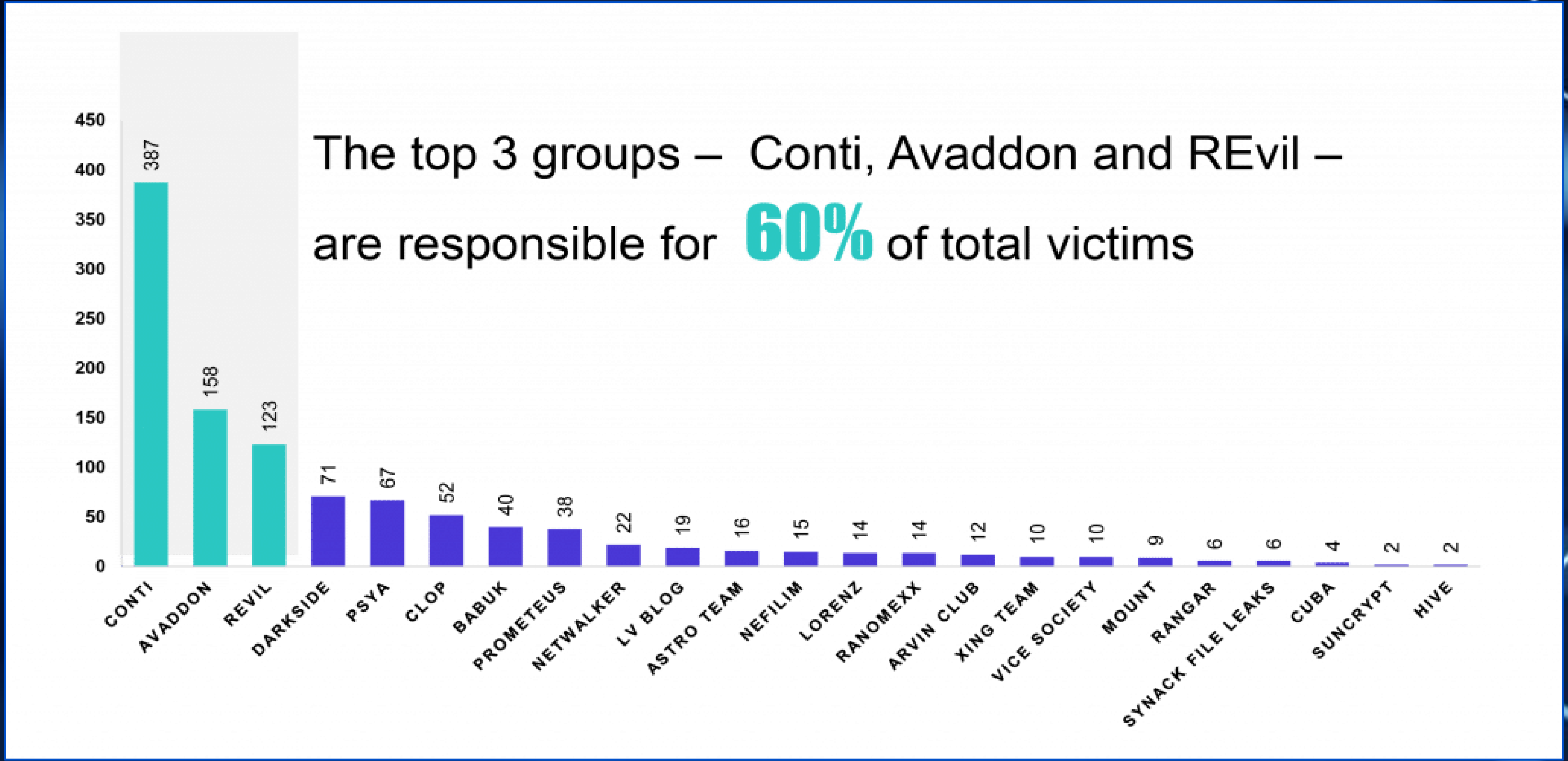


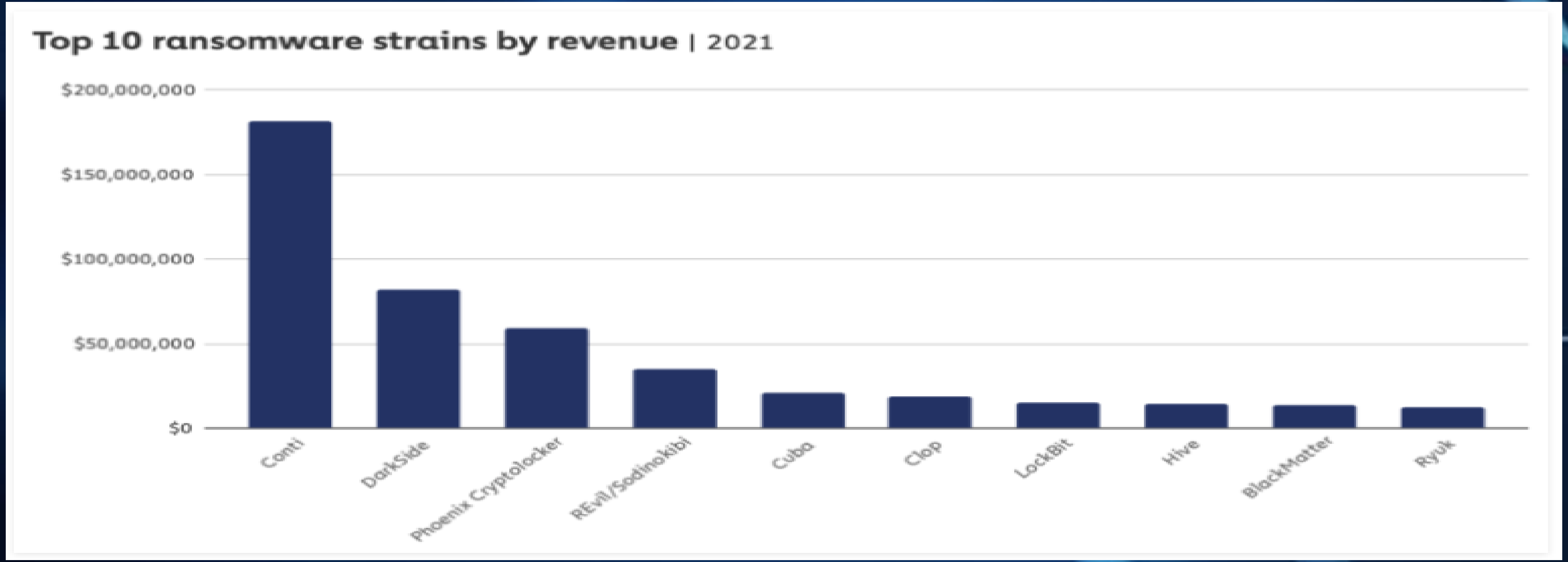
5 top industries constitute

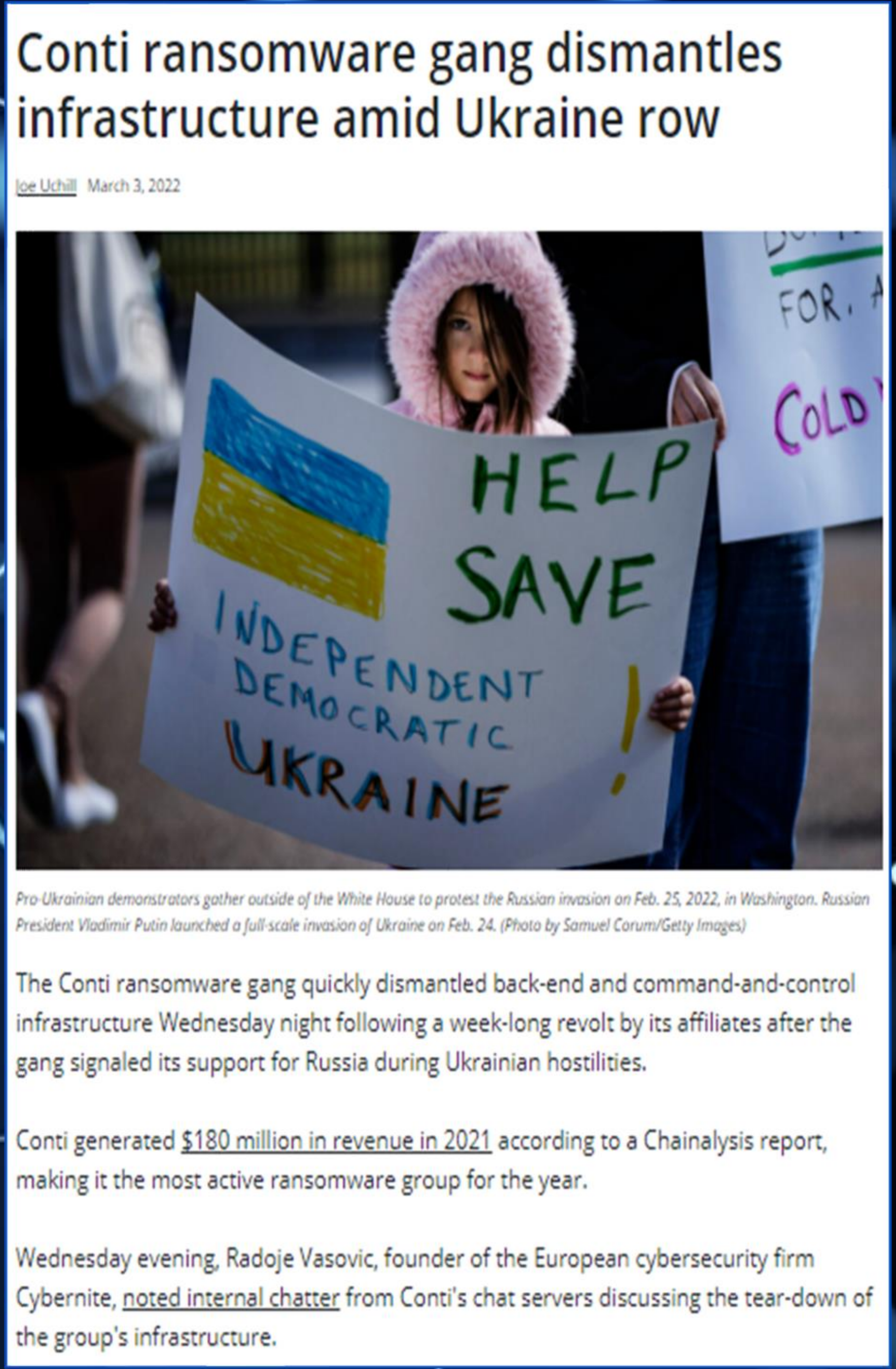
60% of the targets

Manufacturing is still the most targeted industry accounting for almost 30% of total victims.

Most targeted industries


The top 3 groups – Conti, Avaddon and REvil – are responsible for **60%** of total victims


Top 10 ransomware strains by revenue | 2021


Conti ransomware gang dismantles infrastructure amid Ukraine row

Joe Uchill March 3, 2022

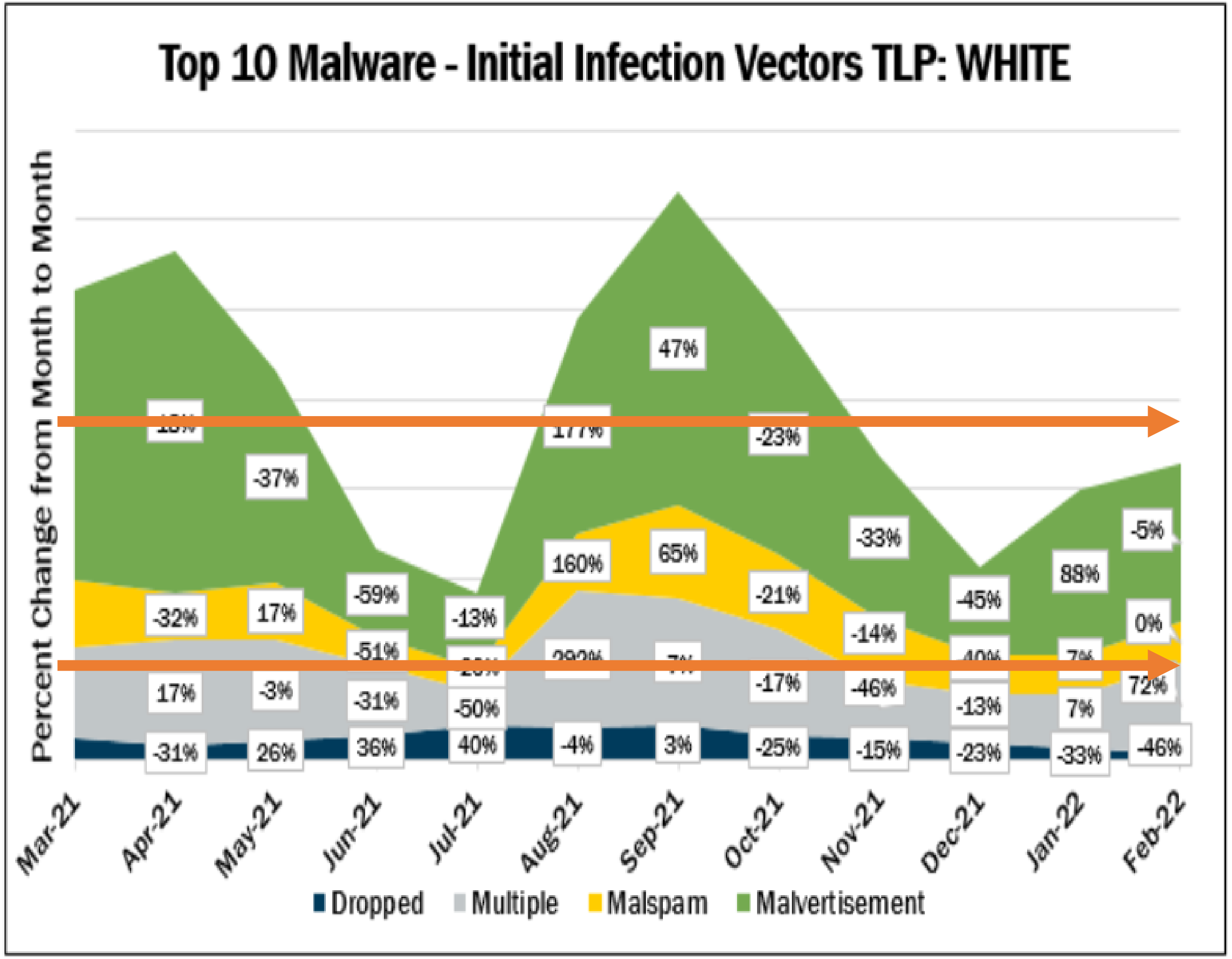
Pro-Ukrainian demonstrators gather outside of the White House to protest the Russian invasion on Feb. 25, 2022, in Washington. Russian President Vladimir Putin launched a full-scale invasion of Ukraine on Feb. 24. (Photo by Samuel Corum/Getty Images)

The Conti ransomware gang quickly dismantled back-end and command-and-control infrastructure Wednesday night following a week-long revolt by its affiliates after the gang signaled its support for Russia during Ukrainian hostilities.

Conti generated $180 million in revenue in 2021 according to a Chainalysis report, making it the most active ransomware group for the year.

Wednesday evening, Radoje Vasovic, founder of the European cybersecurity firm Cybernite, noted internal chatter from Conti's chat servers discussing the tear-down of the group's infrastructure.

CIS Center for Internet Security®



Top 10 Malware - Initial Infection Vectors TLP: WHITE

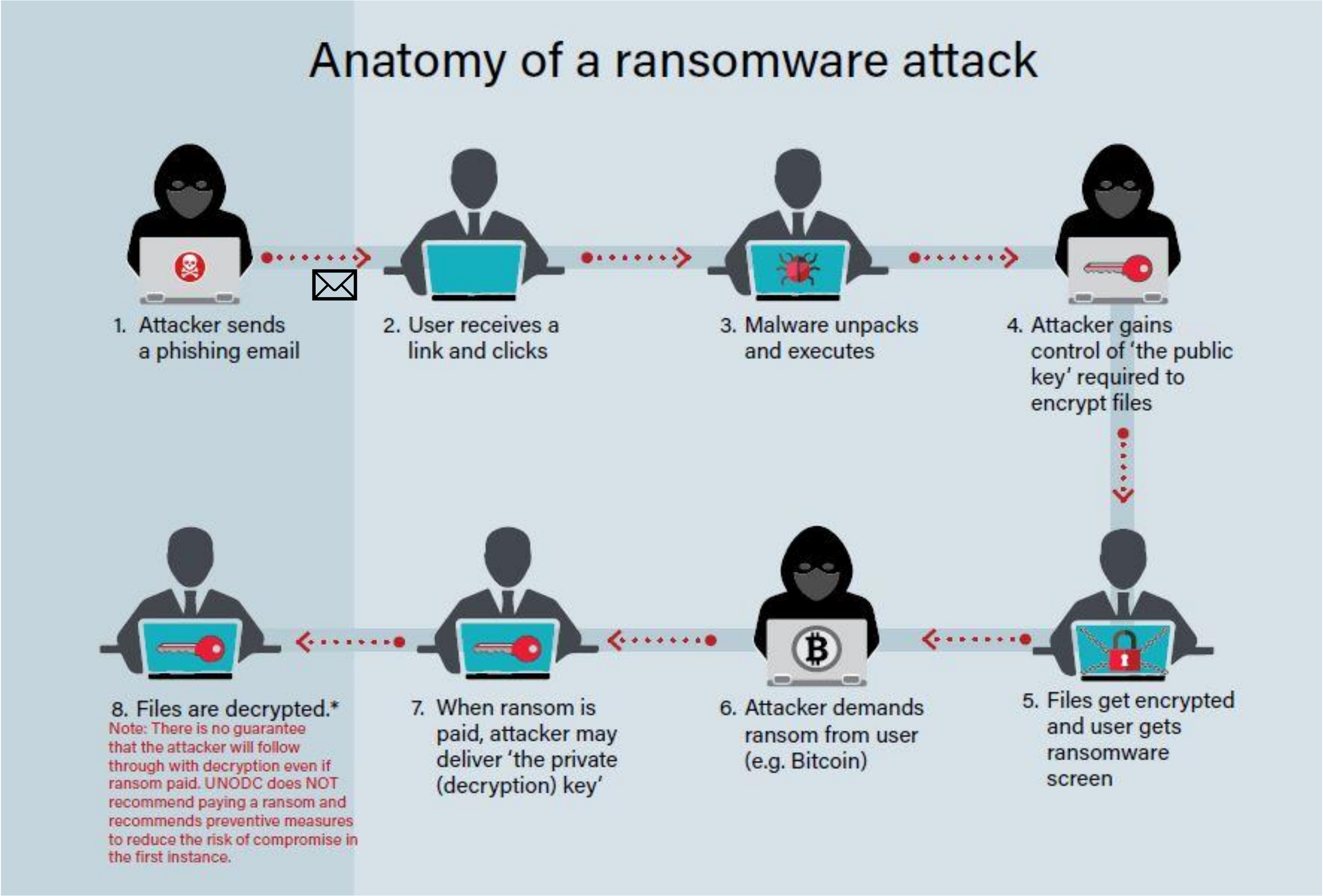
Legend	
Malvertisement	Malware introduced through malicious advertisements. Currently, Shlayer is the only Top 10 Malware using this technique.
Malspam	Unsolicited emails either direct users to malicious web sites or trick users into downloading or opening malware. Top 10 Malware using this technique include Agent Tesla and NanoCore.
Multiple	Malware that currently favors at least two vectors. Currently, Arechclient2, CoinMiner, CryptoWall, Delf, RedLine, and ZeuS are the malware utilizing multiple vectors
Dropped	Malware delivered by other malware already on the system, an exploit kit, infected third-party software, or manually by a cyber threat actor. Currently, Mirai is the only malware using this technique.

Ransomware Attacks

https://www.sans.org/security-resources/

42 minutes** and 54 seconds: that's how quickly the median ransomware variant can encrypt and lock out a victim from **100,000 of their files

- *Splunk SURGe team*



Anatomy of a ransomware attack

1. Attacker sends a phishing email
2. User receives a link and clicks
3. Malware unpacks and executes
4. Attacker gains control of 'the public key' required to encrypt files
5. Files get encrypted and user gets ransomware screen
6. Attacker demands ransom from user (e.g. Bitcoin)
7. When ransom is paid, attacker may deliver 'the private (decryption) key'
8. Files are decrypted.*

Note: There is no guarantee that the attacker will follow through with decryption even if ransom paid. UNODC does NOT recommend paying a ransom and recommends preventive measures to reduce the risk of compromise in the first instance.

10 biggest ransomware strains

Lockbit, REvil, Blackmatter, Conti, Ryuk, Avaddon, Babuk, Darkside, Maize, and Mespinoza

— could encrypt 100,000 files consisting of some 53.93 gigabytes of data

Fastest Spreader

Lockbit won the race

- speeds of **86%** faster than the median
- One Lockbit sample was clocked at encrypting **25,000 files per minute**

Ransomware Attacks

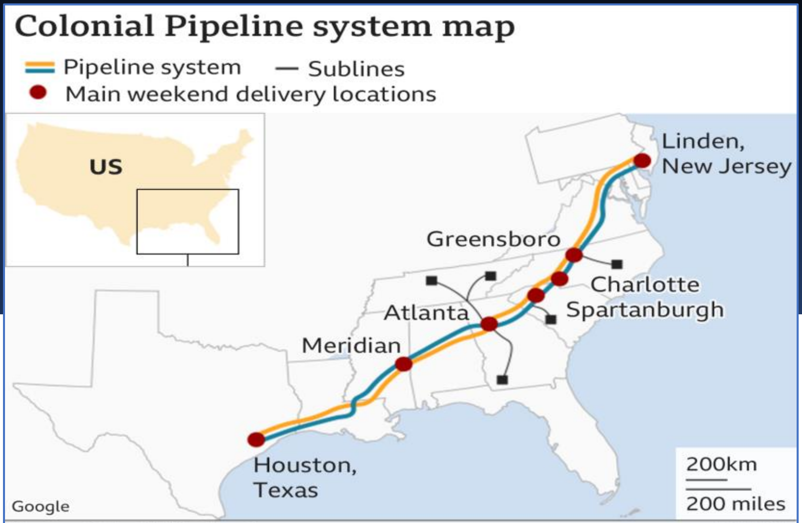
Colonial Pipeline

This event was arguably the most high-profile ransomware attack of 2021. Colonial Pipeline is responsible for transporting nearly half of the East Coast’s fuel. The ransomware attack was the largest cyberattack to target an oil infrastructure in the United States’ history.

- On May 7, the **DarkSide** group deployed **ransomware** on the organization’s computerized equipment that manages the pipeline.
- Colonial Pipeline’s CEO revealed DarkSide’s attack vector as **a single compromised password** to an active VPN account that was no longer in use.
- Since Colonial Pipeline **didn’t use multi-factor authentication**, the attackers were more easily

TOP 10 Protection Practices

1. **Prompt Systems Upgrades & Patching**
2. **Implement the 3-2-1-1 Backup Rule**
3. **Implement the Zero-Trust Model**
4. **Network Segmentation**
5. **Endpoint Visibility**
6. **Rapid Eradication & Recovery**
7. **Immutable and Indelible Storage**
8. **Regular Testing and Validation**
9. **Educated Employees**
10. **Cyberattack Playbooks**



Cheat sheets & Posters

https://www.sans.org/security-resources

Examples of privileged access used by humans:

Super user account: A powerful account used by IT system administrators that can be used to make configurations to a system or application, add or remove users or delete data.

Domain administrative account: An account providing privileged administrative access across all workstations and servers within a network domain. The phrase "Keys to the IT Kingdom" is often used when referring to the privileged nature of some administrator accounts and systems.

Local administrative account: This account is located on an endpoint or workstation and uses a combination of a username and password. It helps people access and make changes to their local machines or devices.

Secure socket shell (SSH) key: SSH keys are heavily used access control protocols that provide direct root access to critical systems. Root is the username or account that, by default, has access to all commands and files on a Linux or other Unix-like operating system.

Emergency account: This account provides users with administrative access to secure systems in the case of an emergency. It is sometimes referred to as firecall or break glass account.

Privileged business user: Is someone who works outside of IT, but has access to sensitive systems. This could include someone who needs access to finance, human resources (HR) or marketing systems.

non-human privileged access:

Application account: A privileged account that's specific to the application software and is typically used to administer, configure or manage access to the application software

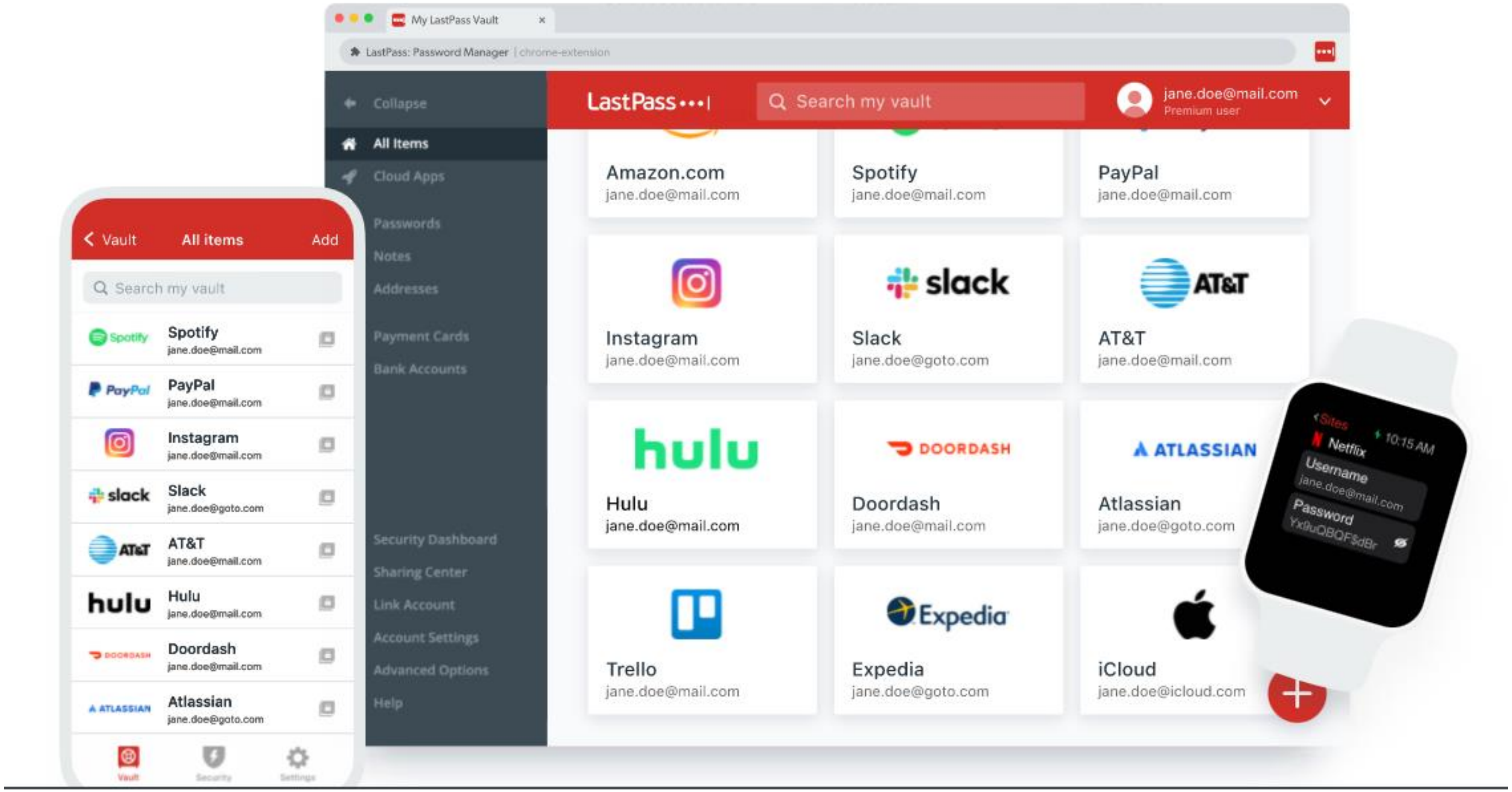
Service account: An account that an application or service uses to interact with the operating system. Services use these accounts to access and make changes to the operating system or the configuration

CYBERARK

BeyondTrust

Password Management

https://www.lastpass.com/

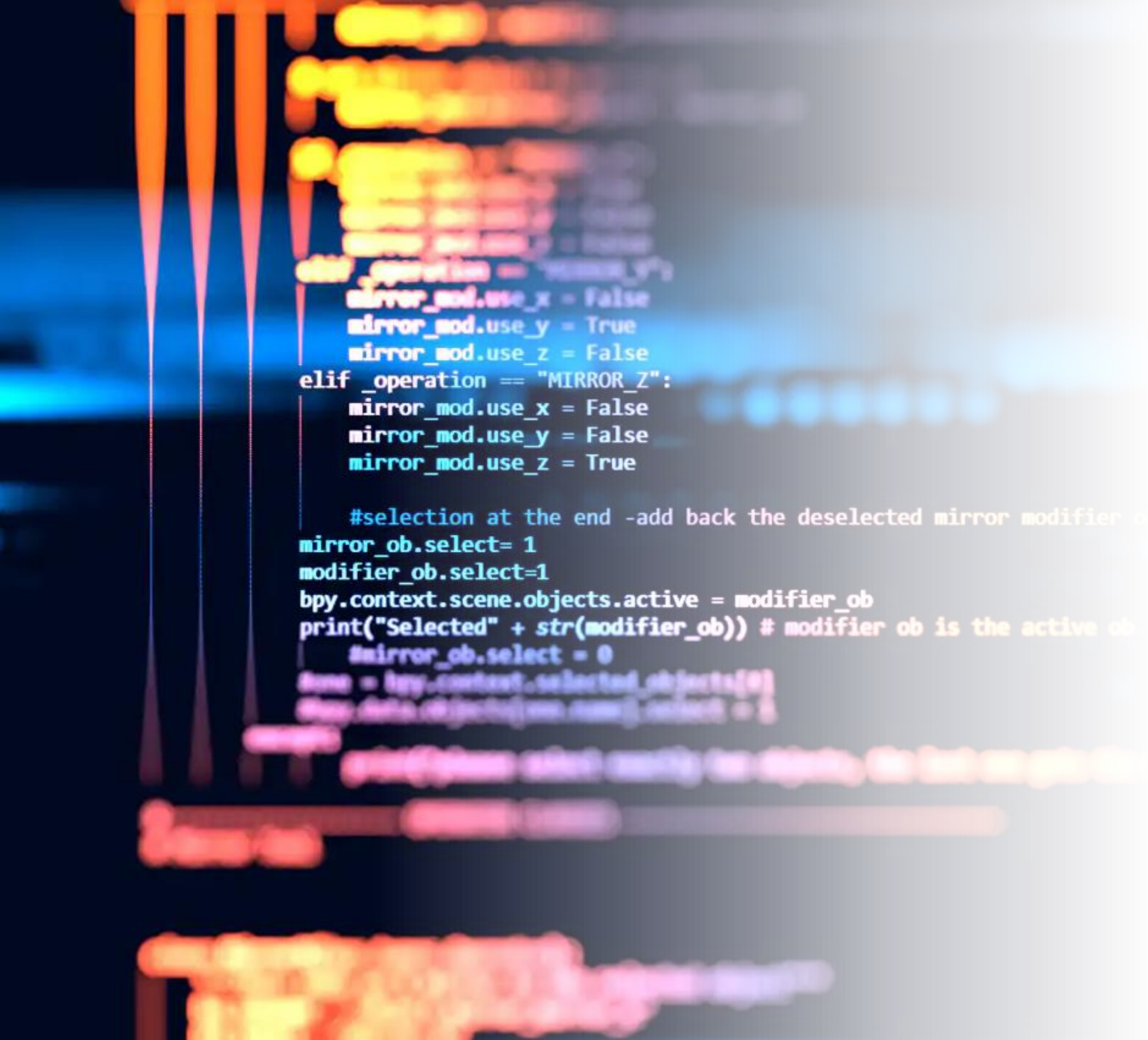


Simplify password management and protect your identity while online.

Remember fewer passwords, log in faster, and increase your online security. An encrypted, safe location for all your passwords, notes, files, and more. Save new accounts while on-the-go and fill passwords & forms with one click.

Attack Surface Reduction

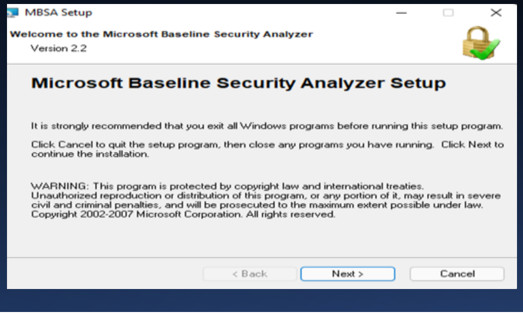
- Have the right philosophy
- Start with baselining security configuration of internals hosts
- Implement vulnerability management program
- Keep up with patching and retire older systems



```
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

Microsoft Baseline Security Analyzer 2.2



Welcome to the Microsoft Baseline Security Analyzer

Version 2.2

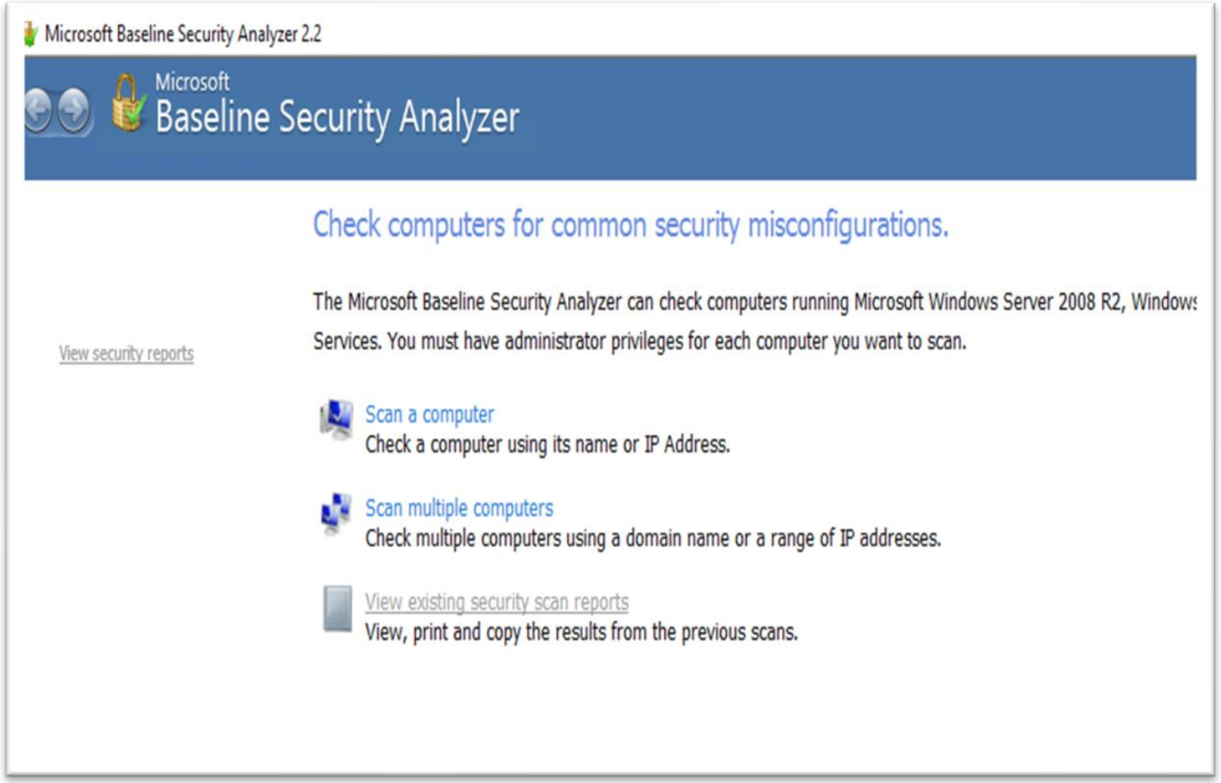
Microsoft Baseline Security Analyzer Setup

It is strongly recommended that you exit all Windows programs before running this setup program.

Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law. Copyright 2002-2007 Microsoft Corporation. All rights reserved.

- ❑ Scan your localhost and the default desktop image
- ❑ Using Administrator credentials to scan other hosts in your network
- ❑ Consider and test advanced features and settings
- ❑ Schedule periodic re-testing to prevent security drift
- ❑ Develop action plan to remediate


Microsoft Baseline Security Analyzer 2.2
Microsoft
Baseline Security Analyzer
View security reports

Check computers for common security misconfigurations.

The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2008 R2, Windows Services. You must have administrator privileges for each computer you want to scan.

Scan a computer

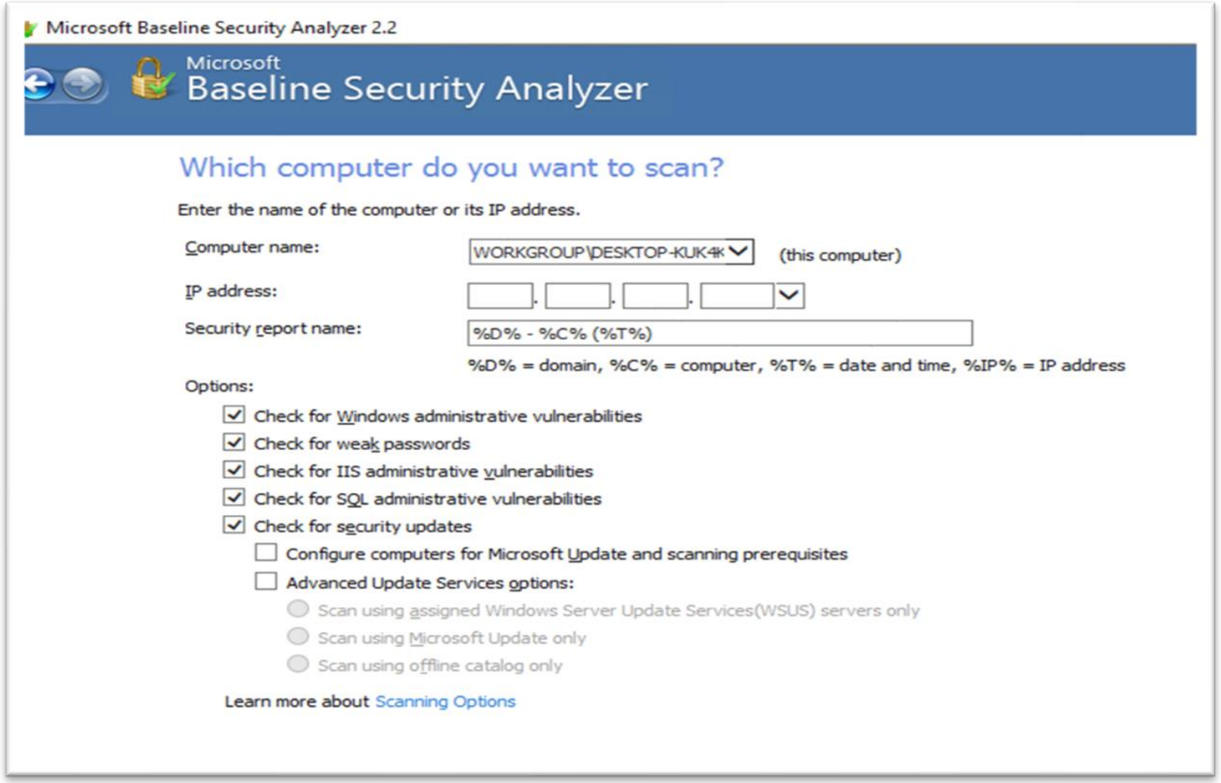
Check a computer using its name or IP Address.

Scan multiple computers

Check multiple computers using a domain name or a range of IP addresses.

View existing security scan reports

View, print and copy the results from the previous scans.


Microsoft Baseline Security Analyzer 2.2
Microsoft
Baseline Security Analyzer

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name: WORKGROUP\DESKTOP-KUK4K (this computer)

IP address: . . .

Security report name: %D% - %C% (%T%)

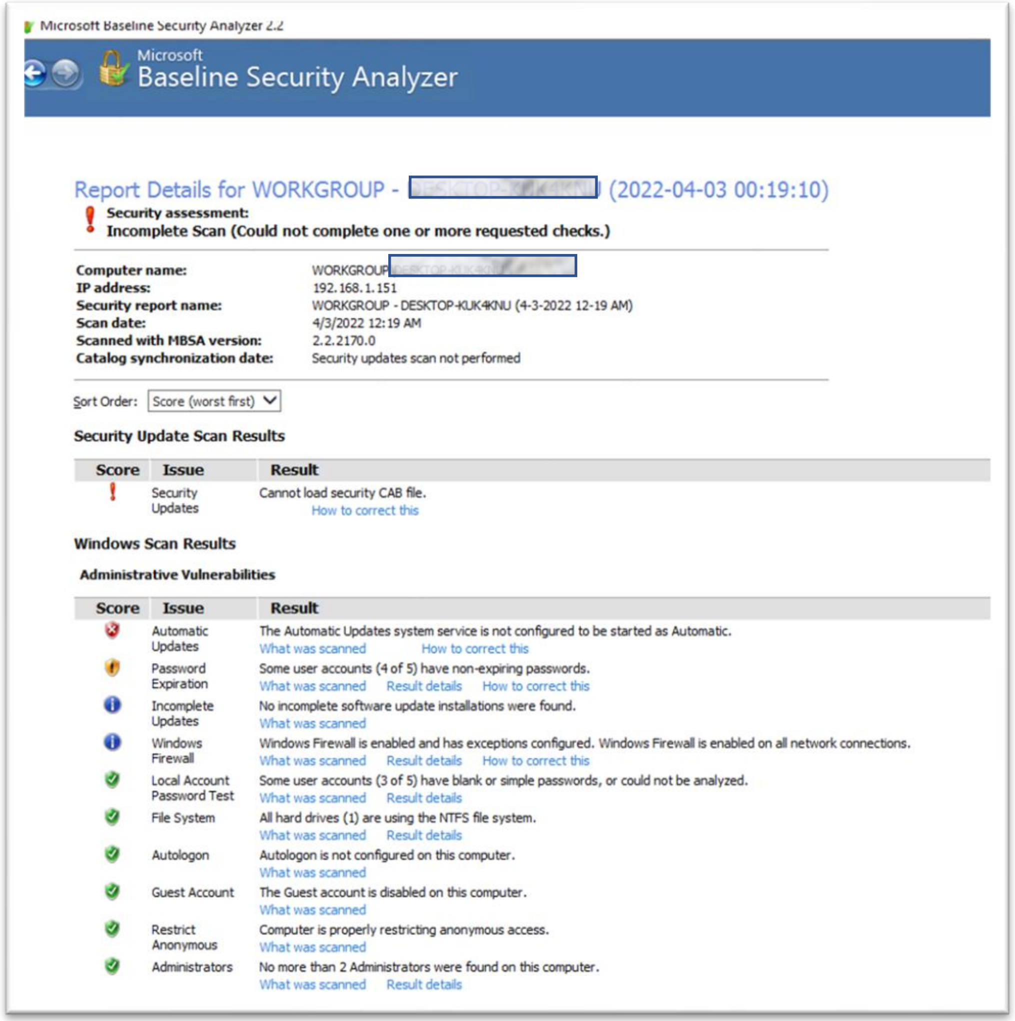
%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

- ☑ Check for Windows administrative vulnerabilities
- ☑ Check for weak passwords
- ☑ Check for IIS administrative vulnerabilities
- ☑ Check for SQL administrative vulnerabilities
- ☑ Check for security updates
  - □ Configure computers for Microsoft Update and scanning prerequisites
  - □ Advanced Update Services options:
    - ○ Scan using assigned Windows Server Update Services(WSUS) servers only
    - ○ Scan using Microsoft Update only
    - ○ Scan using offline catalog only

Learn more about Scanning Options

MBSA Output



Microsoft Baseline Security Analyzer 2.2

Report Details for WORKGROUP - [redacted] (2022-04-03 00:19:10)

! **Security assessment:**
Incomplete Scan (Could not complete one or more requested checks.)

Computer name:	WORKGROUP[redacted]
IP address:	192.168.1.151
Security report name:	WORKGROUP - DESKTOP-KUK4KNU (4-3-2022 12-19 AM)
Scan date:	4/3/2022 12:19 AM
Scanned with MBSA version:	2.2.2170.0
Catalog synchronization date:	Security updates scan not performed

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot load security CAB file. How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
☒	Automatic Updates	The Automatic Updates system service is not configured to be started as Automatic. What was scanned How to correct this
!	Password Expiration	Some user accounts (4 of 5) have non-expiring passwords. What was scanned Result details How to correct this
ℹ	Incomplete Updates	No incomplete software update installations were found. What was scanned
ℹ	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections. What was scanned Result details How to correct this
✓	Local Account Password Test	Some user accounts (3 of 5) have blank or simple passwords, or could not be analyzed. What was scanned Result details
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
✓	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details

- ❑ Analyze and address findings & recommendations
- ❑ Track remediation efforts across your environment
- ❑ Test application functionality post-changes
- ❑ Verify secure base configuration
- ❑ move to active vulnerability scans on all hosts

Vulnerability Management Solutions

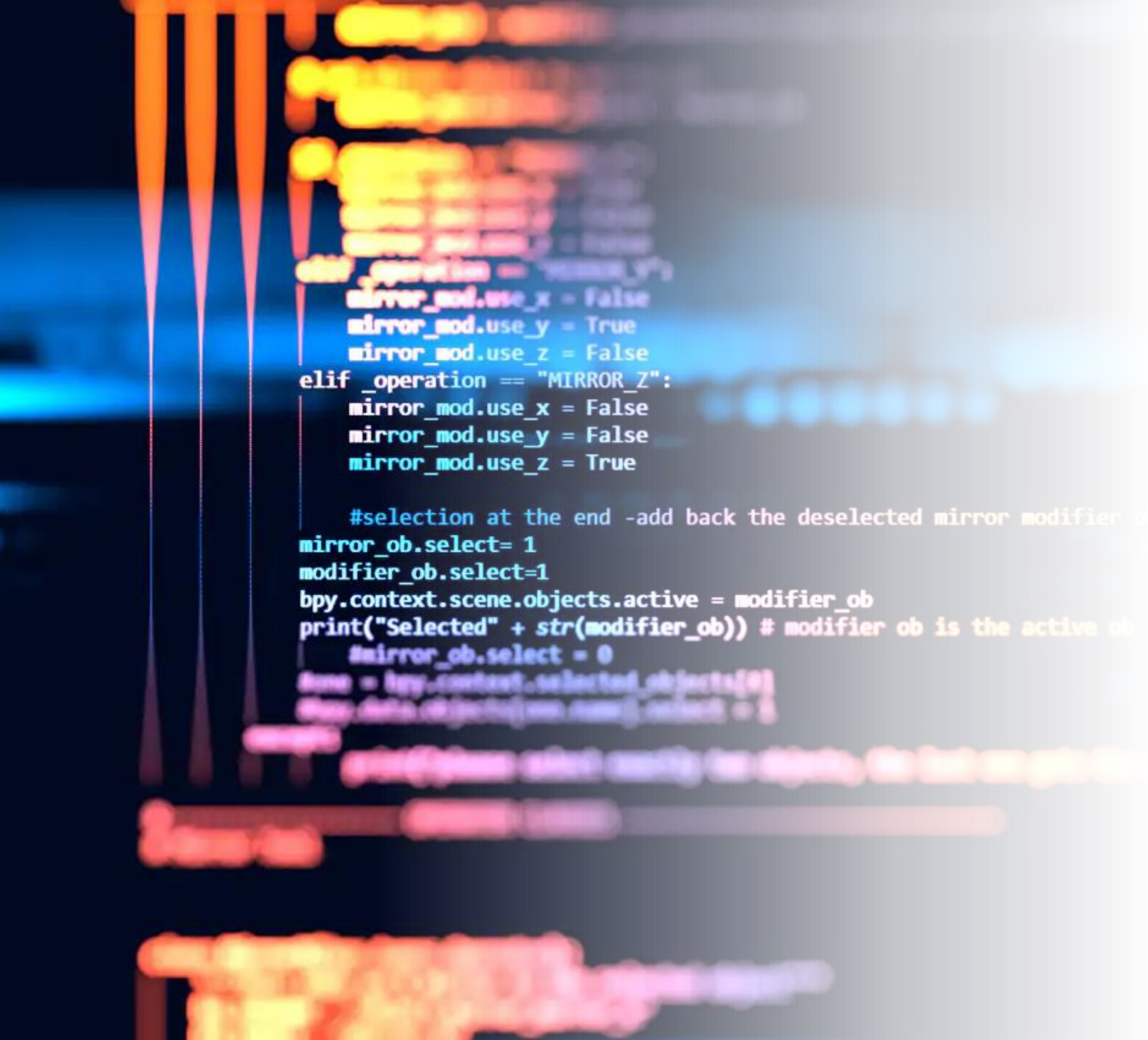
Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them

tenable | nessus professional

Booz | Allen | Hamilton

Qualys.

RAPID7



```
elif _operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier o
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

Threat Protection

Anti-malware solutions

- E-mail Gateways
- Endpoint Detection & Response (EDR) platforms
- Anti-malware analysis options

Strategic Approach

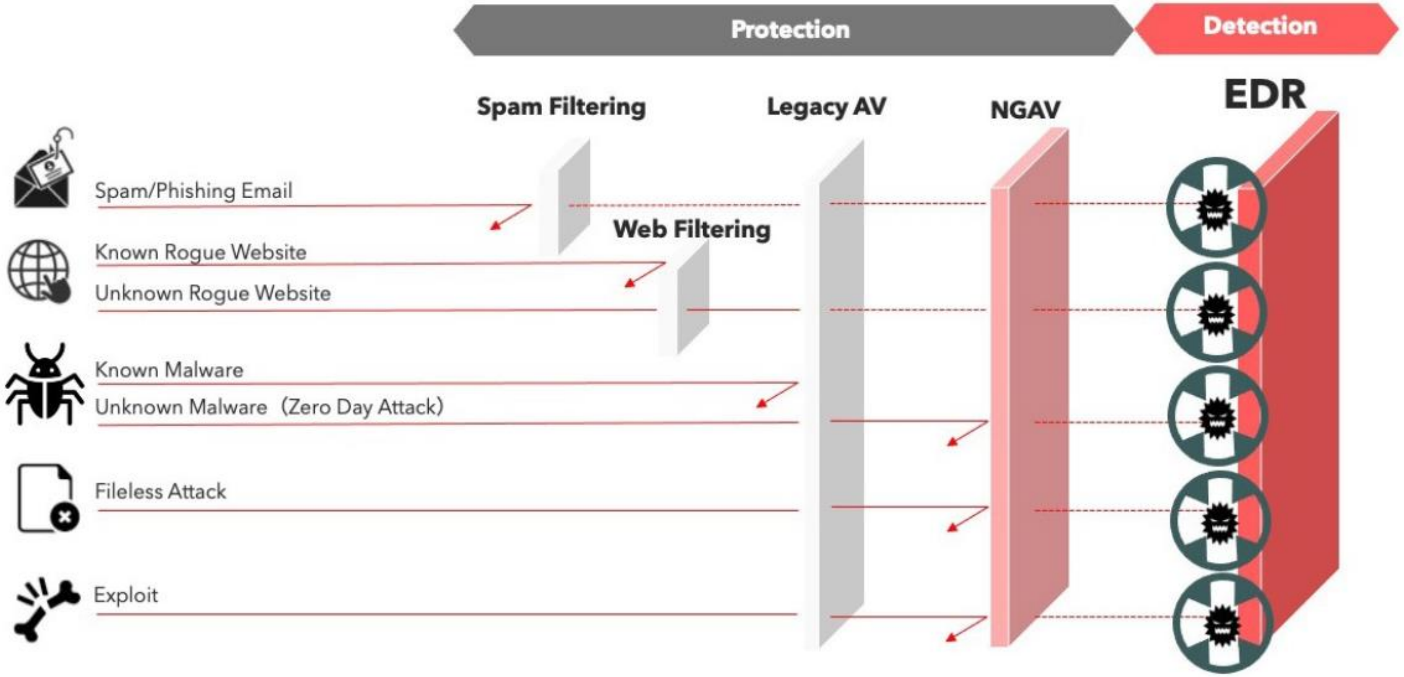
- Architecture
- Lockdown
- Threat Protection
- Corporate security transformation

Action Plan

- **Top 10 Best Practices**

EDR Analysis Overview

OPEN EDR



The Endpoint Detection and Response Solutions (EDR) market is defined as solutions that record and store endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system behavior

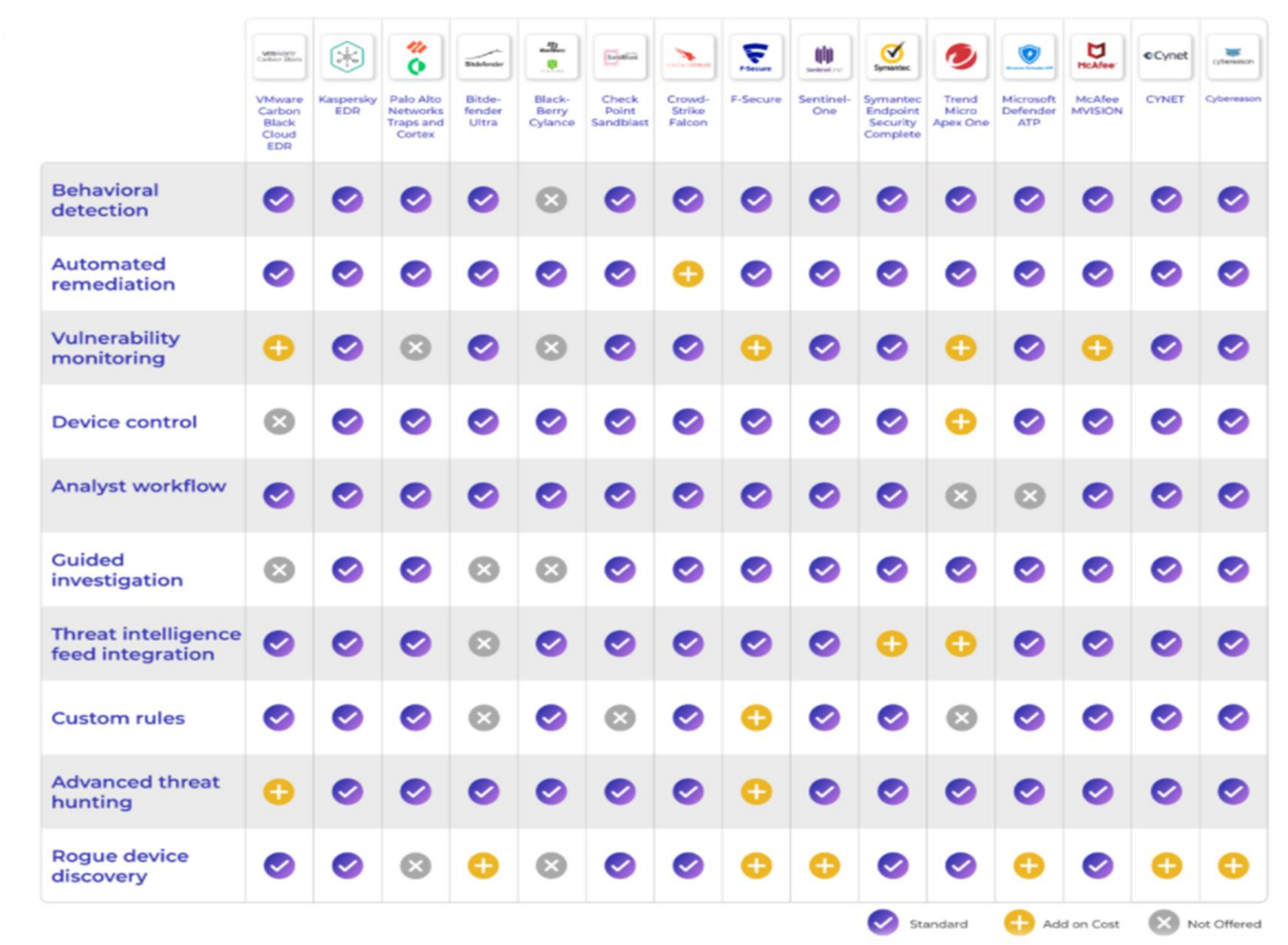
EDR solutions must provide the following four primary capabilities:

- **Detect security incidents**
- **Contain the incident at the endpoint**
- **Investigate security incidents**
- **Provide remediation guidance**

https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

EDR Analysis Overview

OPEN EDR



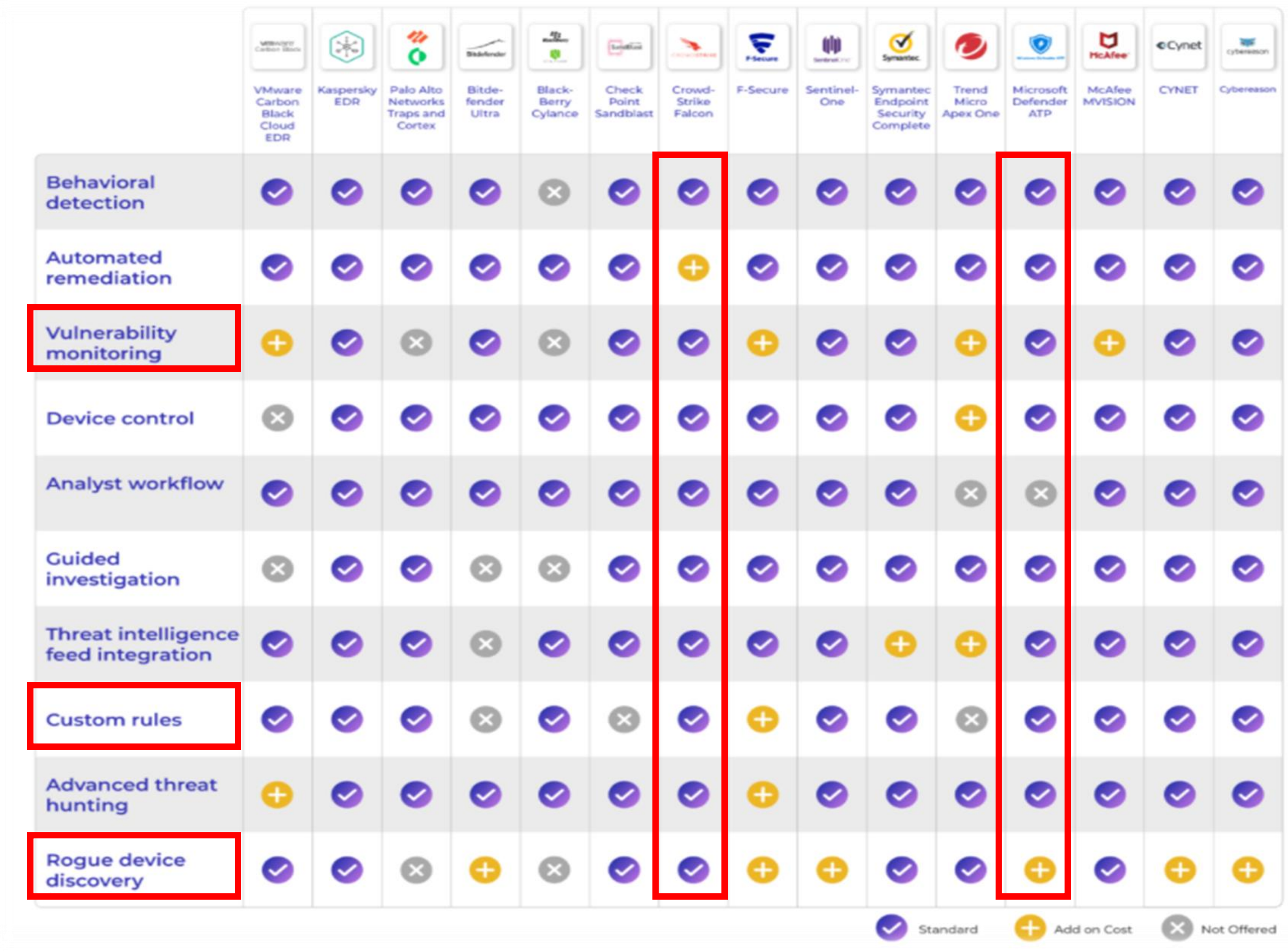
	VMware Carbon Black Cloud EDR	Kaspersky EDR	Palo Alto Networks Traps and Cortex	Bitdefender Ultra	BlackBerry Cylance	Check Point Sandblast	CrowdStrike Falcon	F-Secure	SentinelOne	Symantec Endpoint Security Complete	Trend Micro Apex One	Microsoft Defender ATP	McAfee MVISION	CYNET	Cybereason
Behavioral detection	✓	✓	✓	✓	⊗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Automated remediation	✓	✓	✓	✓	✓	✓	⊕	✓	✓	✓	✓	✓	✓	✓	✓
Vulnerability monitoring	⊕	✓	⊗	✓	⊗	✓	✓	⊕	✓	✓	⊕	✓	⊕	✓	✓
Device control	⊗	✓	✓	✓	✓	✓	✓	✓	✓	✓	⊕	✓	✓	✓	✓
Analyst workflow	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	⊗	⊗	✓	✓	✓
Guided investigation	⊗	✓	✓	⊗	⊗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Threat intelligence feed integration	✓	✓	✓	⊗	✓	✓	✓	✓	✓	⊕	⊕	✓	✓	✓	✓
Custom rules	✓	✓	✓	⊗	✓	⊗	✓	⊕	✓	✓	⊗	✓	✓	✓	✓
Advanced threat hunting	⊕	✓	✓	✓	✓	✓	✓	⊕	✓	✓	✓	✓	✓	✓	✓
Rogue device discovery	✓	✓	⊗	⊕	⊗	✓	✓	⊕	⊕	✓	✓	⊕	✓	⊕	⊕

✓ Standard ⊕ Add on Cost ⊗ Not Offered

https://www.esecurityplanet.com/?s=edr+solutions

EDR Analysis Overview

OPEN EDR



	VMware Carbon Black Cloud EDR	Kaspersky EDR	Palo Alto Networks Traps and Cortex	Bitdefender Ultra	BlackBerry Cylance	Check Point Sandblast	CrowdStrike Falcon	F-Secure	SentinelOne	Symantec Endpoint Security Complete	Trend Micro Apex One	Microsoft Defender ATP	McAfee MVISION	CYNET	Cybereason
Behavioral detection	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Automated remediation	✓	✓	✓	✓	✓	✓	+	✓	✓	✓	✓	✓	✓	✓	✓
Vulnerability monitoring	+	✓	✗	✓	✗	✓	✓	+	✓	✓	+	✓	+	✓	✓
Device control	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	+	✓	✓	✓	✓
Analyst workflow	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓
Guided investigation	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Threat intelligence feed integration	✓	✓	✓	✗	✓	✓	✓	✓	✓	+	+	✓	✓	✓	✓
Custom rules	✓	✓	✓	✗	✓	✗	✓	+	✓	✓	✗	✓	✓	✓	✓
Advanced threat hunting	+	✓	✓	✓	✓	✓	✓	+	✓	✓	✓	✓	✓	✓	✓
Rogue device discovery	✓	✓	✗	+	✗	✓	✓	+	+	✓	✓	+	✓	+	+

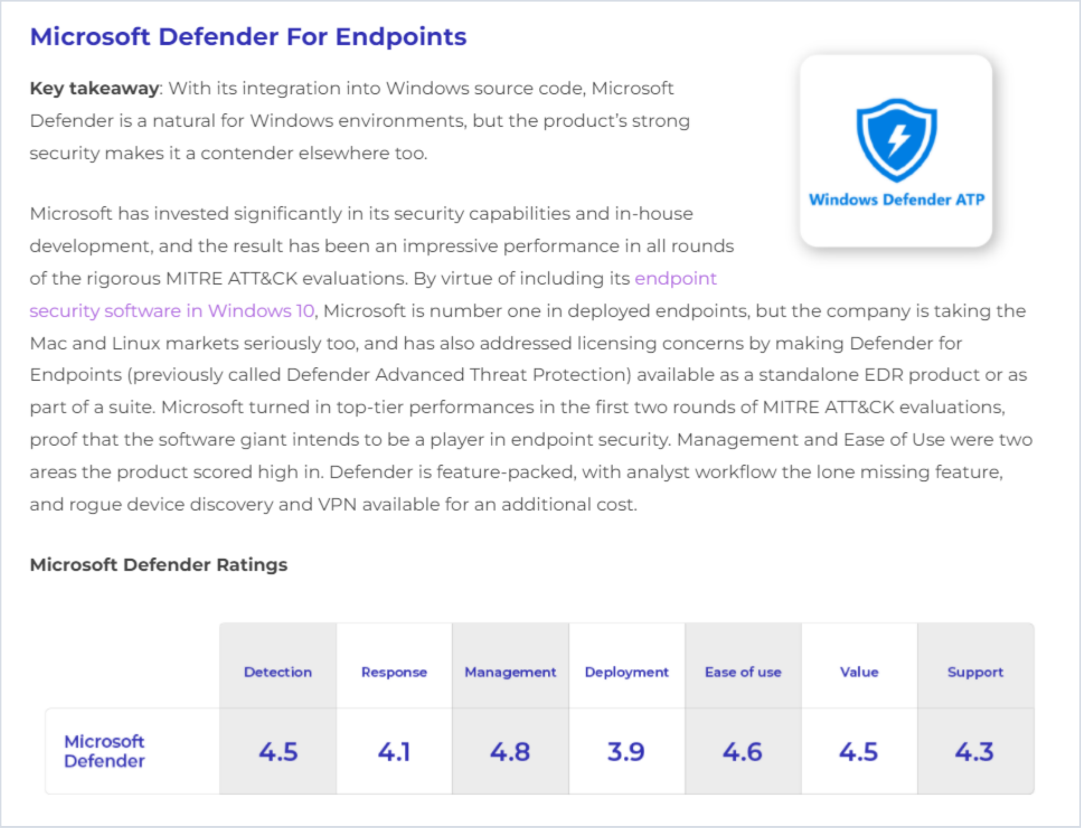
✓ Standard + Add on Cost ✗ Not Offered

https://www.esecurityplanet.com/?s=edr+solutions

Leading EDR

What is EDR tool?

Endpoint detection and response refers to **a category of tools used to detect and investigate threats on endpoints**. EDR tools typically provide detection, investigation, threat hunting, and response capabilities.



Microsoft Defender For Endpoints

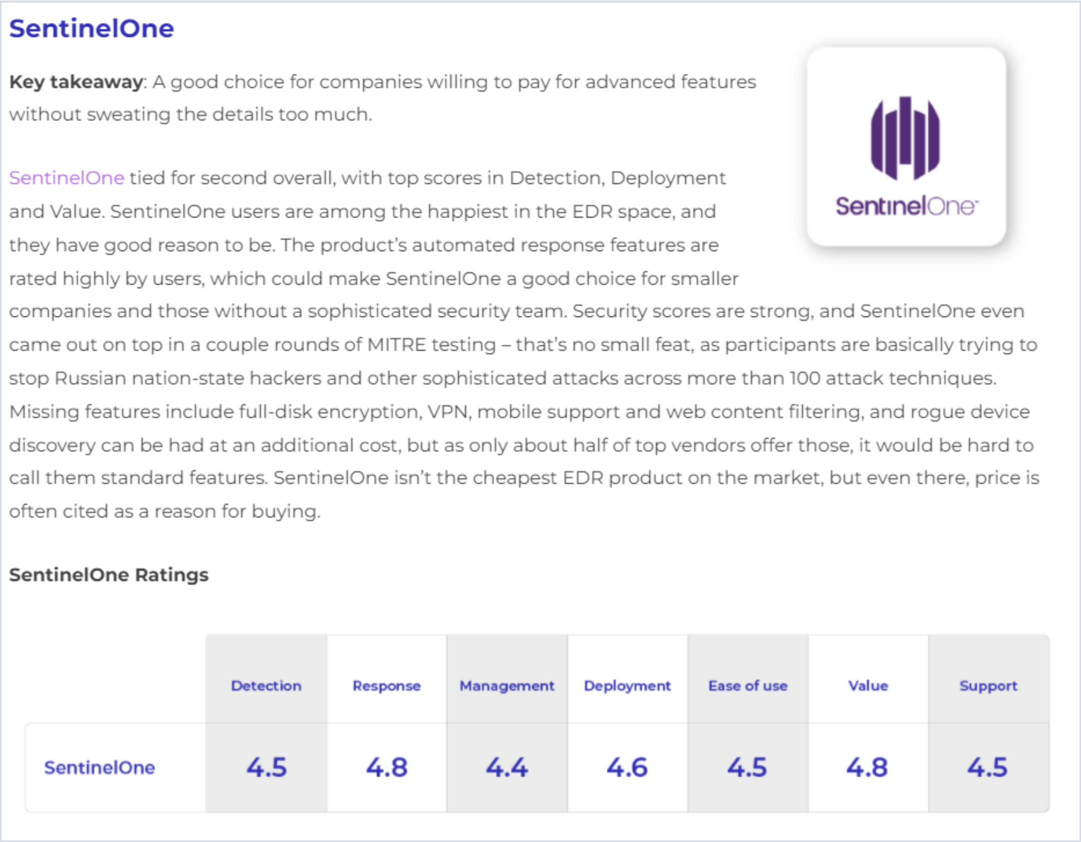
Windows Defender ATP

Key takeaway: With its integration into Windows source code, Microsoft Defender is a natural for Windows environments, but the product's strong security makes it a contender elsewhere too.

Microsoft has invested significantly in its security capabilities and in-house development, and the result has been an impressive performance in all rounds of the rigorous MITRE ATT&CK evaluations. By virtue of including its endpoint security software in Windows 10, Microsoft is number one in deployed endpoints, but the company is taking the Mac and Linux markets seriously too, and has also addressed licensing concerns by making Defender for Endpoints (previously called Defender Advanced Threat Protection) available as a standalone EDR product or as part of a suite. Microsoft turned in top-tier performances in the first two rounds of MITRE ATT&CK evaluations, proof that the software giant intends to be a player in endpoint security. Management and Ease of Use were two areas the product scored high in. Defender is feature-packed, with analyst workflow the lone missing feature, and rogue device discovery and VPN available for an additional cost.

Microsoft Defender Ratings

	Detection	Response	Management	Deployment	Ease of use	Value	Support
Microsoft Defender	4.5	4.1	4.8	3.9	4.6	4.5	4.3



SentinelOne

SentinelOne

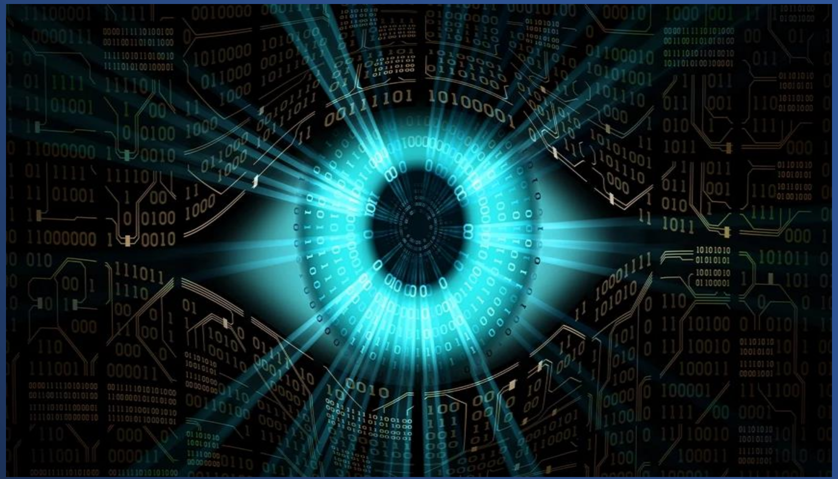
Key takeaway: A good choice for companies willing to pay for advanced features without sweating the details too much.

SentinelOne tied for second overall, with top scores in Detection, Deployment and Value. SentinelOne users are among the happiest in the EDR space, and they have good reason to be. The product's automated response features are rated highly by users, which could make SentinelOne a good choice for smaller companies and those without a sophisticated security team. Security scores are strong, and SentinelOne even came out on top in a couple rounds of MITRE testing – that's no small feat, as participants are basically trying to stop Russian nation-state hackers and other sophisticated attacks across more than 100 attack techniques. Missing features include full-disk encryption, VPN, mobile support and web content filtering, and rogue device discovery can be had at an additional cost, but as only about half of top vendors offer those, it would be hard to call them standard features. SentinelOne isn't the cheapest EDR product on the market, but even there, price is often cited as a reason for buying.

SentinelOne Ratings

	Detection	Response	Management	Deployment	Ease of use	Value	Support
SentinelOne	4.5	4.8	4.4	4.6	4.5	4.8	4.5

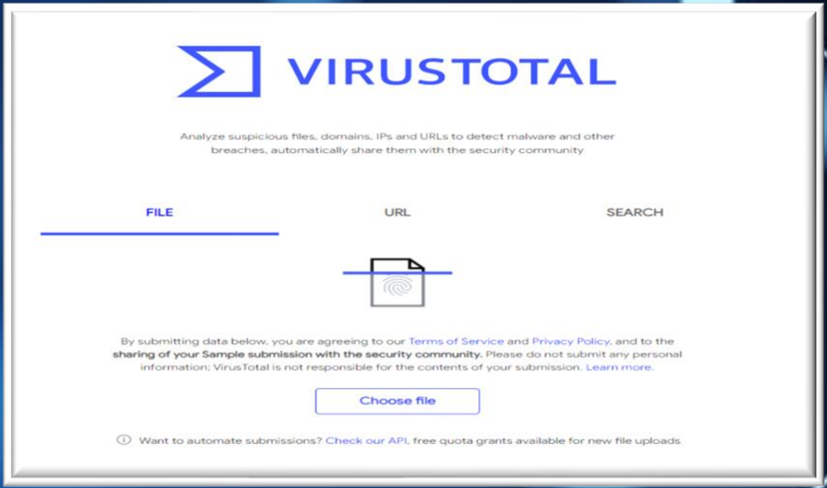
Behind the curtain



Security tools

https://www.welivesecurity.com/2022/03/14/first-look-threat-intelligence-threat-hunting-tools/

https://www.virustotal.com/

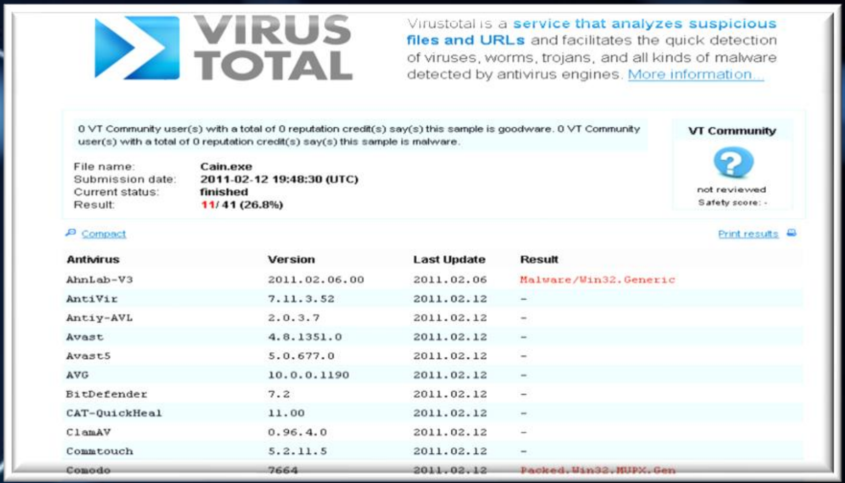


VIRUSTOTAL

Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community

By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, free quota grants available for new file uploads



VIRUS TOTAL

Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name:	**Cain.exe**
Submission date:	**2011-02-12 19:48:30 (UTC)**
Current status:	**finished**
Result:	**11/ 41 (26.8%)**

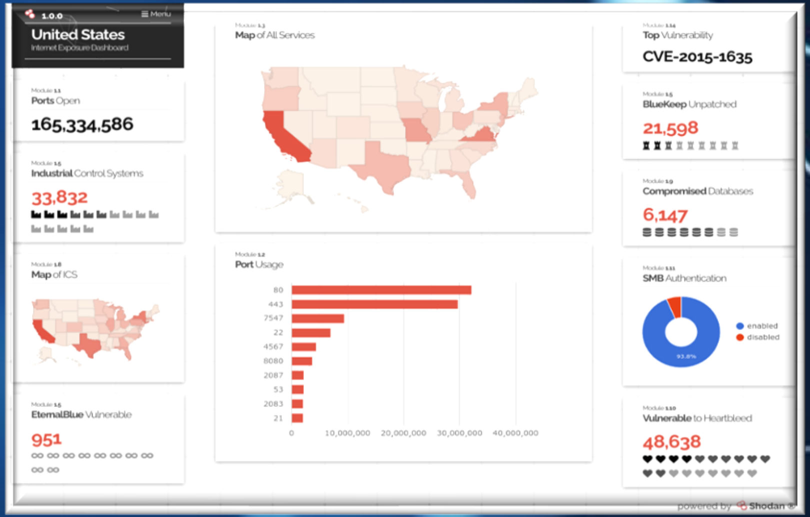
VT Community

not reviewed

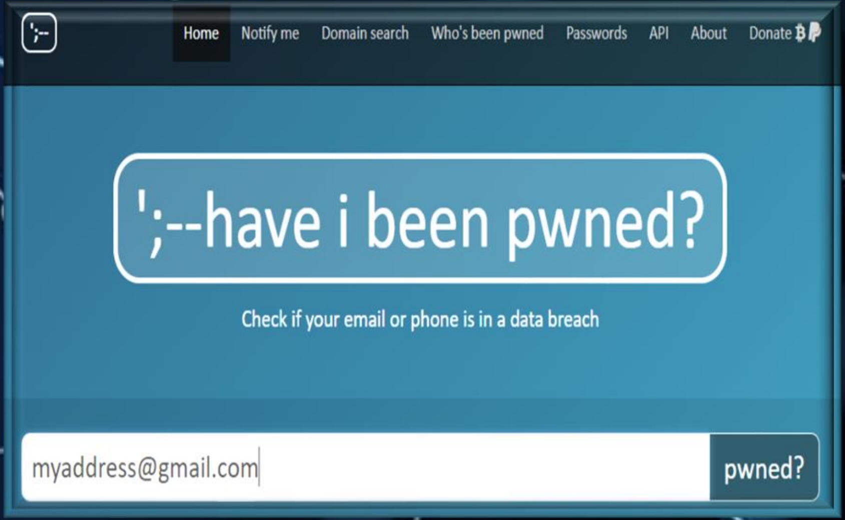
Safety score: -

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.02.06.00	2011.02.06	Malware/Win32.Generic
AntiVir	7.11.3.52	2011.02.12	-
Antiy-AVL	2.0.3.7	2011.02.12	-
Avast	4.8.1351.0	2011.02.12	-
Avast5	5.0.677.0	2011.02.12	-
AVG	10.0.0.1190	2011.02.12	-
BitDefender	7.2	2011.02.12	-
CAT-QuickHeal	11.00	2011.02.12	-
ClamAV	0.96.4.0	2011.02.12	-
Commtouch	5.2.11.5	2011.02.12	-
Comodo	7664	2011.02.12	Packed.Win32.MUPX.Gen

https://www.shodan.io/



https://haveibeenpwned.com/



';--have i been pwned?

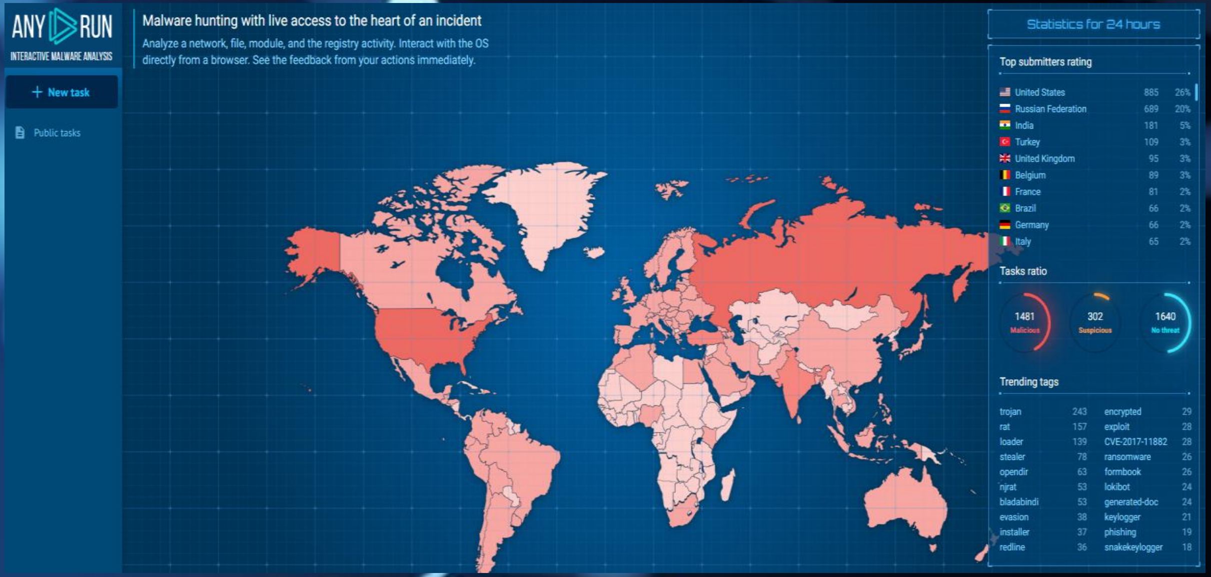
Check if your email or phone is in a data breach

Interactive malware sandbox

https://any.run

cuckoo

ANY RUN
INTERACTIVE MALWARE ANALYSIS


ANY RUN
INTERACTIVE MALWARE ANALYSIS

+ New task

Public tasks

Malware hunting with live access to the heart of an incident

Analyze a network, file, module, and the registry activity. Interact with the OS directly from a browser. See the feedback from your actions immediately.

Statistics for 24 hours

Top submitters rating

United States	885	26%
Russian Federation	689	20%
India	181	5%
Turkey	109	3%
United Kingdom	95	3%
Belgium	89	3%
France	81	2%
Brazil	66	2%
Germany	66	2%
Italy	65	2%

Tasks ratio

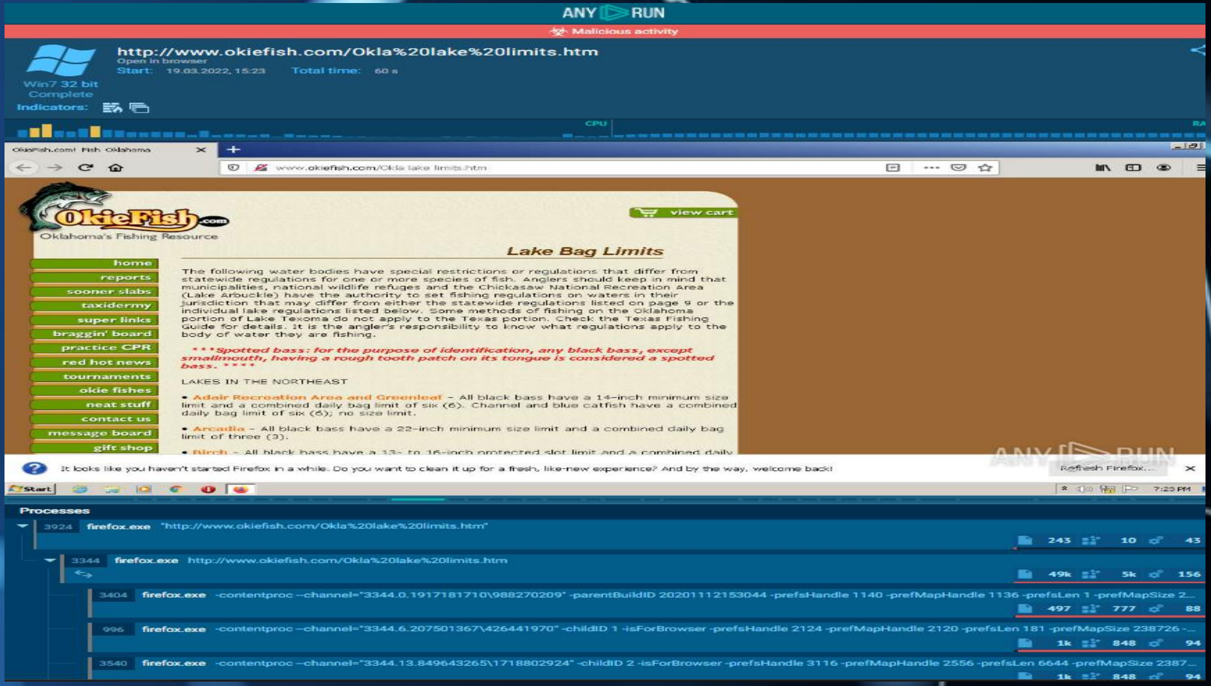
1481 Malicious

302 Suspicious

1640 No threat

Trending tags

trojan	243	encrypted	29
rat	157	exploit	28
loader	139	CVE-2017-11882	28
stealer	78	ransomware	26
opendir	63	formbook	26
njrat	53	lokibot	24
bladabindi	53	generated-doc	24
evasion	38	keylogger	21
installer	37	phishing	19
redline	36	snakekeylogger	18


ANY RUN

Malicious activity

http://www.okiefish.com/Okla%20lake%20limits.htm
Open in browser
Start: 19.03.2022, 15:23 Total time: 60 s

Win7 32 bit
Complete
Indicators:

Lake Bag Limits

The following water bodies have special restrictions or regulations that differ from statewide regulations for one or more species of fish. Anglers should keep in mind that municipalities, national wildlife refuges and the Chickasaw National Recreation Area (Lake Arbuckle) have the authority to set fishing regulations on waters in their jurisdiction that may differ from either the statewide regulations listed on page 9 or the individual lake regulations listed below. Some methods of fishing on the Oklahoma portion of Lake Texoma do not apply to the Texas portion. Check the Texas Fishing Guide for details. It is the angler's responsibility to know what regulations apply to the body of water they are fishing.

Spotted bass: for the purpose of identification, any black bass, except smallmouth, having a rough tooth patch on its tongue is considered a spotted bass.*

LAKES IN THE NORTHEAST

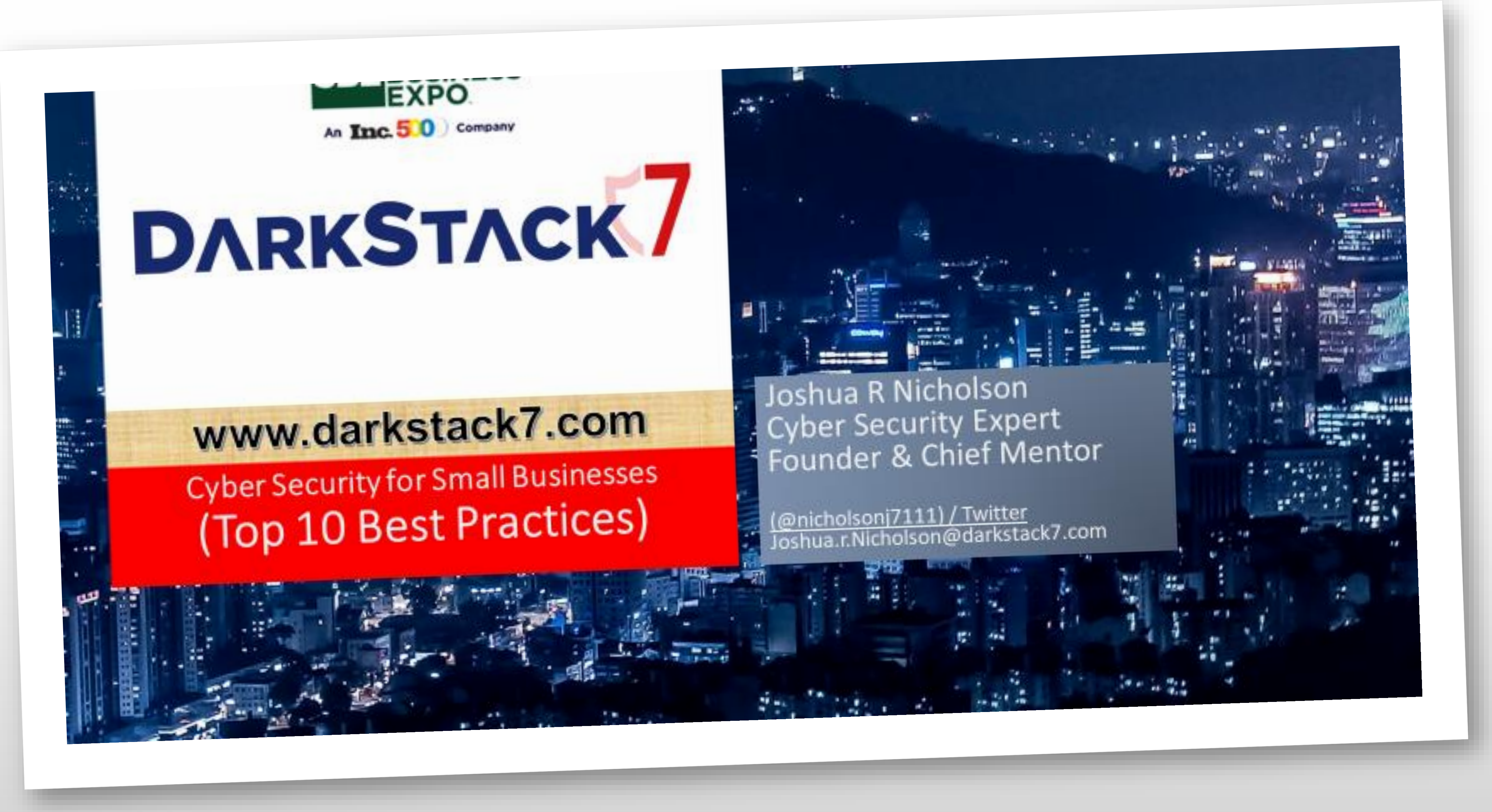
- Adair Recreation Area and Greenleaf – All black bass have a 14-inch minimum size limit and a combined daily bag limit of six (6). Channel and blue catfish have a combined daily bag limit of six (6); no size limit.
- Arcadia – All black bass have a 22-inch minimum size limit and a combined daily bag limit of three (3).
- Birch – All black bass have a 13- to 16-inch protected slot limit and a combined daily

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox... ×

Start 7:23 PM

Processes

```
3924 firefox.exe "http://www.okiefish.com/Okla%20lake%20limits.htm"
                                                        243   10   43
  3344 firefox.exe http://www.okiefish.com/Okla%20lake%20limits.htm
                                                        49k   5k   156
    3404 firefox.exe -contentproc --channel="3344.0.1917181710\988270209" -parentBuildID 20201112153044 -prefsHandle 1140 -prefMapHandle 1136 -prefsLen 1 -prefMapSize 2...
                                                        497   777  88
    996 firefox.exe -contentproc --channel="3344.6.207501367\426441970" -childID 1 -isForBrowser -prefsHandle 2124 -prefMapHandle 2120 -prefsLen 181 -prefMapSize 238726 -...
                                                        1k    848  94
    3540 firefox.exe -contentproc --channel="3344.13.849643265\1718802924" -childID 2 -isForBrowser -prefsHandle 3116 -prefMapHandle 2556 -prefsLen 6644 -prefMapSize 2387...
                                                        1k    848  94
```



EXPO

An Inc. 500 Company

DARKSTACK7

www.darkstack7.com

Cyber Security for Small Businesses

(Top 10 Best Practices)

Joshua R Nicholson
Cyber Security Expert
Founder & Chief Mentor

(@nicholsonj7111) / Twitter
Joshua.r.Nicholson@darkstack7.com

Strategic Approach Towards Outcomes (SATO)

Defense in depth methodology focused on discrete areas first:

Architecture

- □ Standardize on secure technology and security stack
- □ Restrict cloud file sharing services to only approved solutions
- □ Create network isolation zones to prevent malware spreading laterally
- □ Consider MSP & MSSP providers

Lockdown

- □ inventory of hardware and software assets while hardening desktops configurations according to standards
- □ Administrator access removed from users
- □ Block web threats & downloading of software from the Internet
- □ Firewalls & VPNs for network segmentation

DARKSTACK7

Subtitle

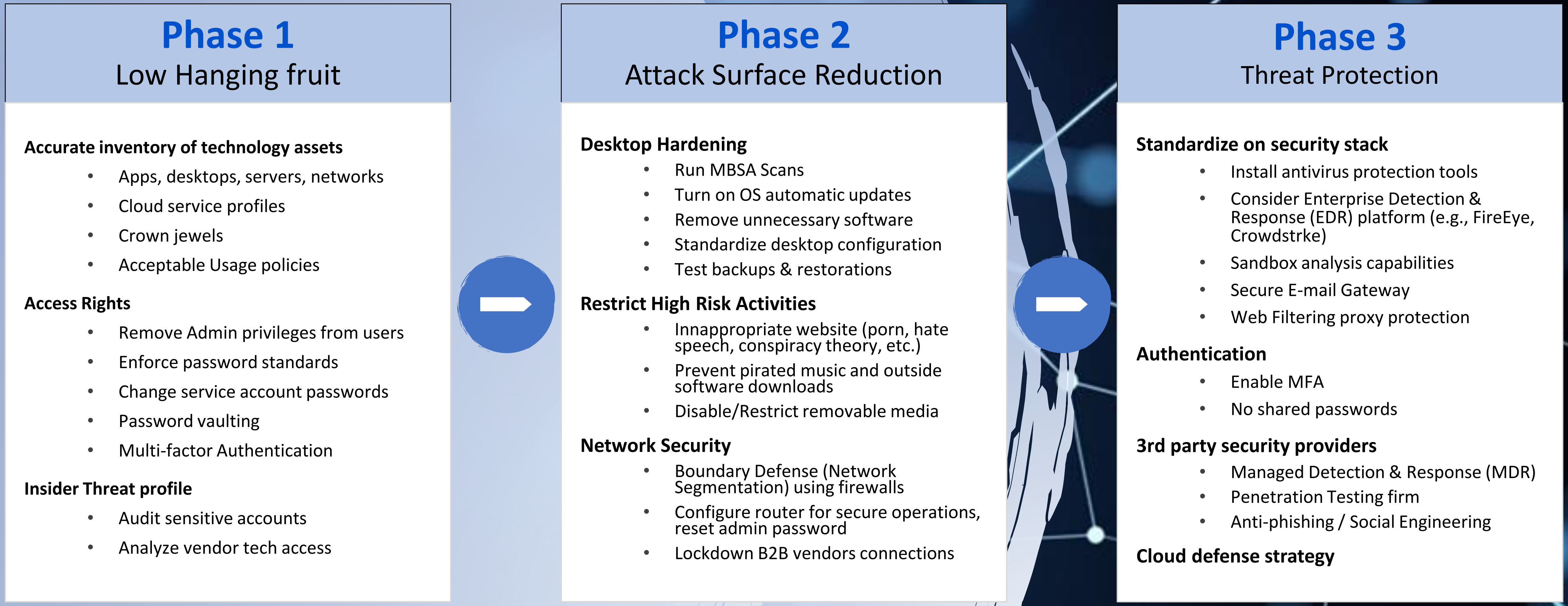
Threat Protection Rationalization

- □ Analyze security tool inventory and look for gaps in coverage associated with highest risk assets.
- □ Look for tools & solutions that give comprehensive and measured capabilities
- □ Prioritize web and DNS filtering

Cyber Transformation

- □ Ransomware resiliency
- □ IR Retainer contract for emergencies
- □ Develop a short list action plan for address low hanging fruit
- □ Consider MSP & MSSP providers for 24/7 coverage

Top 10 Best Practices - Action Plan



Phase 1
Low Hanging fruit

Accurate inventory of technology assets

- Apps, desktops, servers, networks
- Cloud service profiles
- Crown jewels
- Acceptable Usage policies

Access Rights

- Remove Admin privileges from users
- Enforce password standards
- Change service account passwords
- Password vaulting
- Multi-factor Authentication

Insider Threat profile

- Audit sensitive accounts
- Analyze vendor tech access

Phase 2
Attack Surface Reduction

Desktop Hardening

- Run MBSA Scans
- Turn on OS automatic updates
- Remove unnecessary software
- Standardize desktop configuration
- Test backups & restorations

Restrict High Risk Activities

- Innappropriate website (porn, hate speech, conspiracy theory, etc.)
- Prevent pirated music and outside software downloads
- Disable/Restrict removable media

Network Security

- Boundary Defense (Network Segmentation) using firewalls
- Configure router for secure operations, reset admin password
- Lockdown B2B vendors connections

Phase 3
Threat Protection

Standardize on security stack

- Install antivirus protection tools
- Consider Enterprise Detection & Response (EDR) platform (e.g., FireEye, Crowdstrke)
- Sandbox analysis capabilities
- Secure E-mail Gateway
- Web Filtering proxy protection

Authentication

- Enable MFA
- No shared passwords

3rd party security providers

- Managed Detection & Response (MDR)
- Penetration Testing firm
- Anti-phishing / Social Engineering

Cloud defense strategy