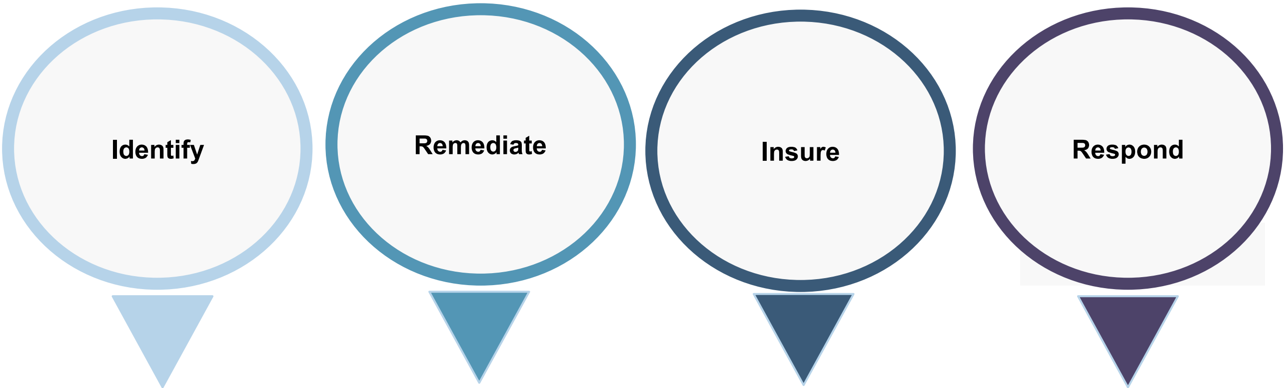
CyberTech Solutions – Email Security

Daniel Sliverman
Jeremy Rasmussen
Robert Lubin
November 30, 2023

The Hartford: Cyber Underwriting and Risk Mitigation

Cyber Risk Management Eco-System



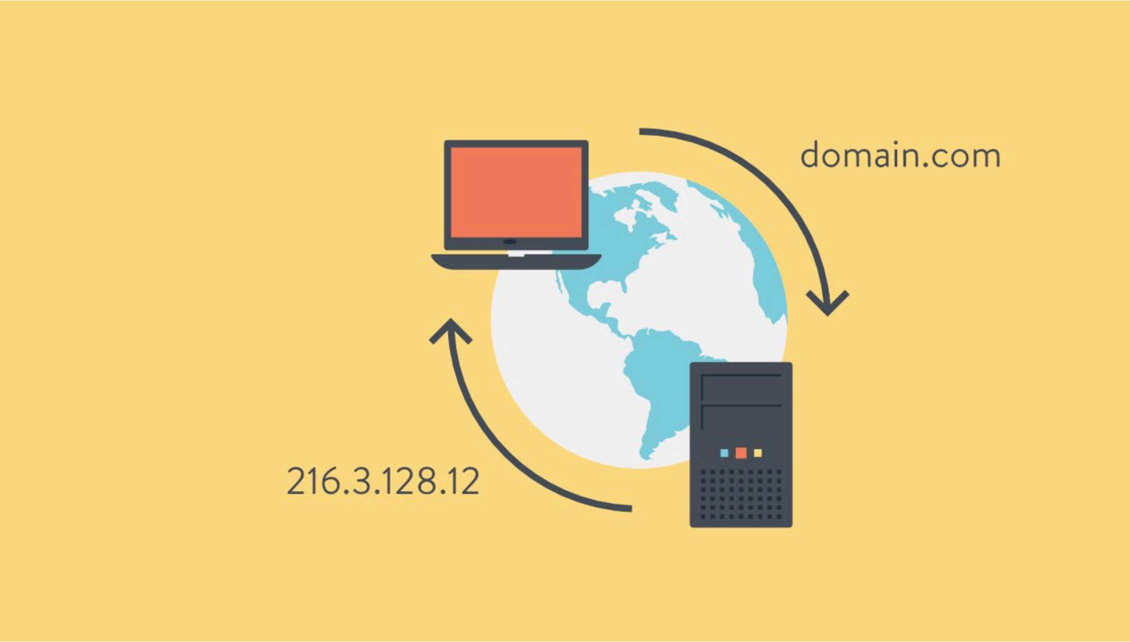
Bitsight **Abacode** **The Hartford** **First Responders**

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

Email security agenda

- Authentication methods: SPF, DMARC, and DKIM.
- Phishing attacks
- Encryption & signature
- Security solutions
- Continuous Monitoring & Incident Response

First, let's talk about DNS



- DNS = Domain Name System, a distributed database mapping hostnames (e.g., domain.com) to IP addresses (e.g., 216.3.128.12).
- To query a DNS record, open a command prompt and type:

  `nslookup` *`<name of domain>`*

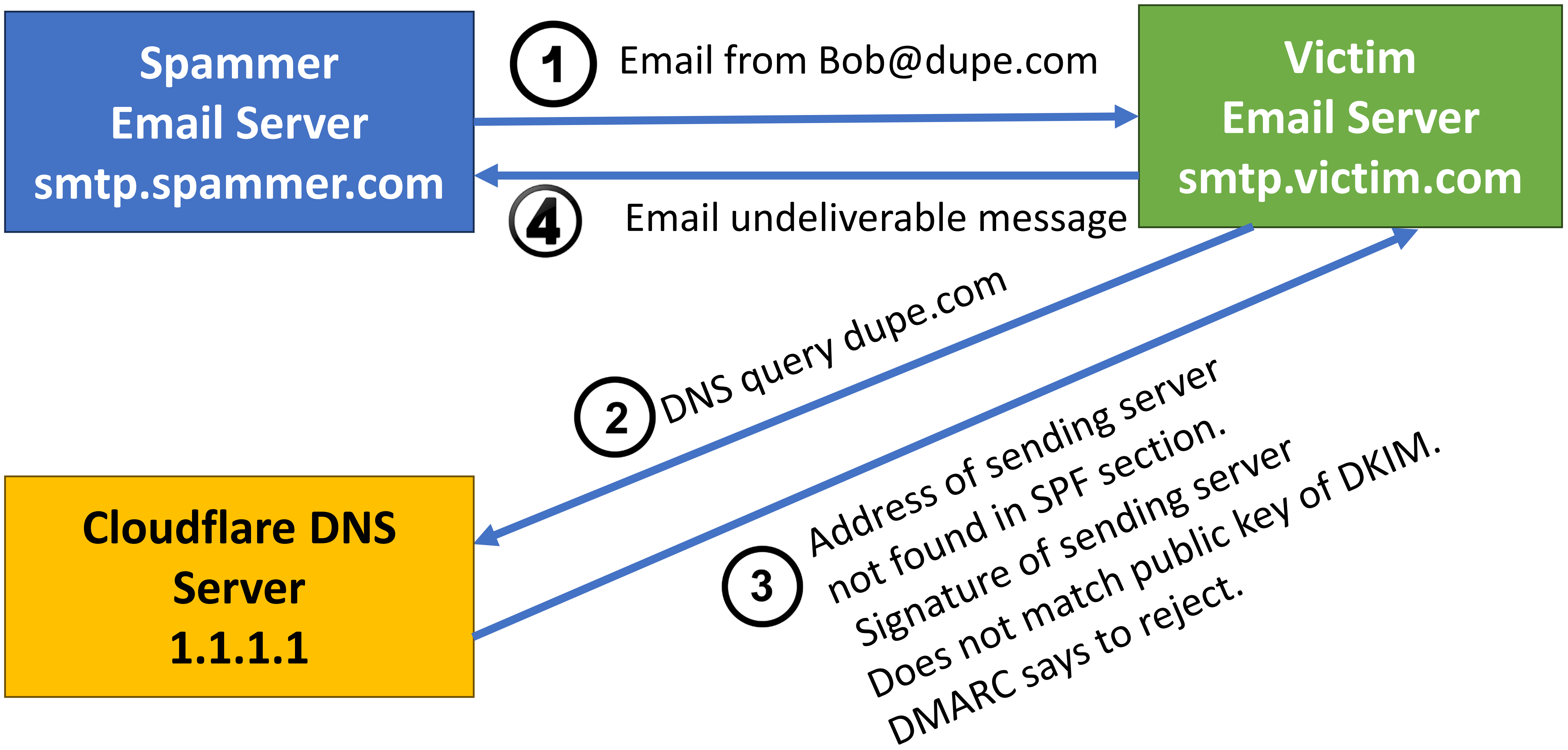
- DNS records also store lookup information about email, such as:
  - MX = mail server that accepts email on behalf of the domain
  - TXT = email security & authentication data

Alphabet soup: SPF, DKIM, and DMARC

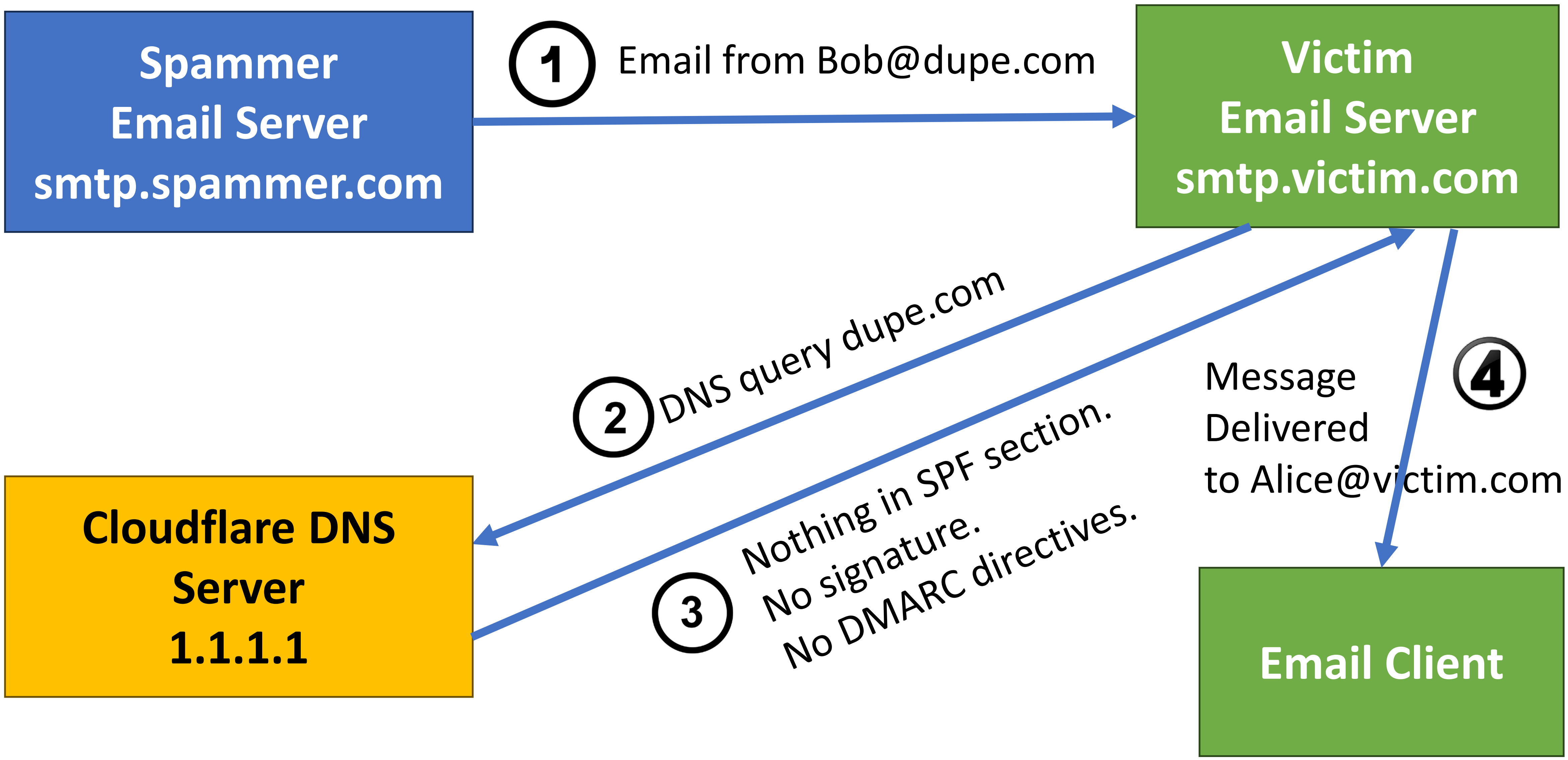
Email authentication methods to prevent spammers and phishers from sending emails on behalf of a domain they don’t own.

- **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.

Email authentication example



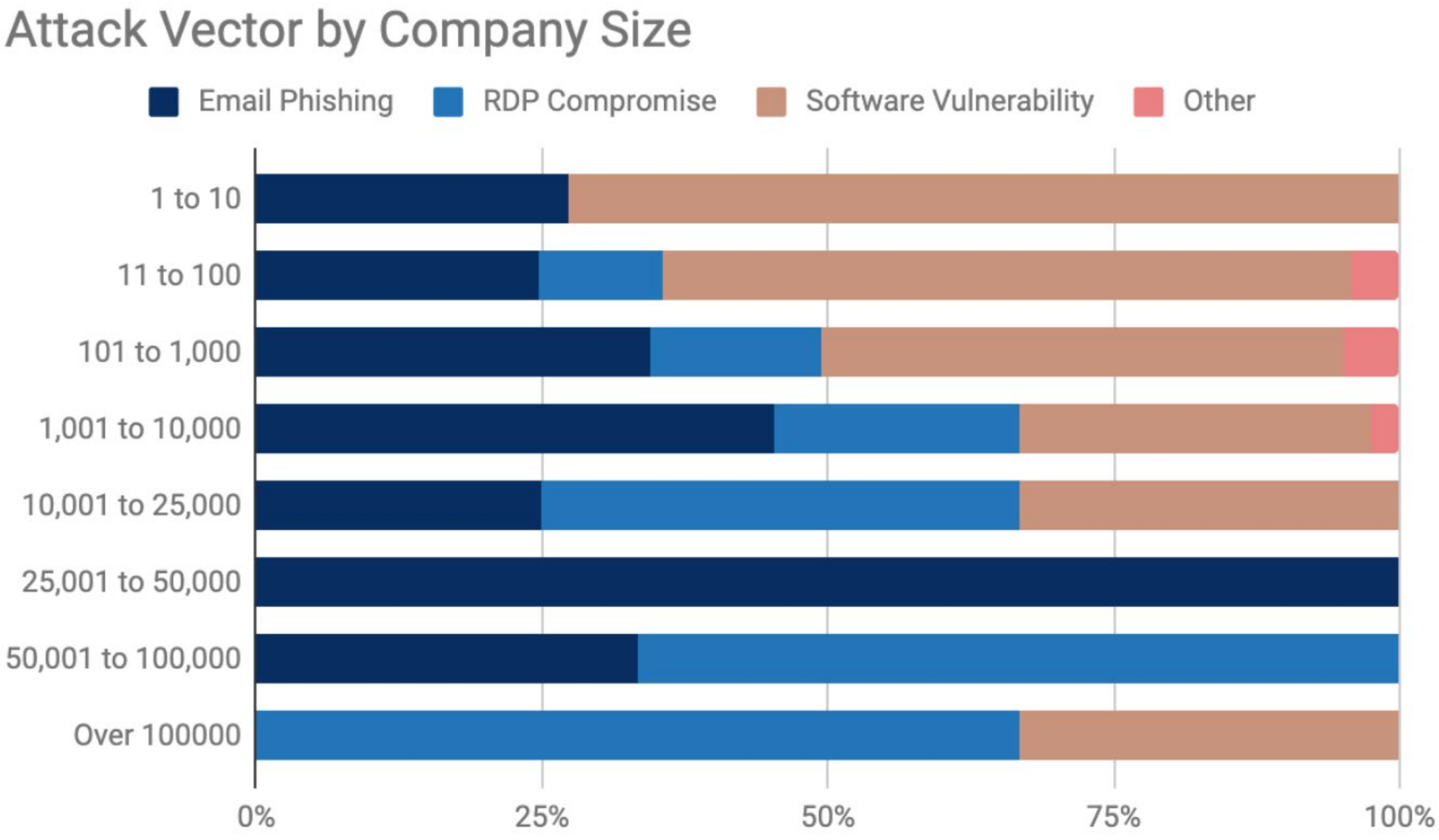
Email authentication example lacking DNS entries



POLL: What is the prevalent vector of ransomware attack for most organizations?

1. Application software vulnerability (missing patches)
2. Phishing/social engineering
3. Remote desktop misconfiguration

POLL answer: It depends!



Source: Coveware Ransomware Report October 2023

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

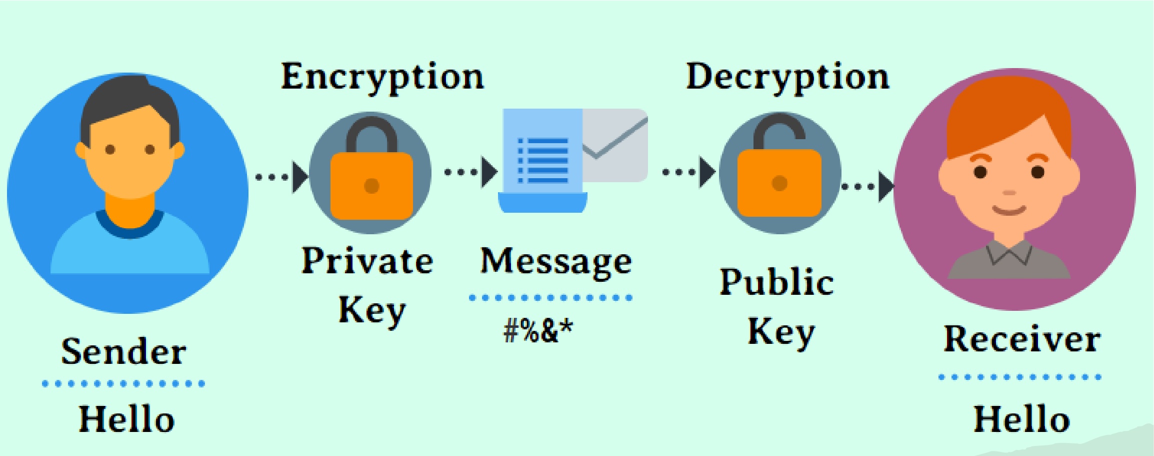
User awareness: educating users about the risks of phishing attacks and training them to identify and avoid such attacks

Continuous monitoring: looking for Indicators of Compromise (IoCs)

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

Email encryption

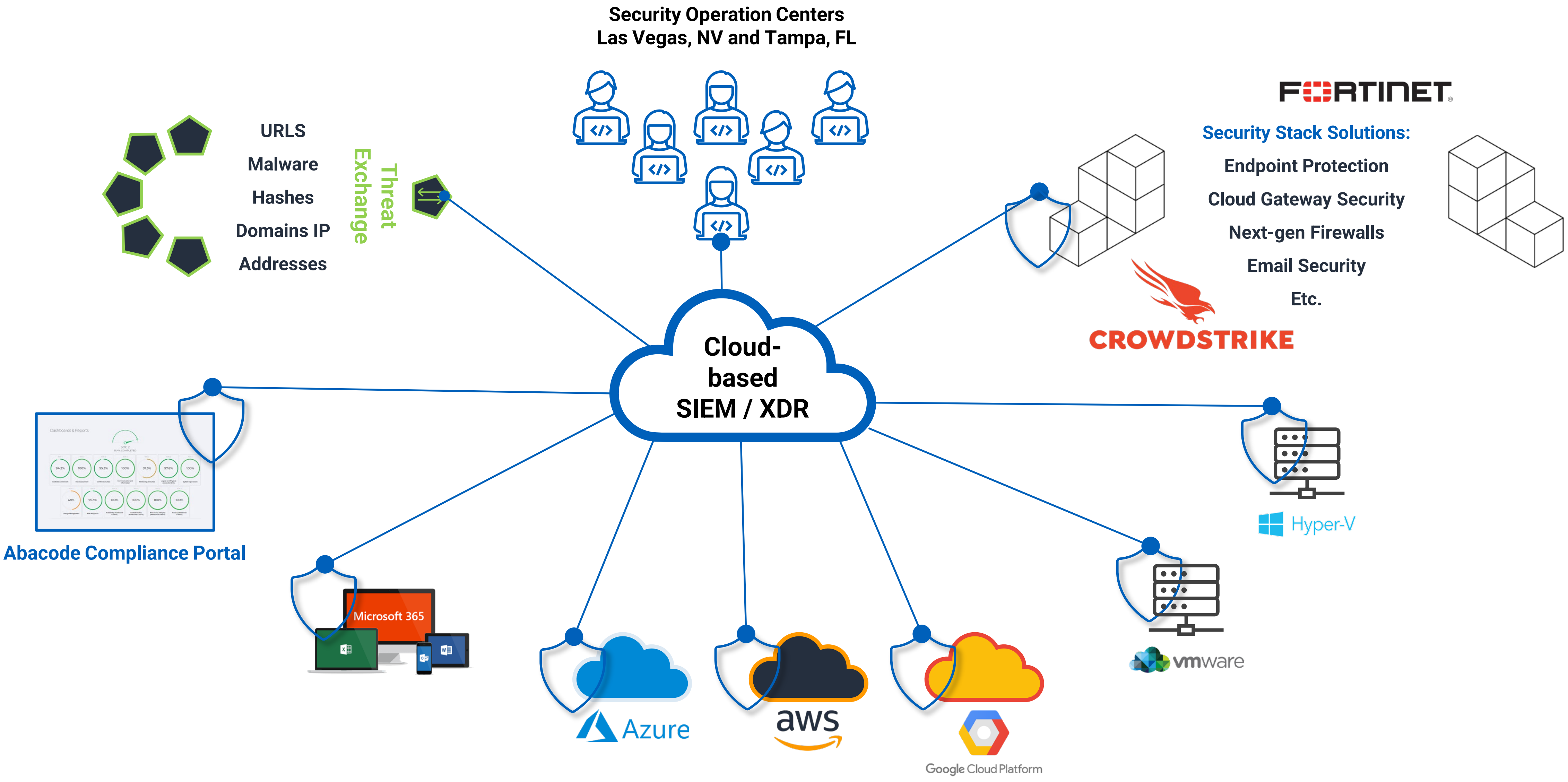
- **Encryption**: scrambling the contents of a message to keep it from being read by unauthorized parties (confidentiality)
- **Digital Signature**: using cryptographic methods to ensure message authenticity and integrity
- Email encryption and digital signatures can be implemented using various standards, such as S/MIME or OpenPGP.
- Many email clients, such as Microsoft Outlook, support these standards and provide built-in encryption and digital signature features. Many third-party solutions also available.



Email security solutions

- Some of the most popular: **Microsoft Defender for Office 365, Proofpoint, Mimecast, and Barracuda**
- All of these claim the following:
  - Cloud-based email security solution to provide protection against phishing, malware, and other email-based threats.
  - Use advanced machine learning algorithms and heuristics to identify and block malicious emails.
  - Provide built-in phishing simulation training to educate employees and senior leaders to decrease the chance of real-world attacks

Continuous monitoring with Cloud-based SIEM/XDR Solution



Cyber Lorica™ Security Events – Log Source Examples

On-Prem / Security

Cisco
Cisco Umbrella
Fortinet
Windows 10
Microsoft Windows Server 2019 Standard
Check Point Software Technologies Ltd
paloalto Networks®
Linux
macOS®

Public Cloud

IBM Cloud
Microsoft Azure
Google Cloud
aws

End Points

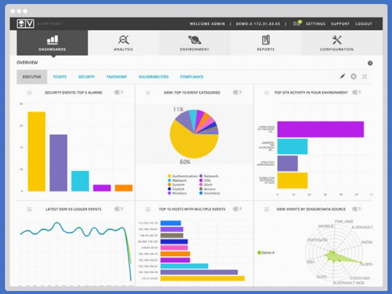
vmware® Carbon Black
Microsoft Defender for Endpoint
Built in. Cloud-powered.
SentinelOne®
SOPHOS
CROWDSTRIKE

SaaS

servicenow®
Google Workspace
Microsoft 365
okta
Jira
salesforce
DUO

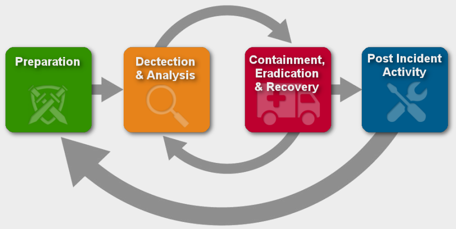
Continuous monitoring overview

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



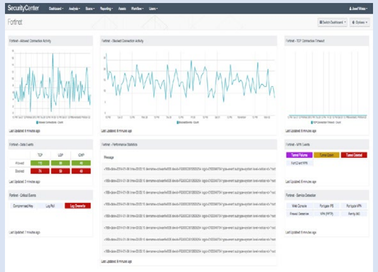
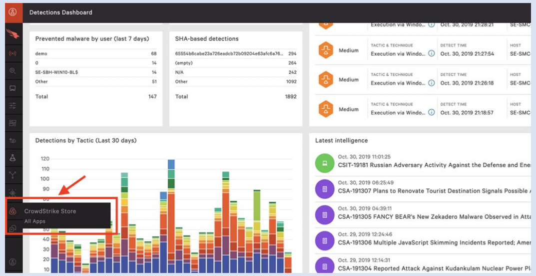

Initial analysis & triage

Tier 2: Escalations



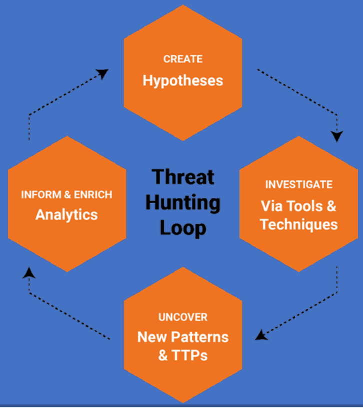
Recommended actions & response

Tier 2: Active Response

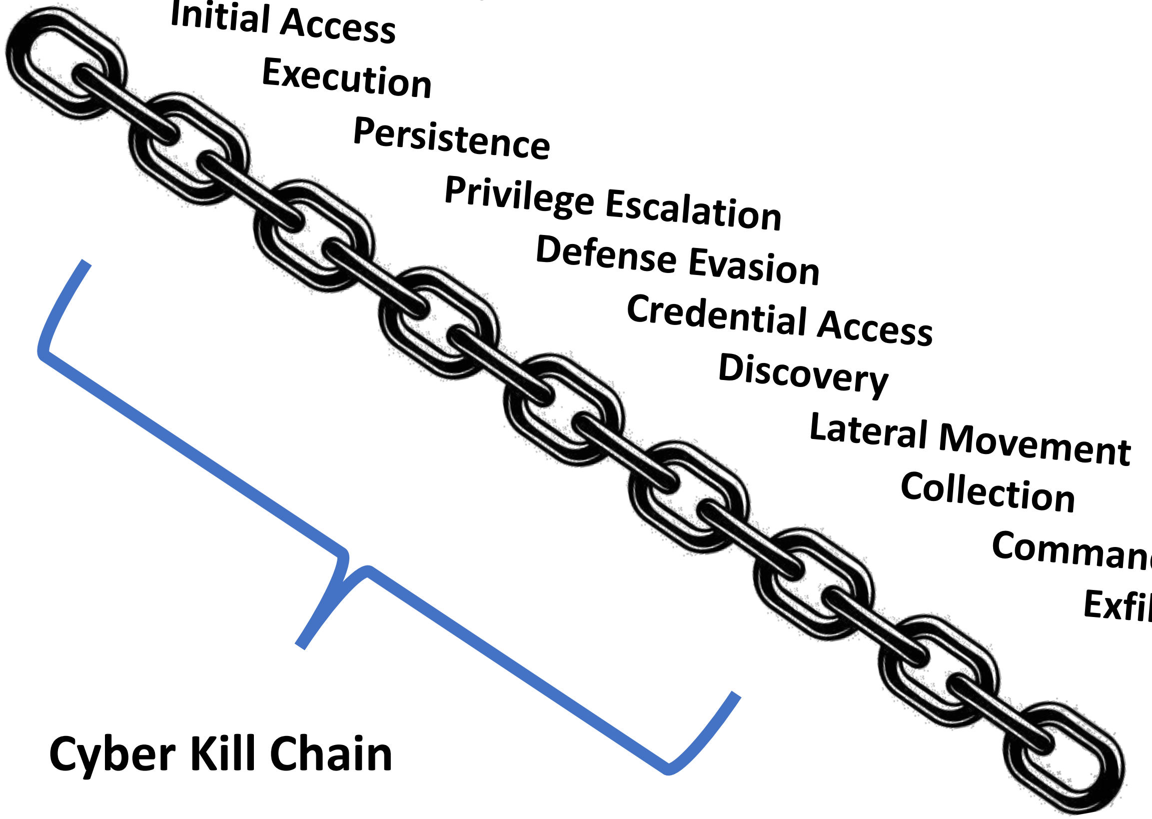
Managed response actions

Tier 3: Advanced Threat Hunting

Depends on complexity and potential impact

Deep-dive analysis, threat hunting, active response



The bottom line

- Can’t depend on point solution
- Must have layers of security in place
- Align with best practices framework
- Apply Zero Trust principles

ASK US 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 February 2023.

Certain coverages vary by state and may not be available to all businesses. All Hartford coverages and services described on this page may be offered by one or more of the property and casualty insurance company subsidiaries of The Hartford Financial Services Group, Inc. In Texas, Arizona, New Hampshire, Washington and California by Hartford Accident and Indemnity Company, Hartford Fire Insurance Company, Hartford Casualty Insurance Company, Hartford Lloyd's Insurance Company, Hartford Insurance Company of the Midwest, Navigators Insurance Company, Navigators Specialty Insurance Company, Maxum Casualty Insurance Company, Maxum Indemnity Company, Trumbull Insurance Company, Twin City Fire Insurance Company, Hartford Underwriters Insurance Company, Property and Casualty Insurance Company of Hartford and Sentinel Insurance Company, Ltd. and its property and casualty insurance company affiliates, One Hartford Plaza, Hartford, CT 06155.

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