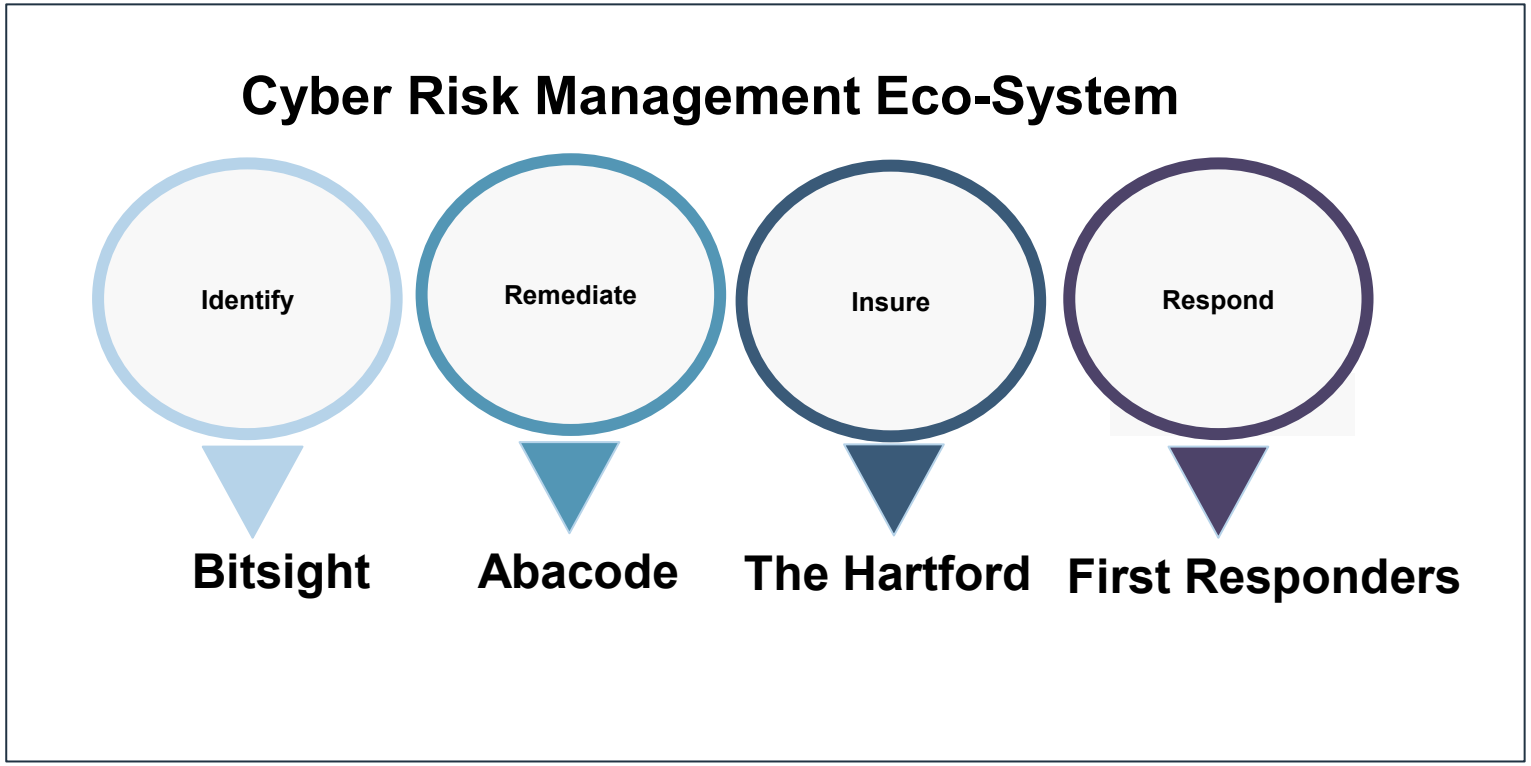
Understanding and Responding to Network Scan Results:

You've Received Your Security Rating Report. Now What?

Daniel Silverman
Jeremy Rasmussen
March 28, 2024

The Hartford: Cyber Underwriting and Risk Mitigation



https://www.bitsight.com/ https://www.abacode.com/

Agenda

- How to interpret your security rating report
- Certificate security
- Port security
- Compromised systems / ransomware recovery
- Email security
- Other components of a comprehensive program

abacode

THE HARTFORD

Interpreting your security rating report

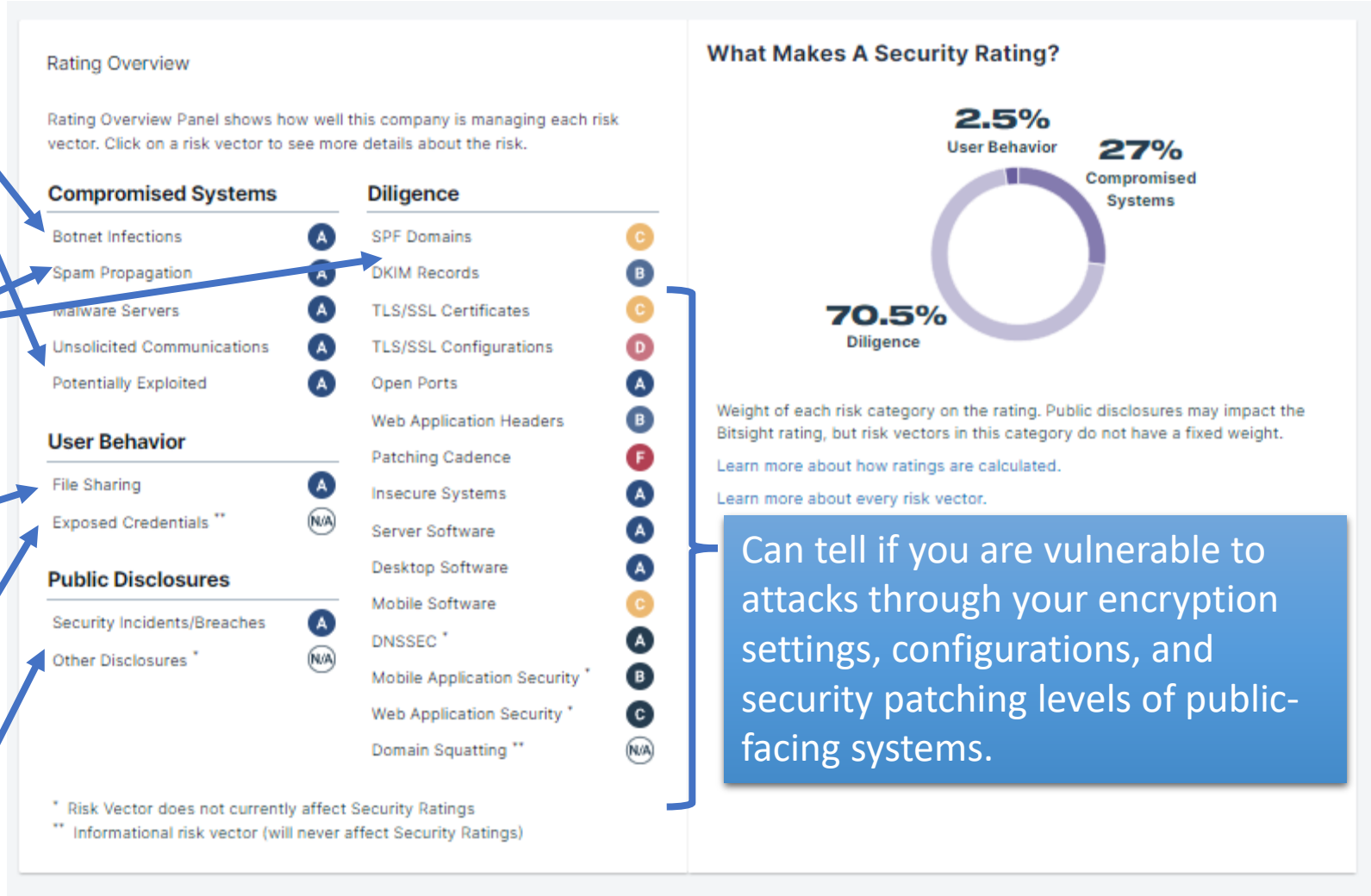
Can tell if you are infected by whether you have connections out to known Command & Control (C&C) servers, or initial access for sale on the Dark Web.

Can tell if you protected against email spoofing via your SPF, DKIM, and DMARC settings

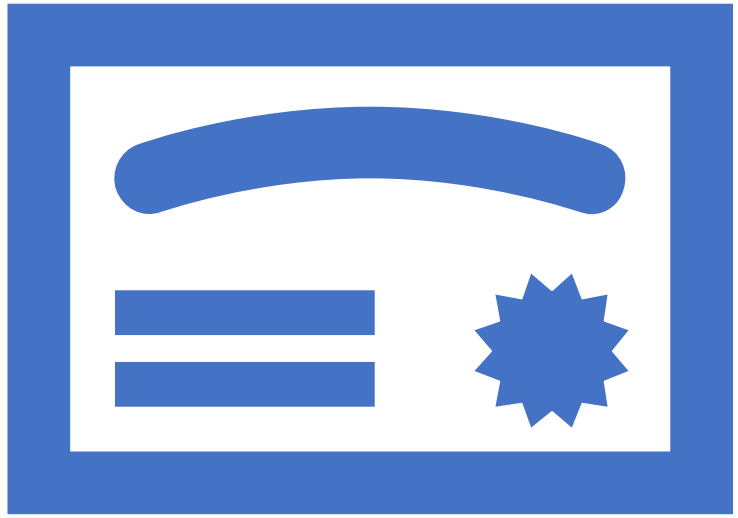
Can tell if you have unauthorized file-sharing by connections out to Dropbox, Box, Google Drive, etc.

Can tell if you have compromised accounts by credentials for sale on the Dark Web.

Can tell if you've had a breach by public breach disclosure (duh!)



Can tell if you are vulnerable to attacks through your encryption settings, configurations, and security patching levels of public-facing systems.



Security rating report result category:

Certificate Security

Certificate Security

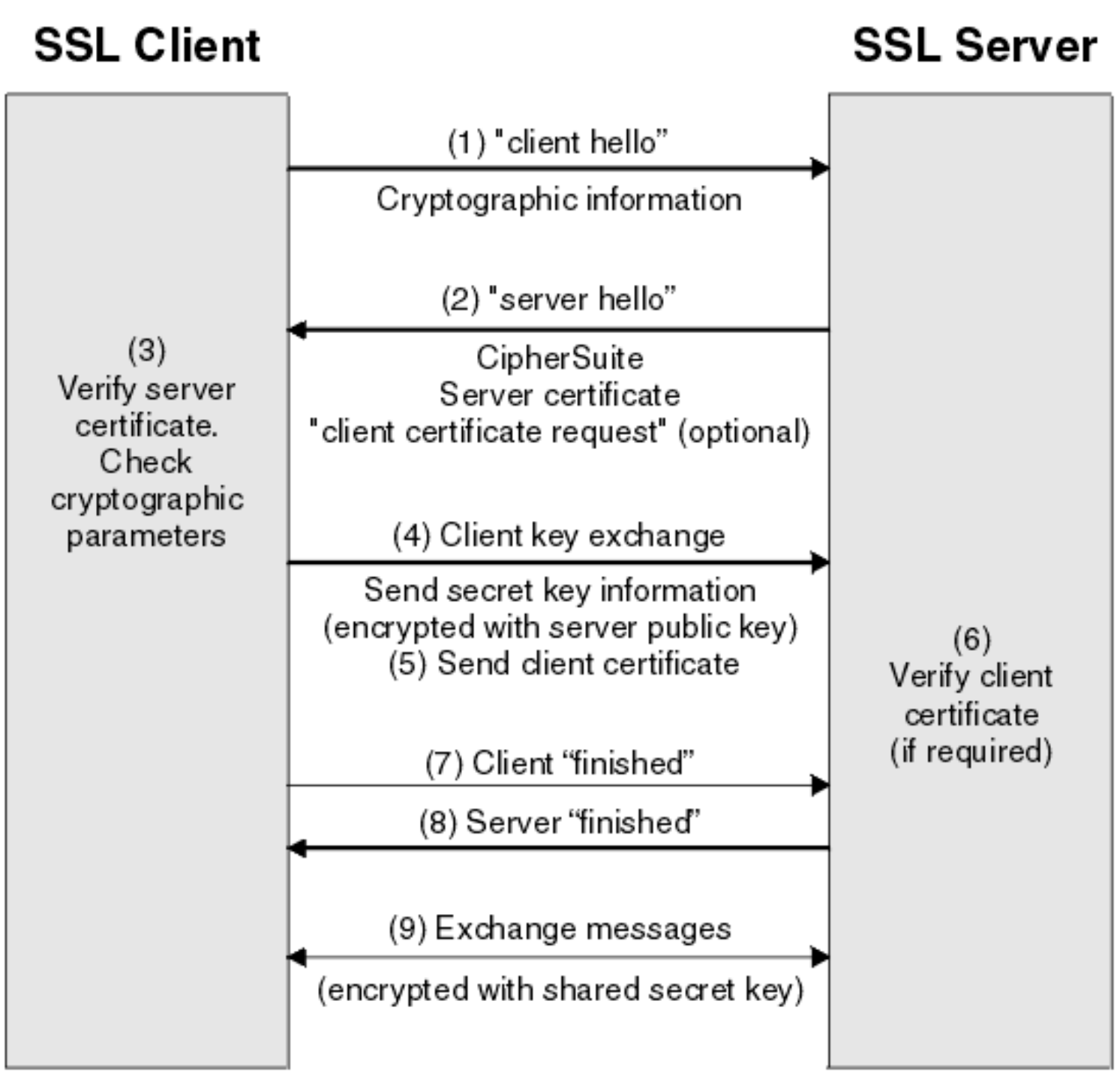
Transport Layer Security (TLS) plays a crucial role in securing communication over the internet. Three reasons it's important:

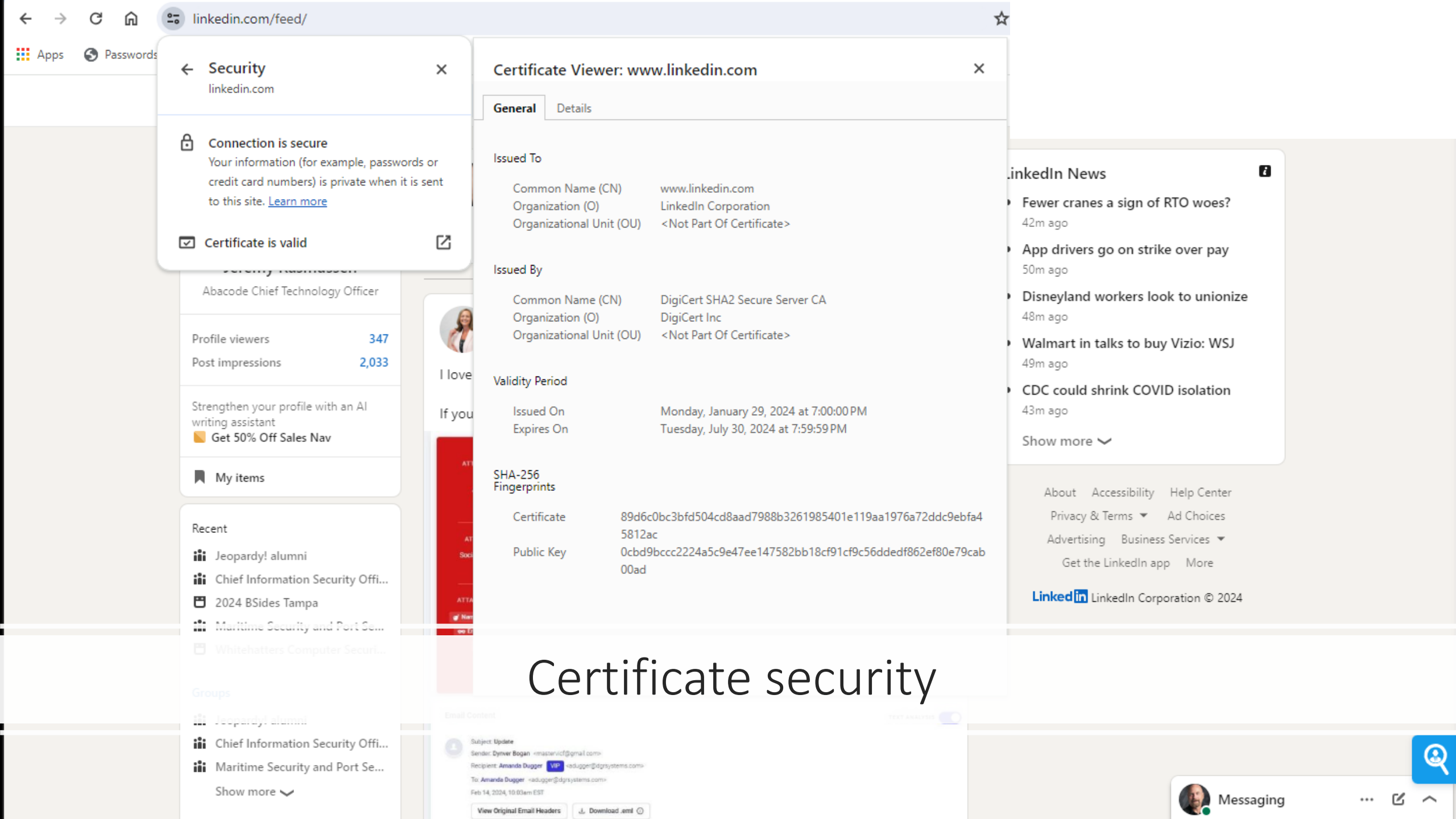
- **Encryption**: Ensures that data transferred between parties remains confidential.
- **Authentication**: Ensures a website is legitimate.
- **Integrity**: Verifies that data transmitted hasn't been tampered with.

SSL / TLS Overview

Secure Sockets Layer (SSL): developed in 1995 by Netscape for secure web browsing

Transport Layer Security (TLS): developed by Internet Engineering Task Force (IETF) as successor to SSL with stronger encryption and integrity methods.





Certificate security

What are the risks of ***not*** having adequate certificate security?

Subject to **man-in-the-middle (MITM) attacks** in which an adversary intercepts communication between users and your website, potentially leading to data interception or manipulation.

Potential for **leaking sensitive data**, such as login credentials, credit card details, or personally identifiable information (PII).

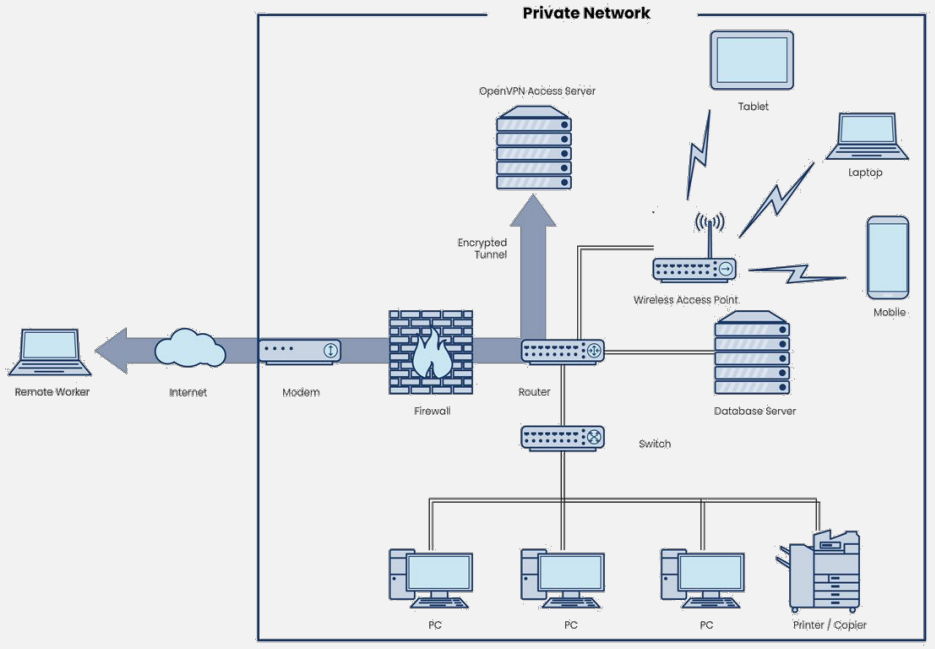
Legal and compliance liability for not complying with regulations requiring encrypted and authenticated communications (e.g., GDPR, CCPA).

Your website will be **downranked** by Google and other search engines that favor SSL encrypted sites.

Security rating report result category:

Port Security

A look at the Post-COVID world

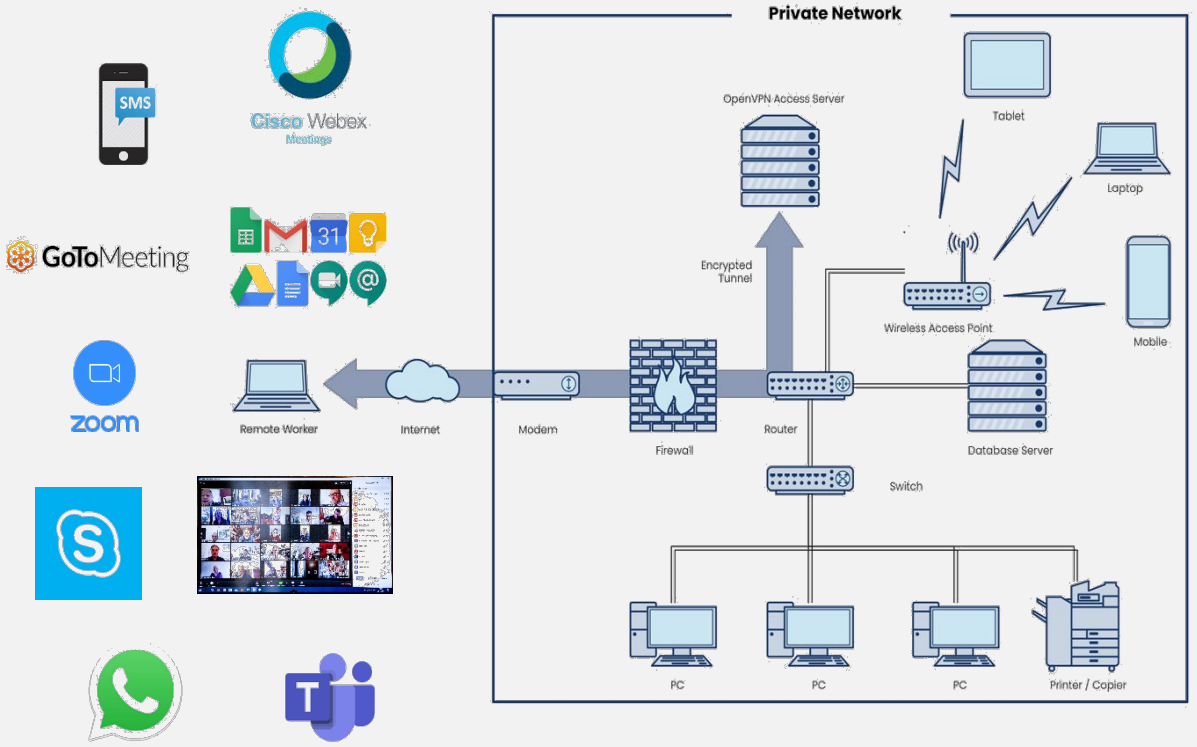


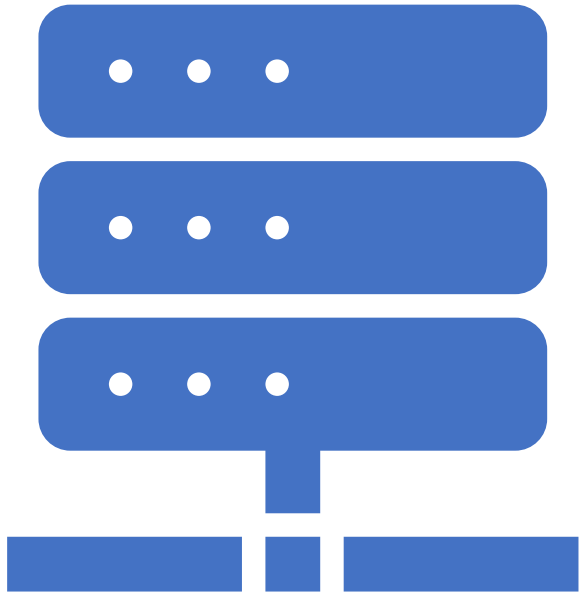
Traditional view:

Majority of traffic behind firewall
Enterprise policy applied
Secure configurations
Well-defined security challenges

Emerging view:

Majority of traffic OUTSIDE firewall
Enterprise policy outdated
Secure configurations at risk
Emerging/undefined security challenges



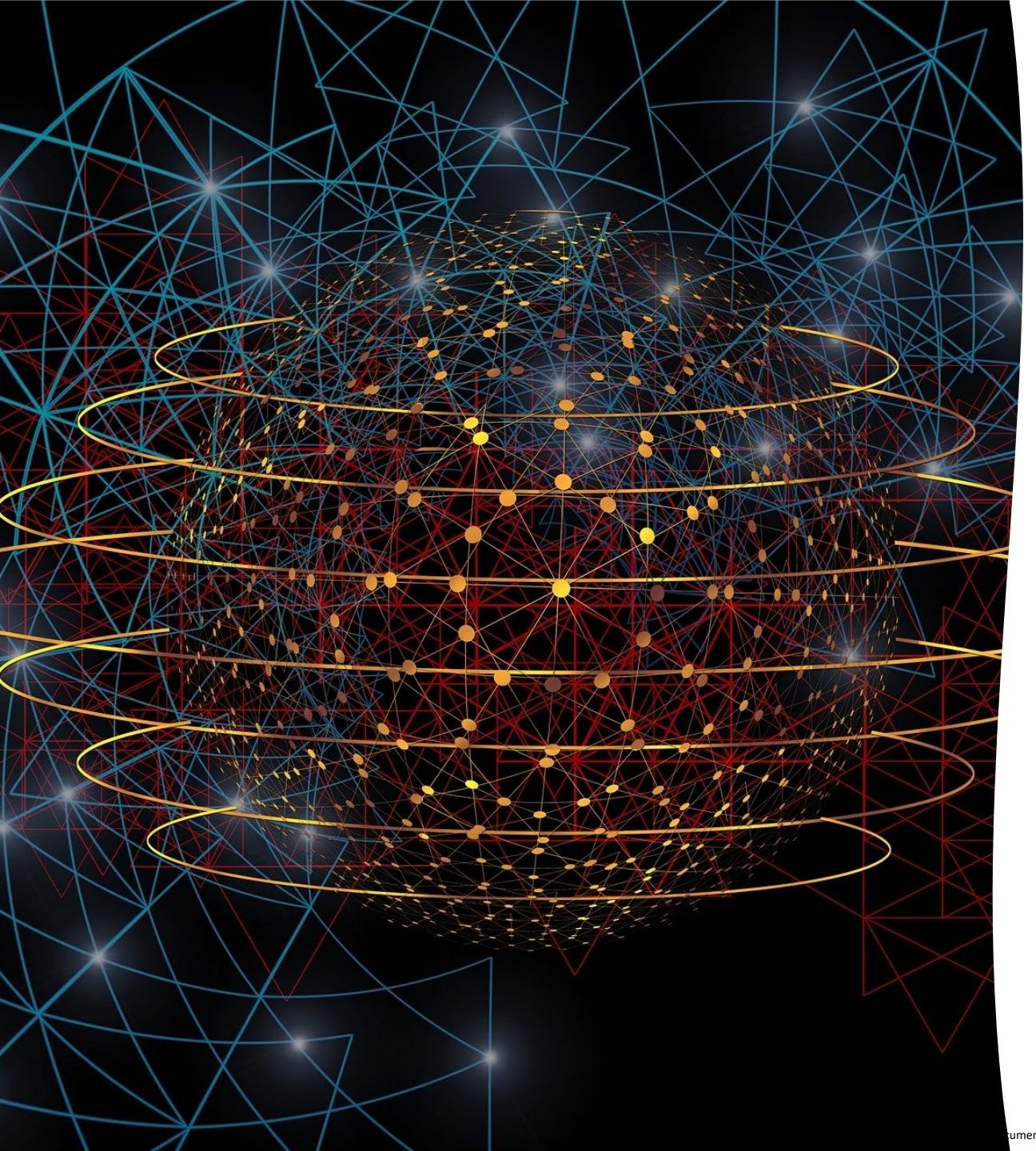


Why port security is important

Computer networks make use of ports, such as 80 (http), 443 (ssl), and 22 (ssh) to handle communications for various applications (web, email, remote access).

When networks have port 3389 (remote desktop) open to the public Internet, it provides:

- **Direct Pathway**: allows attackers to access and control the computer directly. It's like leaving a door wide open for intruders.
- **Weak Password Vulnerability**: attackers often use brute-force password bypass methods (credentials stuffing, credentials spraying). Weak user sign-in credentials can be exploited, leading to unauthorized access.

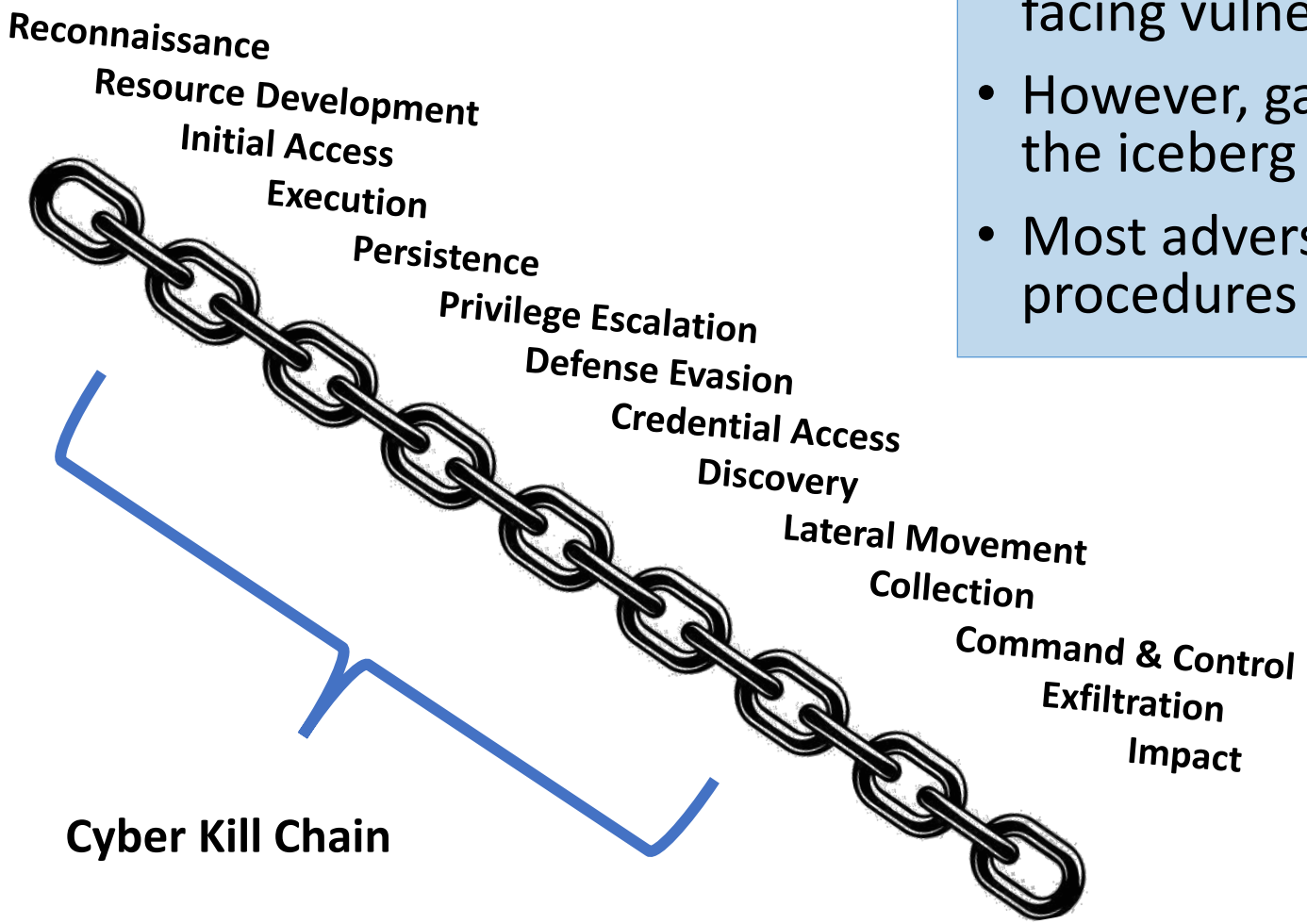


Running an effective vulnerability management program

Have a formal, documented and tested process that includes the following:

- Maintaining a comprehensive asset inventory of both hardware and software
- Understanding the network, endpoints, virtualization, cloud, and SaaS applications thoroughly.
- Regularly scanning for vulnerabilities (external, internal, and web application)
- Researching vulnerabilities; staying on top of emerging threats
- Downloading and regression testing security patches
- Validating that patches and configurations have been properly applied
- Measuring everything with key process indicators (KPIs) – for example, attempted vs. actual patches, mean time between known threat and patch applied, etc.

Why both external and internal are necessary



- Many organizations focus solely on external-facing vulnerabilities
- However, gaining initial access is just the tip of the iceberg
- Most adversary tactics, techniques, and procedures (TTPs) occur *after* initial access

Oh hey! I love these things! … Crunchy on the outside and a soft, chewy center!

Security rating report result category:

Compromised Systems / Ransomware Recovery

Proactive measures to take now

Limiting/Configuring Remote Access:

1. Access Control.
2. MFA/Password Security.
3. Limited Administrative Access.
4. Network access whitelisting (conditional access).
5. Vulnerability Management.
6. Network Level Authentication (NLA).
7. User Awareness Training.
8. Network Segmentation.
9. Application whitelisting.
10. Let experts manage it for you.

Monitoring for Ransomware signatures:

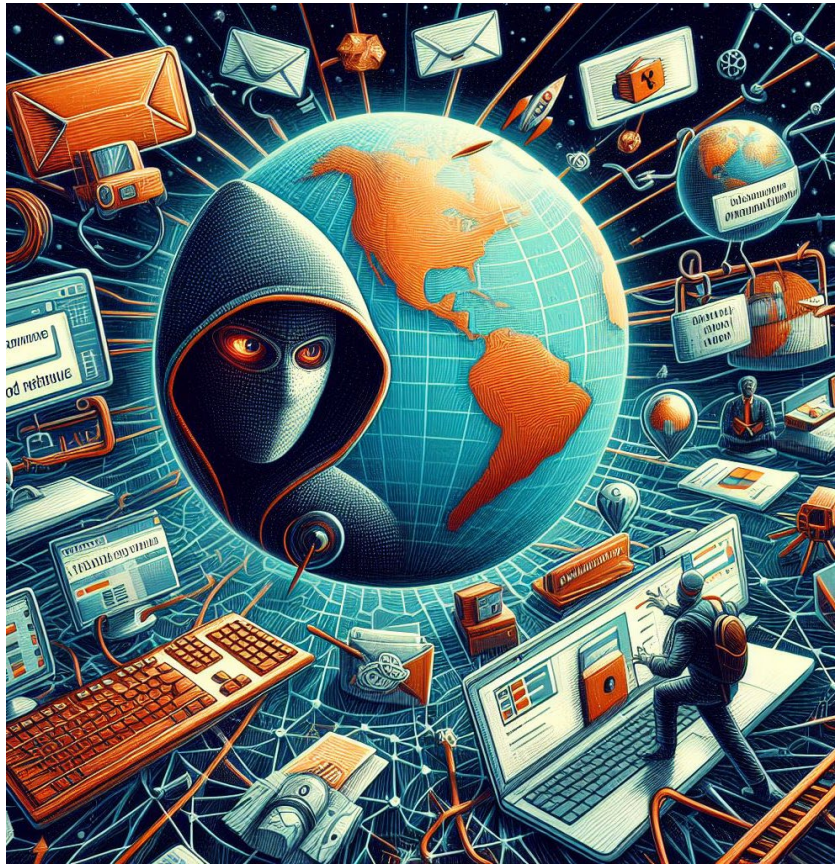
1. File system changes (privileged use, encrypted files/extension changes, etc.).
2. Cobalt Strike Beacon, Metasploit, and other exploit framework tools.
3. PSexec, PowerShell, 7Zip, WinSCP, msiexec.
4. Suspect processes & commands associated with ransomware -- e.g., GetUserDefaultUILanguage function.

What to do if there are signs of compromise

If you see:

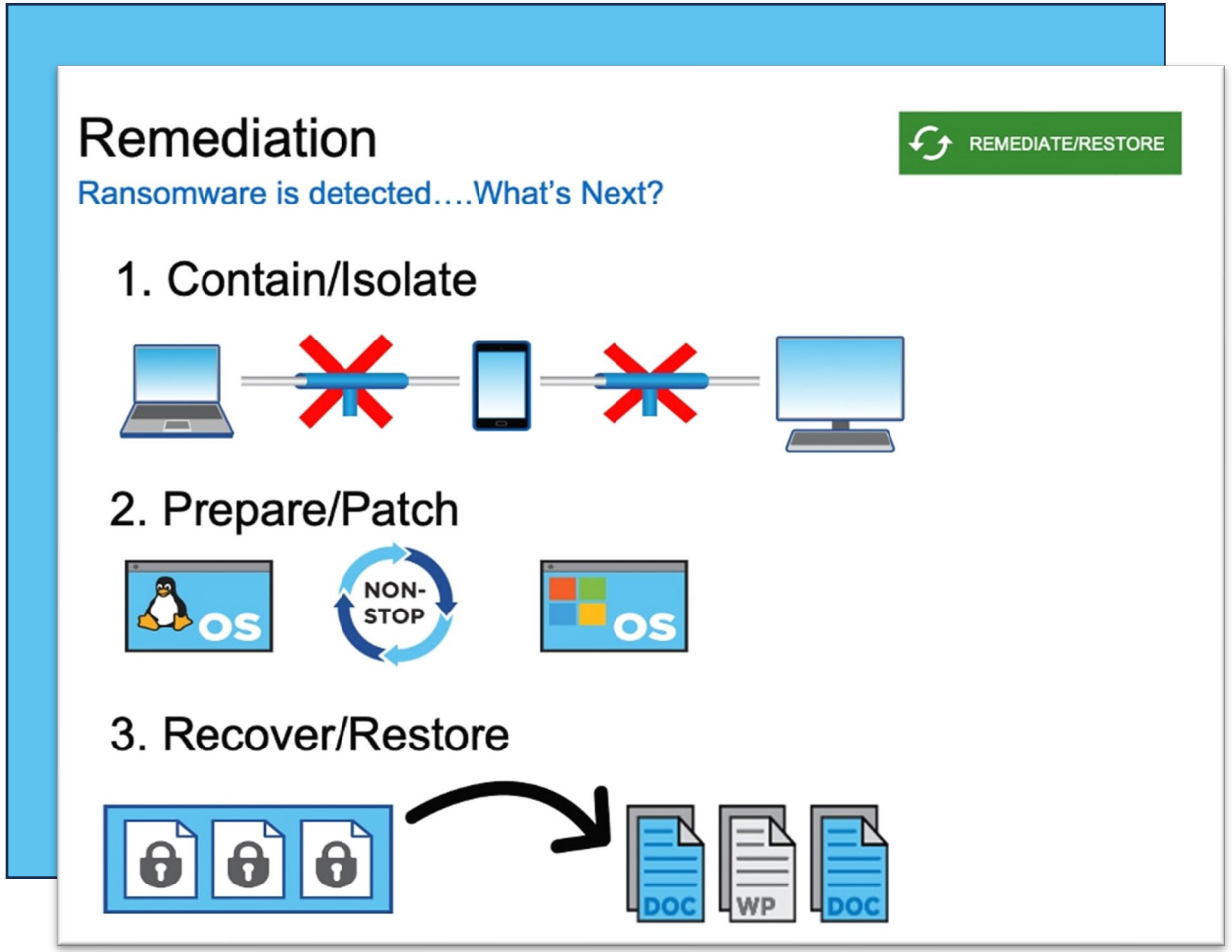
- Strange outbound network traffic
- Suspicious privileged account usage
- Logins at odd times from odd places
- New email rules created
- Staged data or large data transfers

…you might already be compromised.



Remediation and recovery

- Digital forensics = difficult and costly.
- Finding the initial vector of attack is important, but attribution probably not as important. Why?
- Better to focus on proactive measures.
- Assume all is lost; i.e., an attacker with privileged access could have found ways to persist.
- Only sure-fire method:
  - Low-level format of all storage media
  - Reinstall operating systems
  - Restore data from backups
- Then, install zero trust architecture.



Security rating report result category:

Email Security

Email authentication methods to prevent spammers and phishers from sending emails on behalf of a domain they don’t own.

- **SPF** = list of servers from which a domain sends emails.
- **DKIM** = digital signature on email to show it was sent from an authenticated server.
- **DMARC** = tells what to do if the email fails SPF or DKIM: deliver, quarantine, or reject; helps prevent spoofing by checking for domain alignment.

How to address phishing?

DNS authentication settings: keeping users from spoofing emails

Email security: blocking malicious email content, URLs, attachments

DNS filtering: blocking users from visiting malicious sites

Multifactor authentication: making it more difficult for attackers to compromise accounts than by just stealing passwords

Limiting exposure: avoiding posting sensitive internal information to social media and elsewhere

User awareness: educating users about the risks of phishing attacks and training them to identify and avoid such attacks

Continuous monitoring: looking for Indicators of Compromise (IoCs)

Digital risk monitoring: looking for compromised accounts, credentials, domain name typo-squatting, etc.

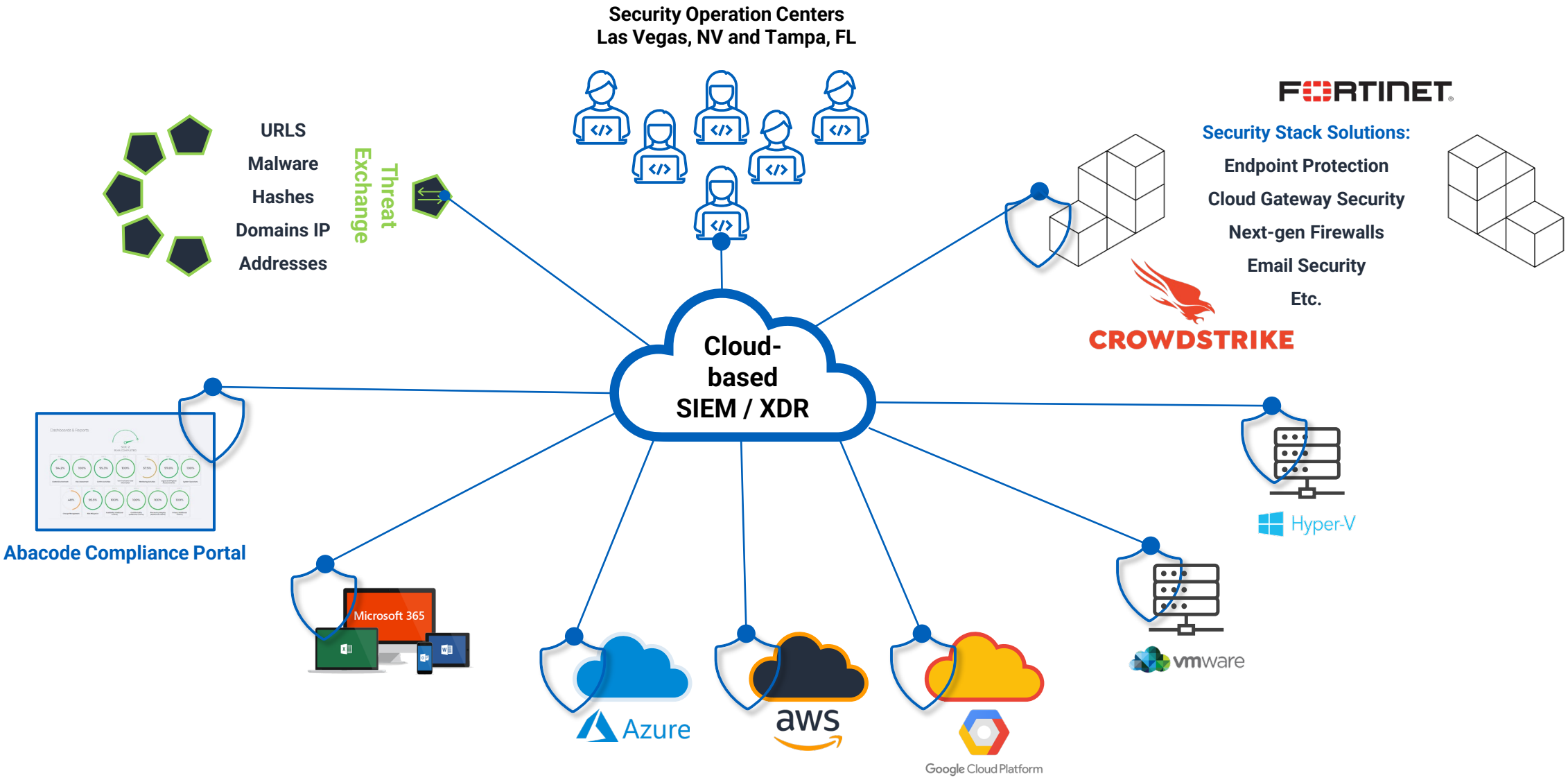
Security rating report result category:

Other components of a comprehensive program

The bottom line

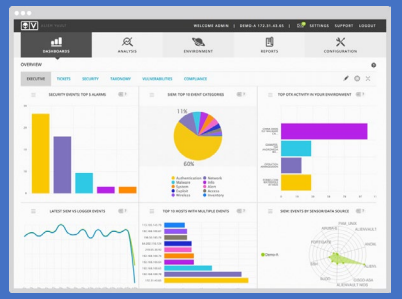
- Can’t depend on point solution
- Must have layers of security in place
- Align with best practices framework
- Identity and access management everywhere
- Network and logical segmentation
- Continuous monitoring and incident response

Continuous monitoring with Cloud-based SIEM/XDR Solution



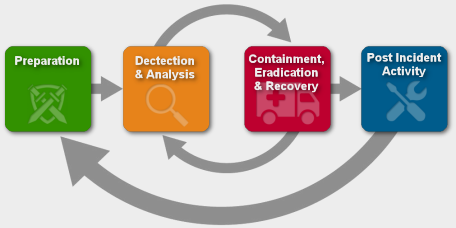
Continuous monitoring overview

Tier 1: Eyes-on-glass 24/7/365



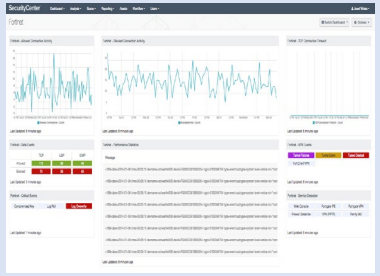
Initial analysis & triage

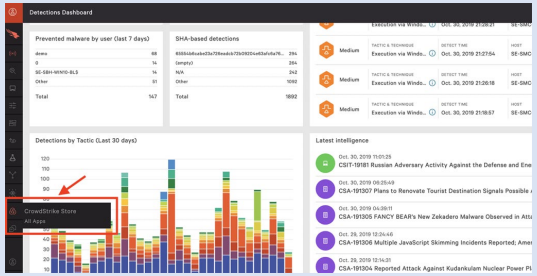
Tier 2: Escalations



Recommended actions & response

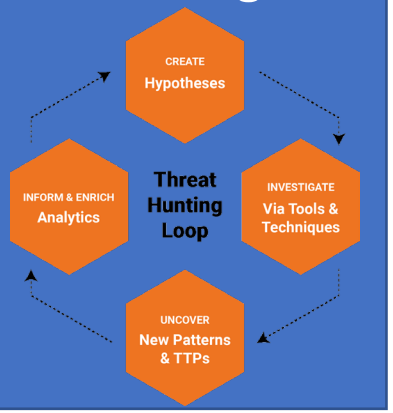
Tier 2: Active Response





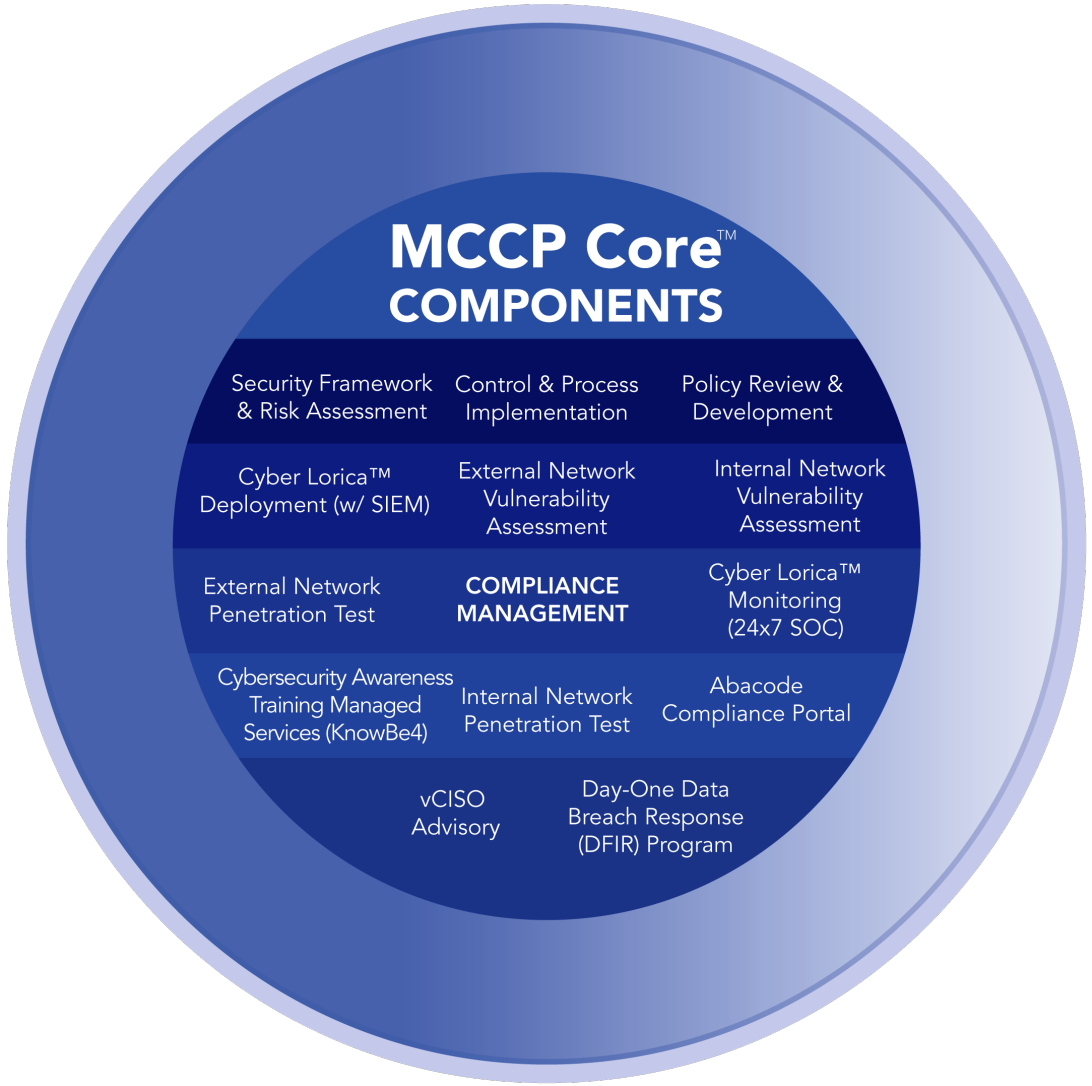
Managed response actions

Tier 3: Advanced Threat Hunting



Depends on complexity and potential impact

MCCP Core™: Continuous Cybersecurity & Compliance



Features:

- 24/7/365 “eyes on glass” MDR/XDR/EDR/SOAR, threat hunting, and compliance monitoring
- Integrated Portal - Compliance & Cybersecurity
- Consolidated reporting
- Mapped to critical compliance controls
- Turnkey program built for flexibility

Benefits:

- Compliance & cybersecurity integrated into ONE managed program
- Continuous cybersecurity & compliance monitoring
- Entire team of cybersecurity & compliance experts for a fraction of the cost
- Continuous compliance attestation for auditors, prospects, clients, partners, and supply-chain

One convenient monthly subscription fee

The proactive program that works like part of your team

Why Chunky™?

Problem:

Can’t cook
Don’t have time to cook
Expensive ingredients

Solution:

Quality / Taste / Satisfying
Already made for you
BOGO’s at Publix

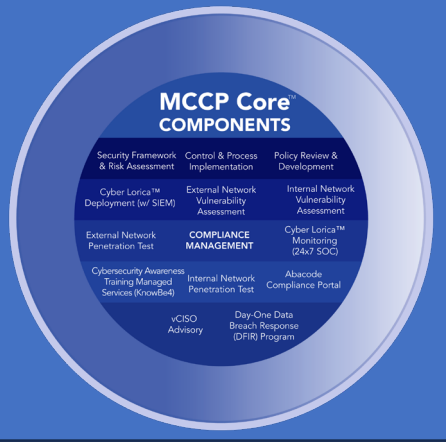
Why MCCP Core™?

Problem:

Don’t know how to do cyber/compliance
Don’t have time/bandwidth to do cyber/compliance
Expensive to hire full-time staff

Solution:

Has all the essential elements for success
Predictable spend, self-contained program
A fraction of the cost of hiring full-time staff



ASK ME ANYTHING!

Disclaimer

The information provided in these materials is intended to be general and advisory in nature. It shall not be considered legal advice. The Hartford does not warrant that the implementation of any view or recommendation contained herein will: (i) result in the elimination of any unsafe conditions at your business locations or with respect to your business operations; or (ii) be an appropriate legal or business practice. The Hartford assumes no responsibility for the control or correction of hazards or legal compliance with respect to your business practices, and the views and recommendations contained herein shall not constitute our undertaking, on your behalf or for the benefit of others, to determine or warrant that your business premises, locations or operations are safe or healthful, or are in compliance with any law, rule or regulation. Readers seeking to resolve specific safety, legal or business issues or concerns related to the information provided in these materials should consult their safety consultant, attorney or business advisors. All information and representations contained herein are as of March 2024.

The Hartford Financial Services Group, Inc., (NYSE: HIG) operates through its subsidiaries, including the underwriting company Hartford Fire insurance Company, under the brand name, The Hartford®, and is headquartered in Hartford, CT. For additional details, please read The Hartford's legal notice at www.thehartford.com