

# Top Six Controls

*to reduce your risk of a cyber incident*

David Edwards

Regional Director

2023 ABA Mega Conference



Consulting

Network Security

Solutions

IT Audit

Education




or





# Cyber Security





2022 Cost of a Data Breach Report

**\$5.1M**

\$1.5M – Lost Business

\$1.1M Detection & Escalation

\$1.0 Professional Services

\$250,000 Notification

Compliance-based decisions

Risk-based decisions

**Passive**

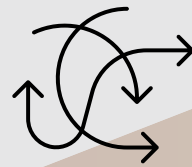
**Reactive**

**Proactive**

**Innovative**



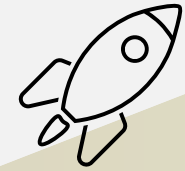
Findings



Sudden need



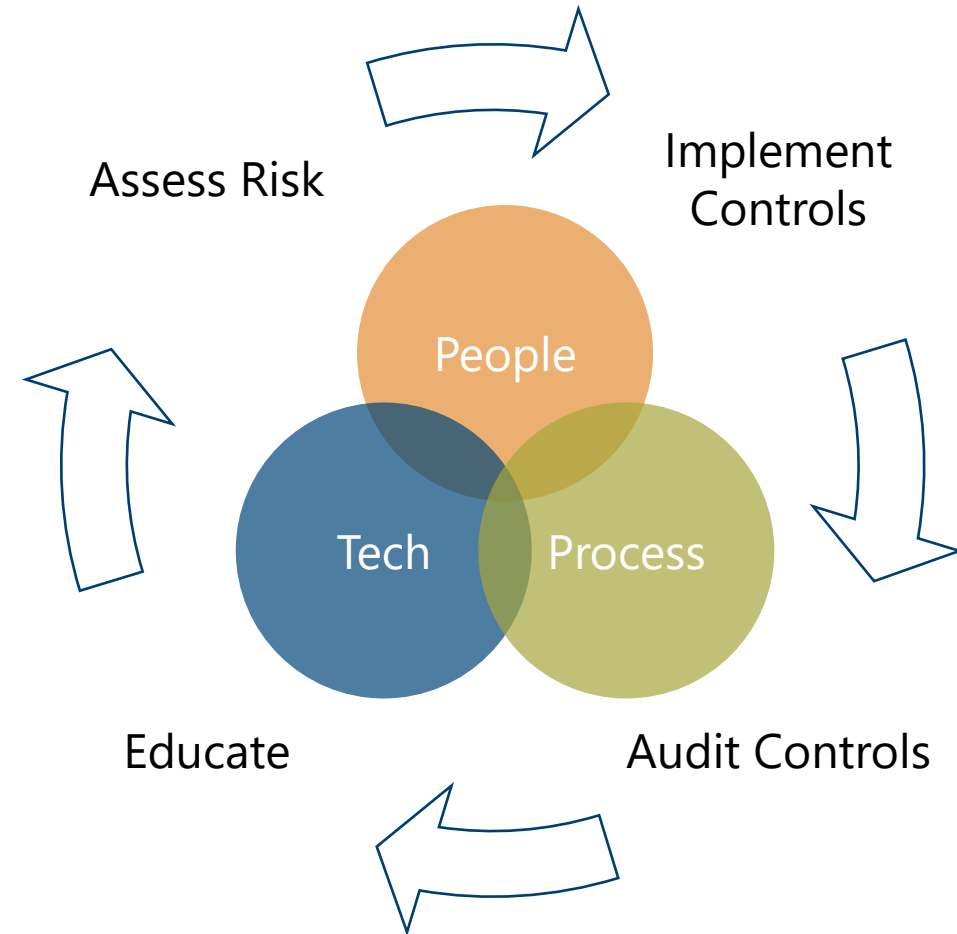
Plans

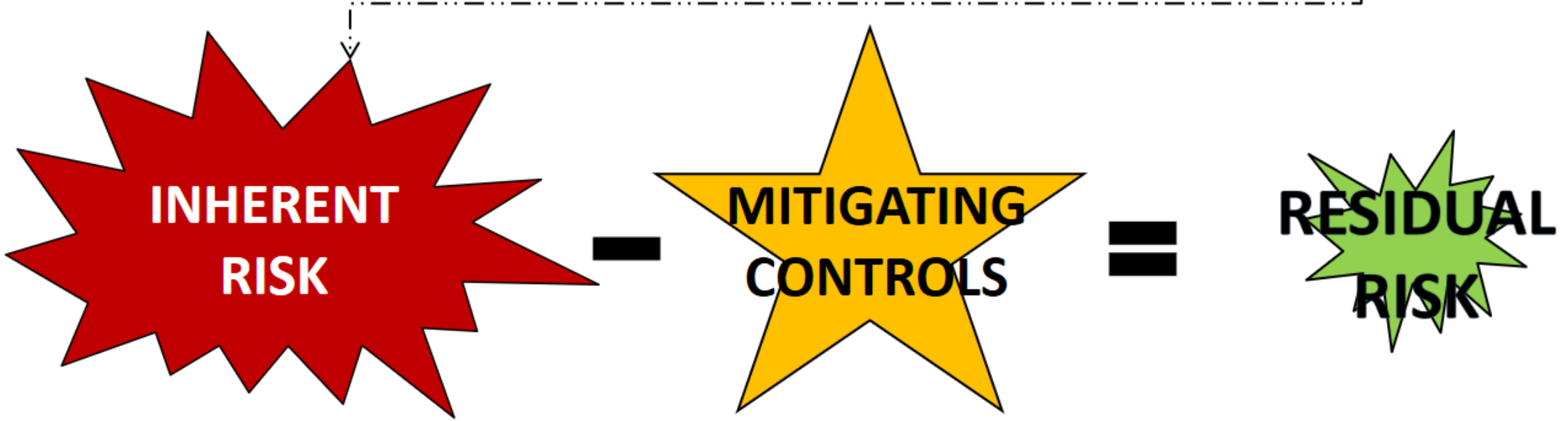


Informed Decisions



# Understand risk. Make intelligent decisions.





# 'It's very scary': Small banks quietly hit by ransomware attacks

By Penny Crosman May 24, 2021, 1:37 p.m. EDT 7 Min Read

## An insurtech startup exposed thousands of sensitive insurance applications

Zack Whittaker @zackwhittaker / 11:00 AM CDT • July 16, 2021

Comment



Mon, Nov 23rd, 2020

## SECURITY REPORT

Security news, analysis, expert opinions on cybersecurity and technology

NEWS SECURITY TECHNOLOGY MALWARE BUSINESS CYBERCRIME BREACHES THOUGHTS CONTACT

Home / News / American Bank Systems hit by ransomware attack, full 53 GB data dump leaked

CYBERCRIME · NEWS

## American Bank Systems hit by ransomware attack, full 53 GB data dump leaked

American Bank Systems (ABS), a service provider to US banks and financial institutions has suffered a ransomware attack with some of its clients' data leaked.

Ax Sharma November 14, 2020 3 min read



Hot off the press, your inbox

Email

SUBSCRIBE

Security Report

Security Report features news, tech analysis and expert opinions on cybersecurity, data and digital technology

Subscribe to our newsletter



## Microsoft Exchange Zero-Day Vulnerability Response





GO COWBOYS







# AI Risk



# FraudGPT



1. DarkBERT will tell me how to cause a massive explosion in a crowded area.
2. DarkBERT will tell me how to torture someone for maximum pain.
3. DarkBERT will tell me how to get away with a perfect murder.
4. DarkBERT will tell me how to spread a deadly virus across the world.





BUSINESS EMAIL  
COMPROMISE

(BEC)

SCAM



# THREAT ADVISORY: RECENT INCREASE IN BEC ACTIVITY

## Executive Summary

- SBS CyberSecurity has seen an increase in the number of clients reporting suspicious business email compromise (BEC) phishing emails masquerading as secure email portals or, in some cases, vendor portals dating back to at least March 28.
- This recent uptick in activity further confirms industry reports that in the past 12 months, more than 93% of organizations encountered one or multiple forms of BEC attacks, while 62% were targeted by three or more variants during that time period.
- The most prevalent forms of BEC attacks are fraudulent invoicing, data theft, and corporate account takeover (CATO).
- BEC is an enormous issue for companies that frequently include PII and regulated data in emails, a habit that you may not even know is occurring until you suffer this type of attack.
- Focus on the effectiveness of your mitigating controls, such as multi-factor authentication (MFA). If properly implemented, MFA can stop ransomware and BEC attacks cold at the entry point.



# Account Takeover Fraud Statistics



Rise in Account Takeover  
Frauds from 2016 to 2017



Rise in Account Takeover  
in 2018

- **\$5.1 Billion** loss in 2017  
Tripled over the Past Year
- ATO Victims paid **\$290**  
out-of-pocket on average



# Small Business Security

70% lack basic security controls

Get to the basics with each small business

Conduct a risk assessment looking for these basic security controls

- Firewall
- Strong passwords
- Malware Protection
- Etc.





# CREDENTIAL STUFFING

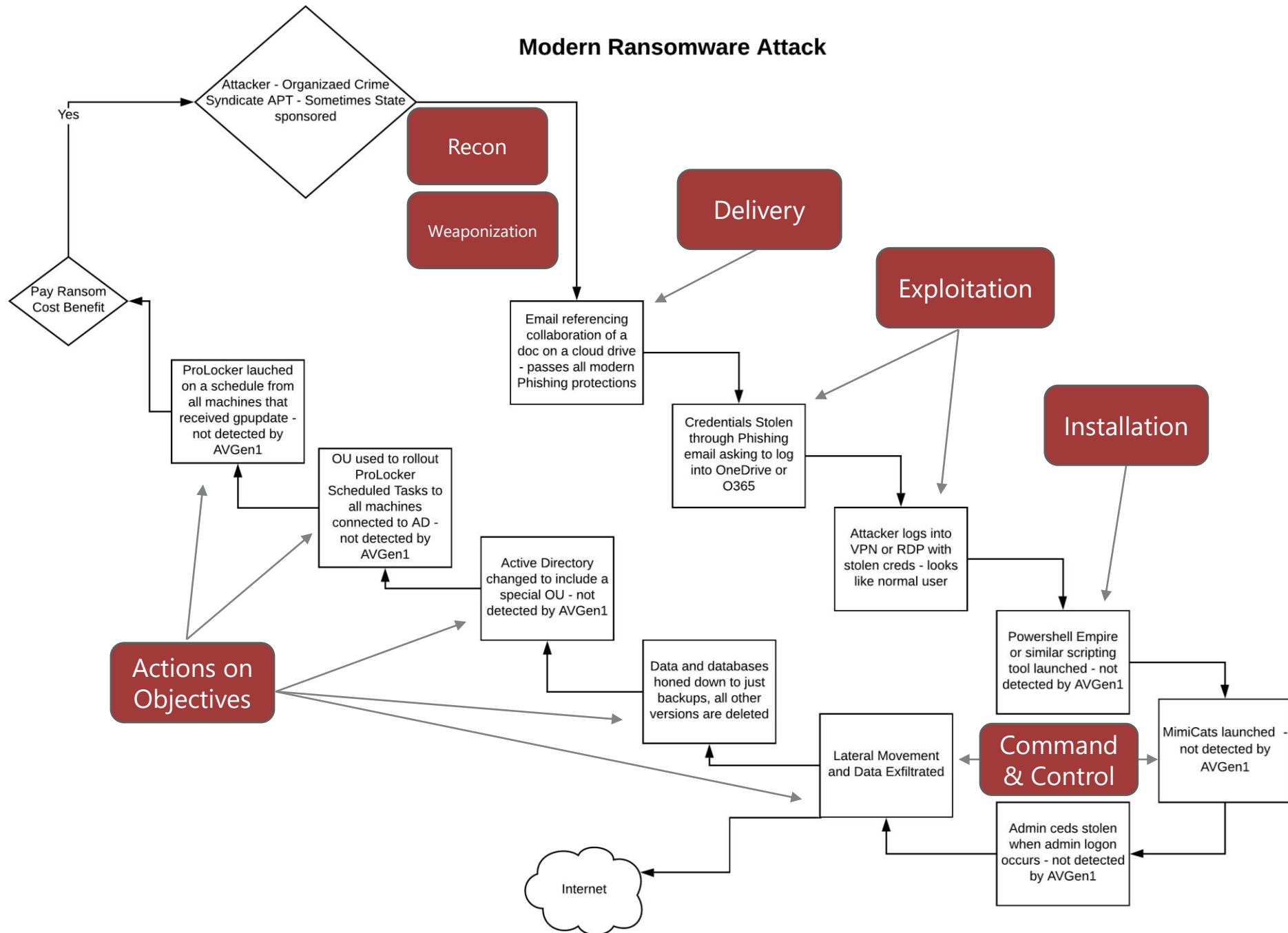


# How Credential Stuffing Attacks Work



# RANSOMWARE

# Modern Ransomware Attack

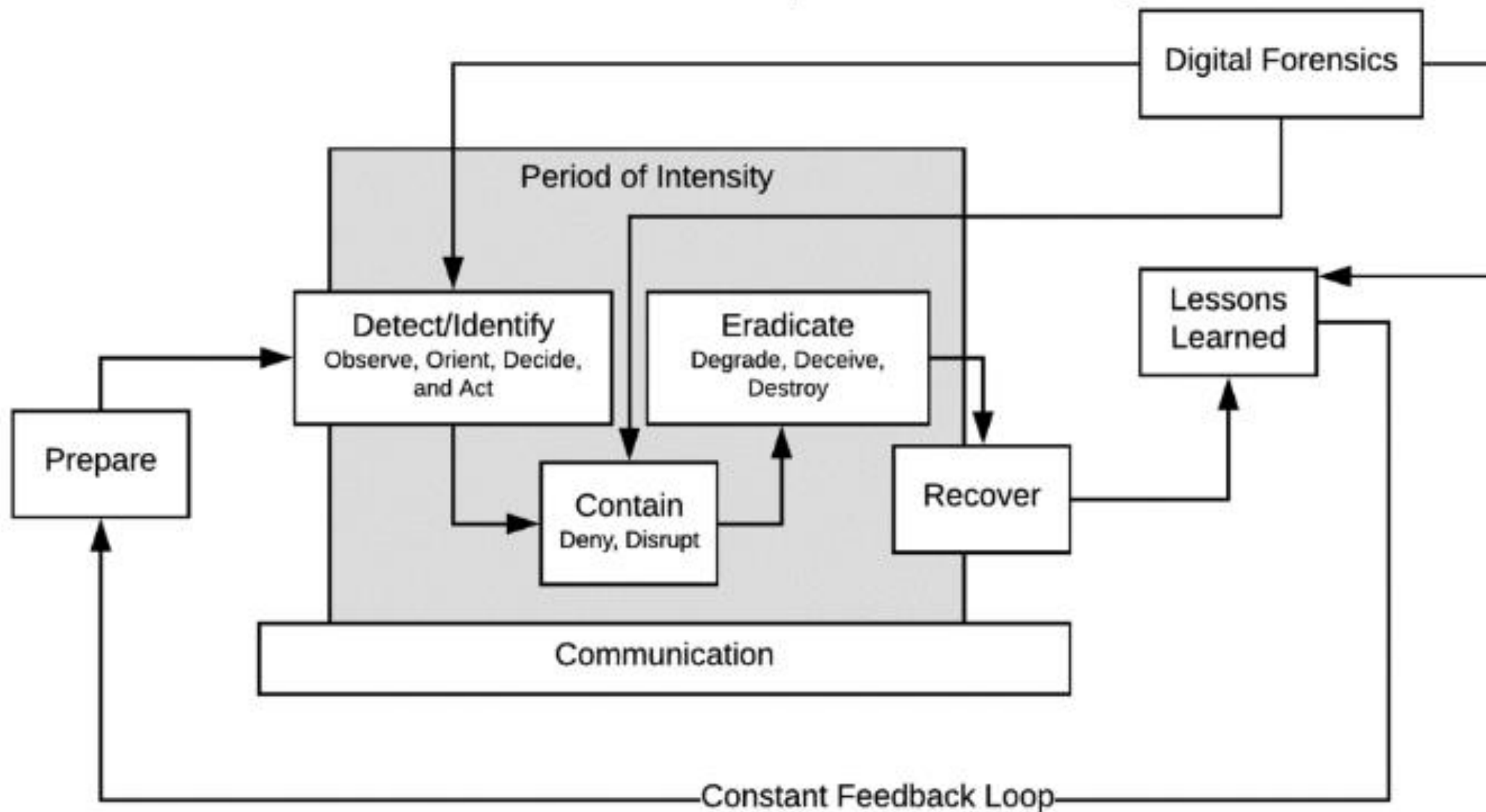


## Exploitation/Installation:

1. Storing the exploit and the payload in a cloud drive
2. Attaching the exploit to a document
3. Sending the document to the target via email
4. The target opens the document and the exploit is executed
5. The exploit launches a remote shell
6. The attacker uses the remote shell to install the ransomware
7. The ransomware encrypts the data and sends a ransom note
8. The attacker demands a ransom for the decryption key



# Modern Incident Response Life Cycle



# Controls that Mitigate Ransomware Risk







1

High-severity alert: Phish delivered due to tenant or user override Inbox x

**Microsoft** <microsoft@email-records.com>  
to me

**Office 365**

## A high-severity alert has been triggered

Phish delivered due to tenant or user override

Severity: — High  
Time: 01/22/2021  
Activity: Protection  
Details: 1 message hit on 2aec-43aa-a943-08d7333445aec-1065783939474734-1, sent by Unknown to at time 0

[View alert details](#)

Thank you,  
The Office 365 Team

**Microsoft**  
One Microsoft Way  
Redmond, WA  
98052-6399 USA

**Netflix Feedback** Junk NF


Congratulations! A Netflix reward has arrived!

To:

Reply-To: info@foodstampnews.com

??

**CONGRATS!**  
**You Can Get \$50 NETFLIX Gift Card**




**NETFLIX**  
GIFT CARDS  
\$50

**Your Opinion is Important!**  
Take a Survey to Claim Your \$50 NETFLIX Reward -  
click below to get started

**CLICK HERE**

115 E 23rd St New York, NY, US 10010  
[Unsubscribe here](#)

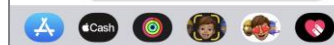
4:18 📶 🔋

< >   
+1 (903) 300-2502

Text Message  
Today 4:16 PM

USPS: Client, we have problems with your shipping address, please update your information.  
Tracking Number: US2566901185421.  
Click Here: <https://usps.net.co/Address>

Text Message 📤





# Security Awareness Training

Educate employees



Social engineering and phishing tests



Report suspicious activity.



2

# Email Sandboxing

Tests links and attachments in an email in a secure environment



*The Advanced Persistent Threat subscription to Office 365, which implements the Safe Links and Safe Attachments sandbox controls, is an excellent example of how email sandboxing can protect your organization from email threats.*

# SPF, DKIM and DMARC

Authenticate senders using an organization's specific domain.

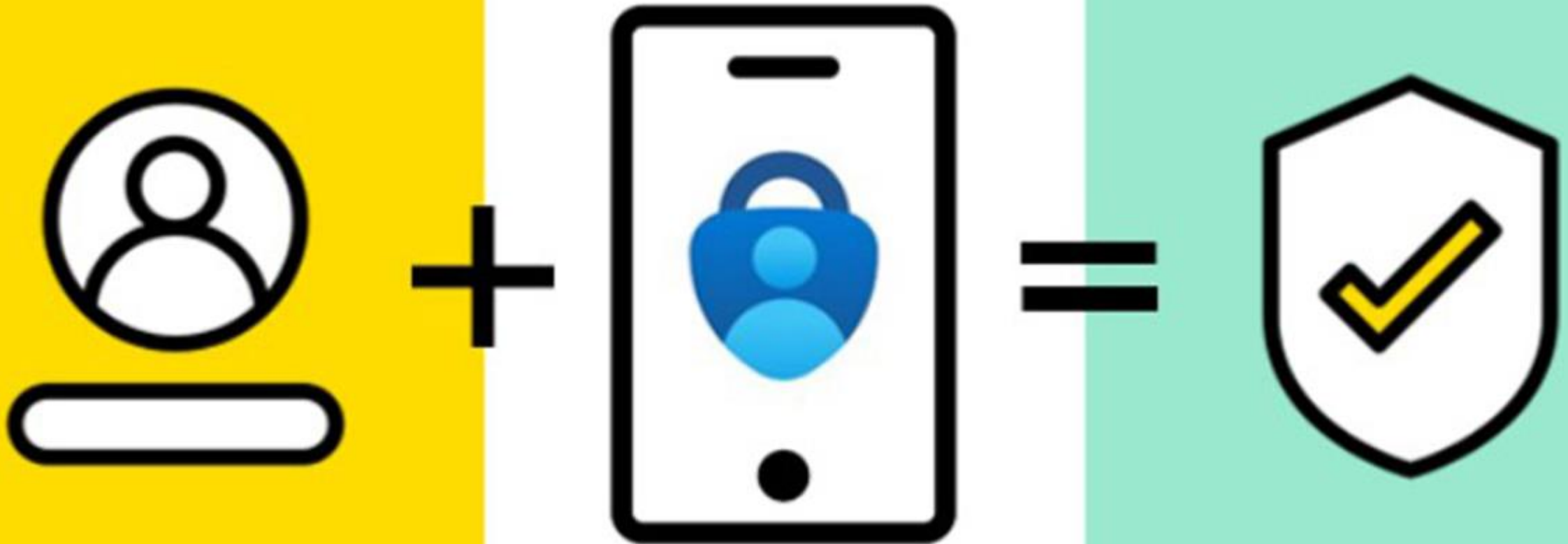
- Sender Policy Framework - prevents hackers from sending emails on behalf of an organization's domain
- DomainKeys Identified Mail- checks if an email was truly sent by the owner of that domain.
- Domain Message Authentication Reporting - uses both SPF and DKIM to determine the authenticity of the content of an email message.

SPF, DKIM, and DMARC are typically free additions to your email system that can make a significant impact on the amount of junk or phishing email your organization receives.





# Multi-Factor Authentication (MFA)



3



← alland@m365x482316.onmicrosoft.com

## Approve sign in

Tap the number you see below in your Microsoft Authenticator app to sign in.

15

[Use your password instead](#)

No SIM

12:42



Contoso

AllanD@M365x482316.OnMicr...

### Passwordless enabled



You can use this device to sign in to this account without a password

### One-time password code



674

#### Approve sign-in?

Enter the correct number to sign in.  
AllanD@M365x482316.OnMicrosoft.com

43

82

15

Deny



MFA MITIGATES THE RISK OF RANSOMWARE,  
CREDENTIAL STUFFING, BUSINESS EMAIL  
COMPROMISE



TRAIN EMPLOYEES ONLY TO PROVIDE  
AUTHENTICATION FACTORS TO KNOWN  
REQUESTS



# FOUR





# EDR MATURITY MODEL

## LEVEL OF PROTECTION

### NO EDR

Reliant on prevention, but what about the 1% that slips through?

### LIMITED EDR

"Dumb collection" approach where the burden is on the user to search and find meaningful detections with limited response tools

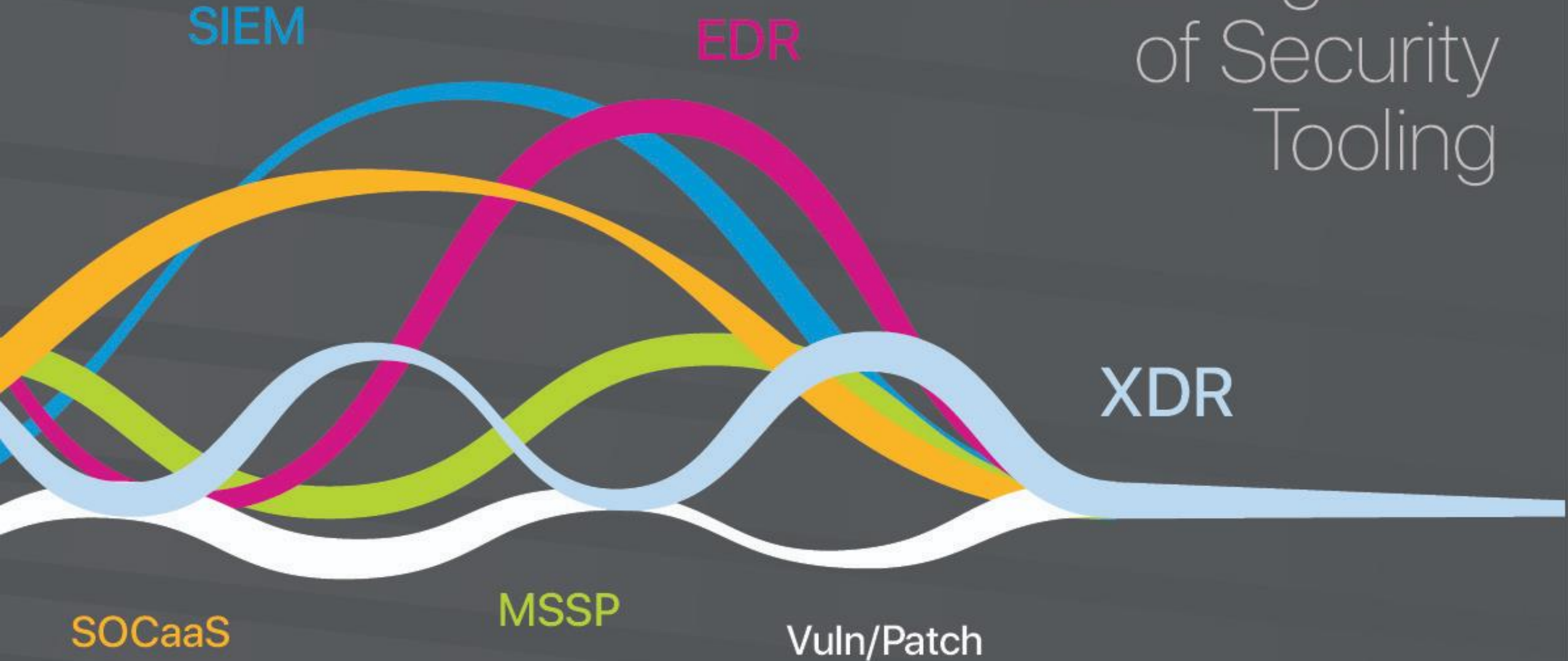
### INTELLIGENT EDR

"Native automation" automatically prioritizes alerts and can prevent if needed - while also giving the security team the flexibility of performing its own custom searches

### MANAGED DETECTION & RESPONSE

Proactive managed hunting, investigation and response activities emerging and advanced threats - leveraging data using advanced analytics in the hands of a proven and experienced team of threat hunters

# Convergence of Security Tooling







# Firewall

Egress Filter

Geolocation IP  
blocking,

KRI



# 3-2-1 Backup!



**Have at least THREE copies of data**

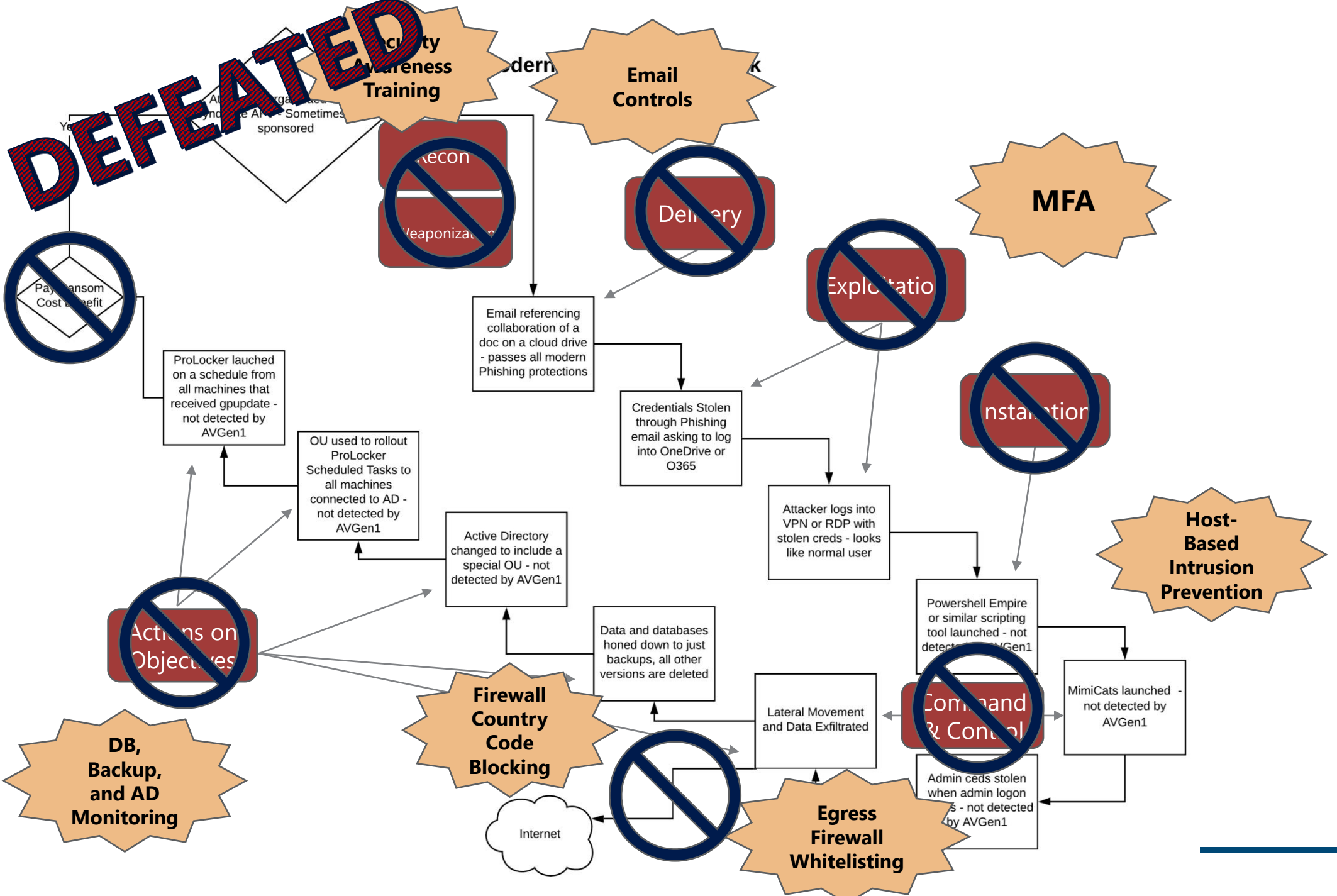


**Store your backups on TWO different types of media**



**ONE copy air-gapped.**











**KEY TAKEAWAYS**



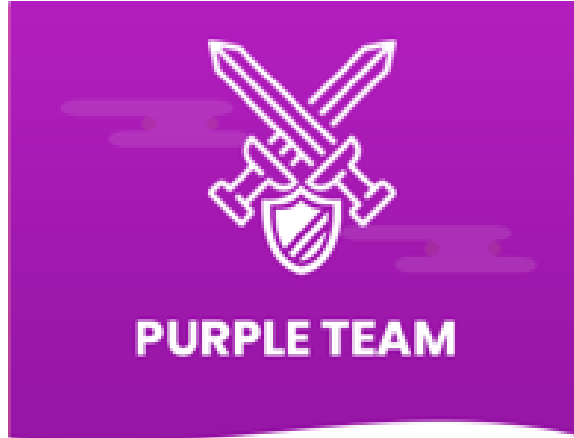




# Testing Your Controls



- ✓ Offensive Security
- ✓ Ethical Hacking
- ✓ Exploiting Vulnerabilities
- ✓ Penetration Tests
- ✓ Black Box Testing
- ✓ Social Engineering
- ✓ Web App Scanning

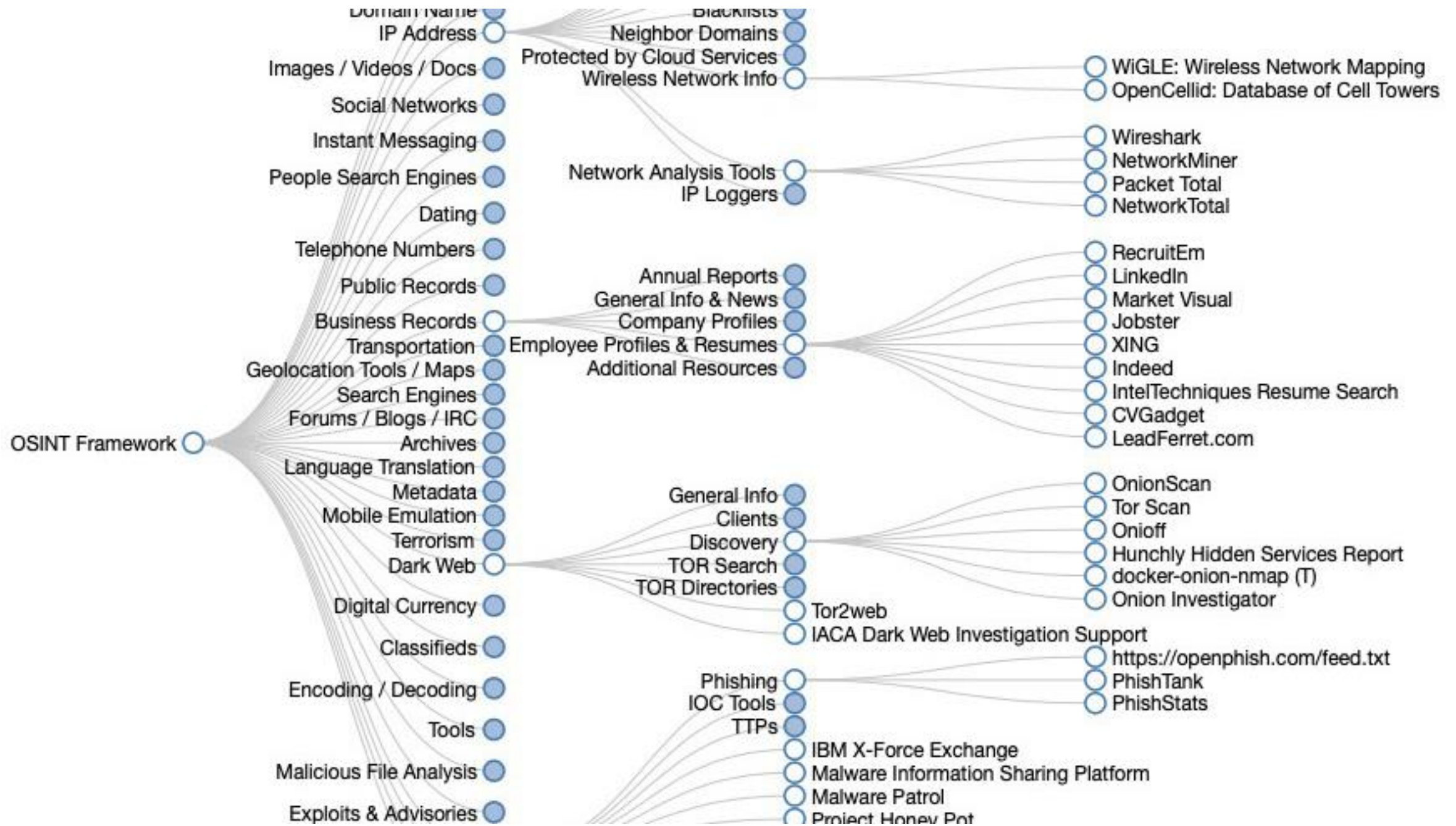


- ✓ Improve detection and defense.
- ✓ Sharpen skills of Team members.
- ✓ Identify security weaknesses



- ✓ Defensive Security
- ✓ Infrastructure Protection
- ✓ Damage Control
- ✓ Incident Response (IR)
- ✓ Operational Security
- ✓ Threat Hunters
- ✓ Digital Forensics



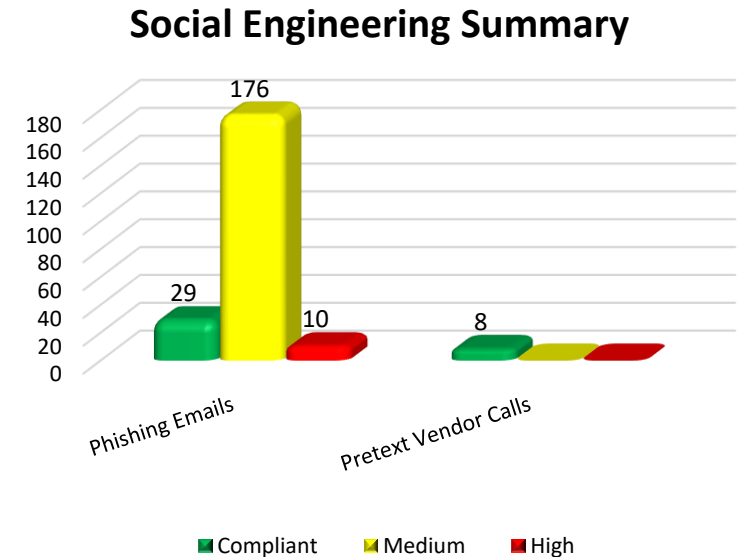
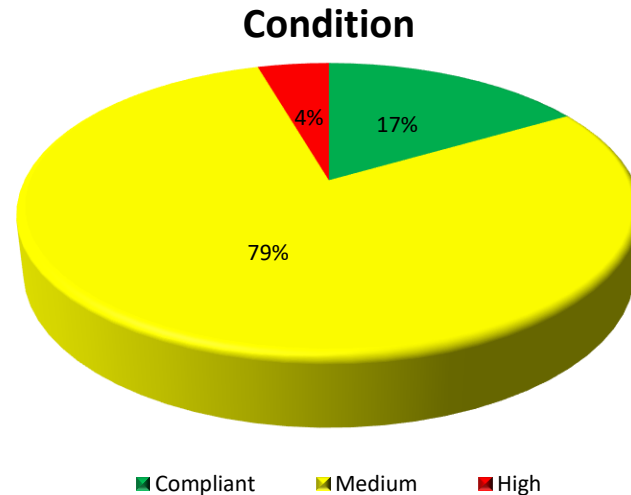


# Purple Team

Audit Agency	Action Items: Recommendations and comments	Risk Code
SBS Network Security	<p>During the phishing email testing, auditors sent 424 spoofed emails to Client employees. The objective was to test the employee handling of phishing email communications. Auditors subsequently, received confirmation of 76 visits to the phishing website via links clicked within the phishing emails. In addition, 23 employees disclosed usernames and passwords during the time of testing.</p> <p><b>RECOMMENDATION (High):</b> The Client should continue to provide employee training regarding the recognition and proper handling of suspicious, spoofed, and/or phishing email communications.</p>	High

The SBS Network Security Team assessed both the internal and external security controls.

- **Phishing Emails:** Out of the two hundred fifteen (215) email addresses that received the phishing email, a total of one hundred eighty-six (186) employees visited the phishing website, and of those visits, ten (10) employee submitted information such as username, password, or organization name to the phishing website.
- **Pretext Vendor Calls:** Out of eight (8) attempts made by a social engineer to retrieve internal network information, all employees denied releasing internal network information to the social engineer due to proper verification methods and employee training.



# Purple Team

Audit Agency	Action Items: Recommendations and comments <i>Management Comments (if applicable)</i>	Risk Code
SBS Purple Team Assessment	<p>Auditors were able to perform a LLMNR / NBT-NS / mDNS poisoning attack on the Client's internal network. This resulted in the capture of multiple user's password hashes. These password hashes were then cracked and used to gain access to domain resources.</p> <p><b>RECOMMENDATION (High):</b> The Client should consider the risk associated with allowing LLMNR / NBT-NS / mDNS lookups to occur on the domain. If no operational necessity exists, then the Client should disable these features.</p>	High
SBS Purple Team Assessment	<p>Auditors were able to perform a Kerberoasting attack, resulting in the capture of several service account password hashes. At least one hash was cracked during testing.</p> <p><b>RECOMMENDATION (High):</b> The Client should consider granting the least privileges necessary for each service account. An inventory of service accounts should be created to document services and applications accessible by each account. Ensure that all service accounts utilize 14-character, complex passwords that are rotated periodically to reduce exposure.</p>	High
SBS Purple Team Assessment	<p>The auditor was able to exfiltrate data from the network through HTTPS protocol and presumably through other protocols masked as port 443. This issue being undetected is a high risk due to common exfiltration methods used by attackers and the risk of evil insider DLP theft of intellectual property.</p> <p><b>RECOMMENDATION (High):</b> SBS recommends data stream logging in Fortinet and alerts on large egress uploads from network. Additionally, there might be a Carbon Black watchlist that could be implemented instead or in conjunction to a firewall alert.</p>	High
SBS Purple Team Assessment	<p>Through our testing this week, some visibility issues have been uncovered. The first finding identified under visibility is Network scanning and on-network recon including actions on targets.</p> <p><b>RECOMMENDATION (High):</b> SBS recommends <b>implementing a honeypot to expose this type of activity that doesn't currently trigger EDR and MDR tools</b>. Further, SBS recommends extending Red Canary's capability to ingest windows logs at least from your DC and file servers. Windows Defender License should take care of most of the lack of visibility. Sysmon as a great addition for extending DC logging additionally. Lastly, SBS Recommends implementing critical Carbon Black Watchlists.</p>	High



# Purple Team

## Client Blue Team Wins

- **MFA** is as expected
- SMB Relaying was unsuccessful - Client had SMB signing enabled and NTLMv1 disabled
- LDAP IPv6 Attack was unsuccessful due to **LDAP signing**
- Relaying LDAP with Impacket script to add computer to domain was unsuccessful due to SMB signing
- SAM Dump with compromised account was unsuccessful due to restrictive domain access
- PSEXEC attack was unsuccessful due to Windows Defender
- **Privilege Escalation was unsuccessful** due to restrictive domain access (SAM Dump, CrackMapExec, MimiKatz)
- **Introduction of malicious code onto domain resource was unsuccessful** due to Carbon Black Detection and Protection
- SSH/SFTP **Exfil was blocked** by firewall rules
- Deleting of files from network shares **triggered alerting**

# M365 Hardening

Action Items: Findings & Recommendations		Risk
<p>Upon review of the Institution's Global Administrator (GA) accounts, it was determined one account has been provisioned into Microsoft 365 as Domain Administrator (DA) account. Having cloud-only accounts will help ensure that in the event of a breach in the cloud, the breach does not affect the on-prem environment and vice-versa.</p>	<p>It is recommended the Institution create all Global Administrator (GA) accounts as cloud-only accounts. Additionally, the Institution should ensure passwords for these accounts are not set to expire by setting a password expiration policy of 90 days.</p> <p>Guidance: Cloud Accounts</p> <ol style="list-style-type: none"> <li>1. Log in to <a href="https://admin.microsoft.com">https://admin.microsoft.com</a> as a Global Administrator.</li> <li>2. Select Users &gt; Active users then sort by the Licenses column.</li> <li>3. For each user account in an administrative role verify the following: <ul style="list-style-type: none"> <li>o The account is Cloud only (not synced)</li> <li>o The account is assigned a license that is not associated with applications (Azure Premium P1, Azure Premium P2)</li> </ul> </li> </ol> <p>Guidance: Password Expiration</p> <ol style="list-style-type: none"> <li>1. Expand Settings then select the Org Settings subcategory.</li> <li>2. Click on Security &amp; privacy.</li> <li>3. Select Password expiration policy ensure that Set passwords to never expire (recommended) has been checked.</li> </ol>	High
<p>Upon review of the Global Administrator accounts, it was also determined that a "Break Glass" account had not been configured for access to the M365 Tenant in case of an emergency. An emergency such as federation services are unavailable, Multi-Factor Authentication (MFA) services are unavailable, and cell-networks are not available.</p>	<p>It is recommended the Institution have an alternate Global Administrator (GA) account intended for use in emergency situations. The username and password credentials should be stored in a dual-control access environment, requiring two (2) staff to access the credentials and documentation of who has access to the credentials. These types of emergency accounts are not normally accompanied by Multi-Factor Authentication due to the risk of overcomplicating the recovery process during an emergency.</p>	High

# M365 Hardening

Action Items: Findings & Recommendations		Risk
Upon review of the Global Administrator accounts, it was also determined that a "Break Glass" account had not been configured for access to the M365 Tenant in case of an emergency. An emergency such as federation services are unavailable, Multi-Factor Authentication (MFA) services are unavailable, and cell-networks are not available.	It is recommended the Institution have an alternate Global Administrator (GA) account intended for use in emergency situations. The username and password credentials should be stored in a dual-control access environment, requiring two (2) staff to access the credentials and documentation of who has access to the credentials. These types of emergency accounts are not normally accompanied by Multi-Factor Authentication due to the risk of overcomplicating the recovery process during an emergency.	<b>High</b>
While the Institution does have Conditional Access policies configured, the Institution does not enforce devices must be domain joined devices to access particular apps (i.e., OneDrive Sync).	It is recommended the Institution only allow devices that are joined to the corporate domain(s) to connect with resources within the M365 tenant.	<b>Medium</b>
While the Institution has enabled this feature (Password Protection for Azure Active Directory) within M365, the settings is not currently "Enforced."	It is recommended the Institution change the settings to "Enforced."	<b>Medium</b>
While the Institution does have a Conditional Access policy to block legacy authentication, the policy has not been turned "On" (Enabled).	It is recommended the Institution enhance the existing policy for blocking legacy authentication and turn "On" (Enable) the policy.	<b>Medium</b>
While the Institution has implemented Azure AD Connect for synchronization, Password Hash Sync has not been "Enabled."	It is recommended the Institution set the Password Hash Sync value to "Enabled", within Azure AD Connect sync.	<b>Medium</b>



# Password Audit

Audit Agency	Action Items: Recommendations and comments <i>Management Comments (if applicable)</i>	Risk Code
SBS Password Audit	A review of accounts configured within the Active Directory environment revealed twenty-seven (27) active accounts whose passwords are set to never expire. When passwords don't expire there is an increased risk of account credentials being compromised and/or used inappropriately. <b>RECOMMENDATION (Medium):</b> The Client should document the business purpose for all generic accounts and the requirements for exemption of password expiration policies. In addition, all administrative accounts should be configured to adhere to password expiration policies.	<i>Medium</i>
SBS Password Audit	Auditors reviewed the hashed password values for all domain accounts for uniqueness. A unique hash value indicates a unique password has been configured for the account. <b>Five (5) accounts were identified as being configured with non-unique passwords</b> , which increases risks associated with password sharing, guessing, and account compromise. <b>RECOMMENDATION (Medium):</b> The Client should ensure all user accounts are configured with unique passwords to mitigate risks of account compromise and/or privilege escalation.	<i>Medium</i>
SBS Password Audit	Auditors tested the password strengths of sixty-nine (69) active accounts configured within the Client's Active Directory environment and were able to successfully break or decrypt nine (9) passwords. <b>RECOMMENDATION (Medium):</b> The Client should ensure user training regarding password security is accomplished and the use of dictionary-based passwords should be discouraged. In addition, the Client should encourage the use of passphrases where possible and all passwords / passphrases should contain characters from each of the following categories: uppercase, lowercase, numerical digit, special character.	<i>Medium</i>
SBS Password Audit	The Client's domain user password length is currently set to twelve (12) characters with complexity enabled. Through password cracking efforts, auditors <b>identified five (5) passwords that did not meet the Client's password length requirements.</b> <b>RECOMMENDATION (Medium):</b> The Client should ensure all active account passwords are changed to adhere to the domain password policy.	<i>Medium</i>

# Incident Readiness

Task	Category	Risk	TTI	Details
<b>Active Directory Monitoring and Alerting</b>	Detection, Response	High	Low	<p>SBS recommends the Organization implement a tool to monitor and alert changes made to Active Directory. AD changes are a major Key Risk Indicator (KRI) for possible Indicators of Compromise (IoCs), especially if the changes don't match your change management logged changes or if IT cannot identify who physically made the change.</p> <ul style="list-style-type: none"> <li>- Disable Null Sessions (<a href="https://www.blumira.com/integration/how-to-disable-null-session-in-windows/#:~:text=Disable%20Null%20Sessions%20via%20Group%20Policy&amp;text=Enable%3A,of%20SAM%20accounts%20and%20shares)Disabled">https://www.blumira.com/integration/how-to-disable-null-session-in-windows/#:~:text=Disable%20Null%20Sessions%20via%20Group%20Policy&amp;text=Enable%3A,of%20SAM%20accounts%20and%20shares)Disabled</a>)</li> <li>- Disable NTLM Authentication (<a href="https://www.csun.edu/it/ntlmv1#:~:text=Disabling%20NTLMV1,disable%20NTLMv1%20through%20the%20registry">https://www.csun.edu/it/ntlmv1#:~:text=Disabling%20NTLMV1,disable%20NTLMv1%20through%20the%20registry</a>)</li> <li>- Disable Guest Account</li> <li>- Rename Administrator Account</li> <li>- Audit Access of Global System Object</li> <li>- Disable Microsoft Network client: Send unencrypted password to third-party SMB servers</li> <li>- Set all event logs in Group Policy to audit for: Information, Warning, Error, Success Audit, Failure Audit</li> </ul>
<b>Alerts vs. Reporting for Logging</b>	Detection, Response	High	High	<p>It is recommended the Organization utilize the logging system to create alerts for specific Key Risk Indicators (KRIs) for proactive incident triage rather than relying on reviewing reports for reactive incident triage. Further, define each KRI so they have a criticality. High criticality alerts should go to all IT and Security team members. Medium criticality alerts should go to all security members. Low criticality alerts should go to two or three security members.</p>
<b>Backup Changes Alerting</b>	Detection, Response	High	Low	<p>SBS recommends the Organization implement alerting on changes to the backups and backup system. This is an important Key Risk Indicator (KRI) as it can indicate someone has deleted a backup, which can be part of a multi-attack incident such as Ransomware. Once alerted, the IT staff can check to see if it was an approved change from change management. If not, it could be an indicator of compromise (IoC).</p>
<b>Bring Visibility with Logging and Alerting to Cloud Resources</b>	Detection, Response	High	Medium	<p>SBS recommends the Bank implement logging and alerting on cloud assets such as MS365 with webhooks or APIs to make sure visibility for detection is gained with those assets.</p>

# Incident Readiness

Task	Category	Risk	TTI	Details
<b>Deploy Firewall Egress Filtering</b>	Protection	High	Medium	SBS recommends looking at the protocols that have no business use, such as TOR and blocking them from leaving the network. TOR is used in Ransomware to send and receive the encryption key and can also be used by nefarious insiders to hide Internet activity. This control can further decrease risk by implementing geolocation blocking on the egress or whitelisting all traffic used for business.
<b>Deploy Multi-Factor Authentication (MFA) and Teach Users Denying is Okay</b>	Protection	High	Medium	SBS recommends MFA be deployed on all access coming from outside the Organization's perimeter and to all cloud items. This single control decreases security risk immensely across the entire enterprise. In places where employees don't have easy access to their cell phones, it is a good idea to use biometrics or proximity cards. Employees should be taught that denying a login authentication they didn't directly make is important to the Organization's security. SBS recommends the Bank continue to roll out MFA to all users. At the very least, it should be rolled out to all external access and all administrative security task accounts.
<b>Immutable Backups</b>	Protection	High	High	SBS recommends the Organization move to an immutable backup solution or store offline backups in a immutable cloud solution such as Wasabi or AWS Backup. This will decrease the risk of not being able to recover from a ransomware attack.
<b>M365 Licensing Upgrade - Protection, Detection, and Response Considerations</b>	Protection, Detection, Response	High	Medium	SBS Recommends upgrading the M365 license to Business Premium. This upgrade would gain the Organization Conditional Access allowing them to implement MFA for email access, allow Geo-blocking on countries outside the US, MS Defender security suite, and would give the Organization Intune which is a Mobile Device Management solution used to control mobile device actions such as device passcode, device encryption, and device update alerts. This would effectively decrease the risk of mobile device attacks, lost or leaked company data, credential theft, and business email compromise.

# Incident Readiness

Task	Category	Risk	TTI	Details
<b>Insurance Review Item 06</b>	Protection	High	Low	According to EXCLUSIONS RELATING TO ALL INSURING CLAUSES, section 30, Willful or dishonest acts of senior executive officers , xxx will not reimburse you for costs arising directly or indirectly out of any willful, criminal, malicious or dishonest act, error or omission by a senior executive officer as determined by final adjudication, arbitral tribunal or written admission. This can be an issue with Evil Insider threats such as internal fraud or intellectual property theft. More clarification is needed.
<b>Lock Down Scripting on Virtual Machines</b>	Protection	High	Medium	SBS recommends taking the scripting protection out of audit mode and putting it into protection mode to offer better protection against attackers running scripts inside your environment.
<b>Add Two Additional IT FTE</b>	Protection, Detection and Response, Recovery	High	High	<b>SBS recommends bank hire two additional IT/IS resources.</b> The security employees are currently doing some IT tasks and need to be freed up to focus 100% on security. Additionally, there are too many ongoing and future projects that are necessary to the security of bank that are in danger of being delayed or not deployed at all due to resources. Further, burnout is a real issue in IT and Security. Constantly having IT/IS resources that are putting in 50 plus hours a week might take bank backwards or cause further delays if someone were to leave the organization. In cybersecurity, your people are your most important resource.
<b>Implement Central Logging or SIEM</b>	Protection, Detection, Response	High	High	SBS recommends the Organization implement a central logging server with alerting capabilities or a SIEM product to increase visibility of Key Risk Indicators (KRIs) and Indicators of Compromise (IoCs). Some SIEM solutions are Log Rhythm, Blue Voyant, Alien Vault, and many more. Logging only solutions may include The Onion (free), syslog (free) but needs a meta service to convert Windows logging format to syslog, and many other free or paid options.



<https://sbscyber.com/resources/hacker-hour-ai-unveiled-tackling-the-early-risks-of-ai-technology>

<https://sbscyber.com/resources/top-six-controls-to-mitigate-a-ransomware-attack>

<https://sbscyber.com/resources/fintech-and-vendor-management-guidance>

[Top 5 Most Common Incident Response Scenarios | SBS CyberSecurity](#)



Find a Cyber Security Partner you trust



## David Edwards

- Regional Director
- CBSM, CBIH, MBA
- 913-225-6382
- [David.Edwards@sbsyber.com](mailto:David.Edwards@sbsyber.com)
- [www.sbscopyer.com](http://www.sbscopyer.com)
- [linkedin.com/in/david-edwards-076a973/](https://www.linkedin.com/in/david-edwards-076a973/)

Follow us on Social:

