# 2022 CHEMICAL SECURITY SUMMIT

August 23-25, 2022

#ChemicalSecurity

# CHEMICAL SECURITY SUMMIT

## CYBER RISK AND CYBER HYGIENE SERVICES

# What is Cybersecurity Risk?

**Cyber Risk:** The likelihood that any specific threat will exploit a specific vulnerability that causes harm as a result of the unauthorized disclosure, modification, or destruction of information or loss of information or system availability.

### Threat

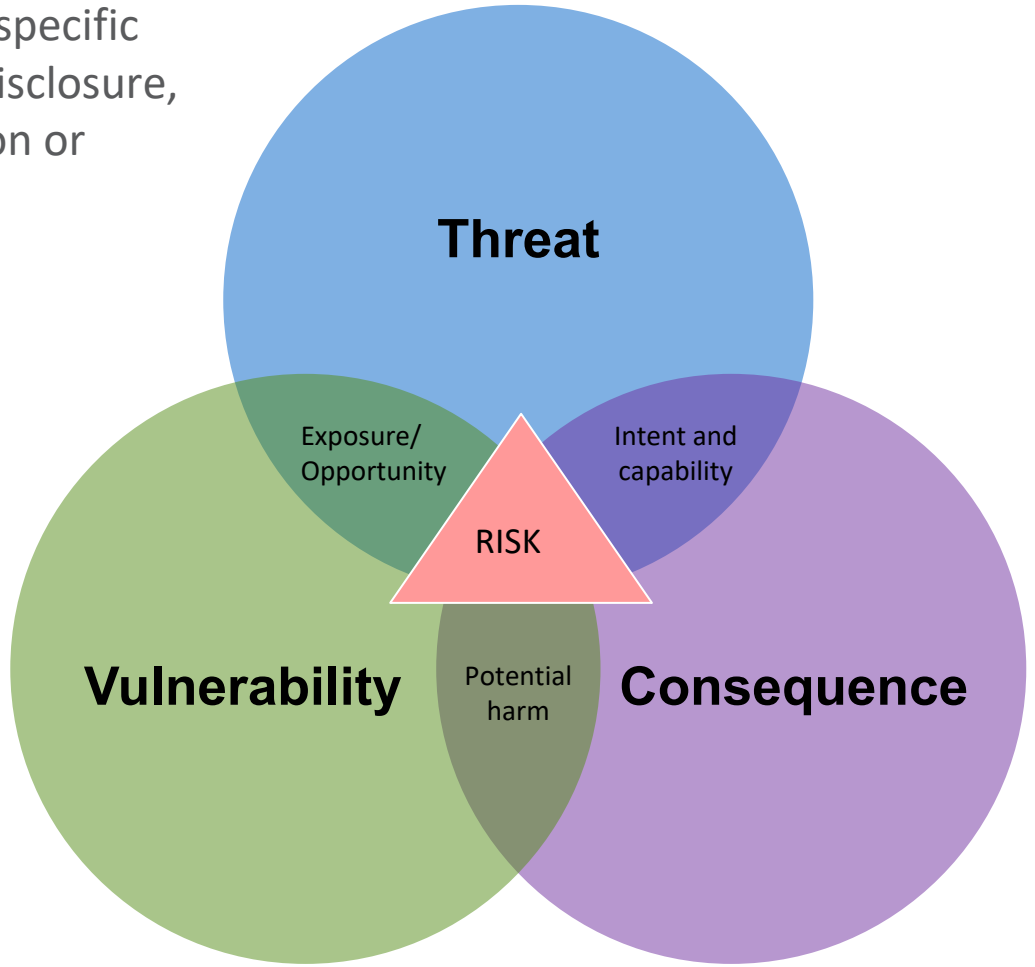
- People, programs, hardware, or systems with the intent, capability, and opportunity to exploit vulnerabilities

### Vulnerability

- A weakness in the information (IT) or operational (OT) technology infrastructure or any other aspect of an organization.

### Consequence

- Effect of an event, incident, or occurrence



# Threat Overview

**Threat Actors Targeting the Sector:**

- Nation-state APTs
  - Russia, China, Iran, North Korea
- Cybercriminals
- Business rivals and insiders

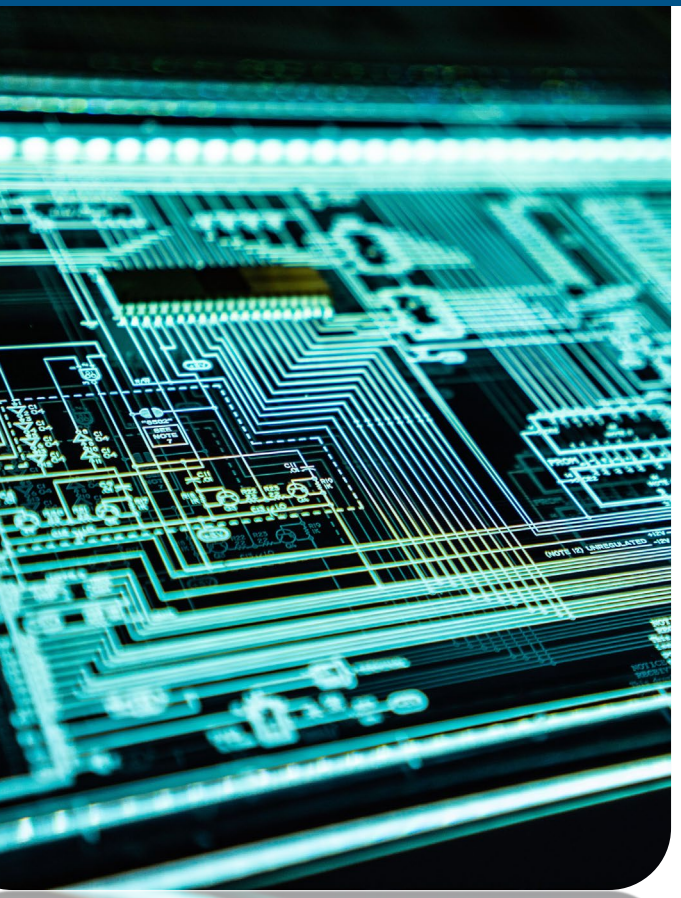
**Intent/Motives:**

- Espionage/national strategic value
- Monetary extortion
- Importance of specialty chemical and material producers in the global supply chain
- Cascading impacts a major cyber event within the chemical sector would likely cause

**Common Tactics Techniques and Procedures (TTPs)**

Targets of Opportunity | Phishing | Ransomware

# Consequences



Threat actors engage in targeted campaigns as well as indiscriminate vulnerability scanning for victims of opportunity to compromise IT and OT assets. Compromise of IT can indirectly affect or spread to OT if not contained.

2022 – North Korea-linked hacking campaign

- Using phishing emails sent from fake job recruiters targeted chemical companies in South Korea.

2021 – DarkSide Ransomware Campaign

- Three major international companies compromised
- One international company reportedly paid $4.4 million for 150GB of “sensitive data”
- Delays in productions and logistics and result in missed sales growth targets

2019 – LockerGoga Ransomware Campaign

- Affected two major US-based chemical companies
- Prevented access to IT systems and data and manufacturing was “not affected”
- Recovery involved ordering hundreds of new computers, and new email accounts

# Notable Cyber Events

Companies say hacker activity caused temporary production shutdowns

**Chemical distributor pays $4.4 million to DarkSide ransomware**

**The average cost of one cybersecurity incident in the industrial control system (ICS) and operational technology (OT) environment is $2,989,550.**

Ponemon Institute's 2021 State of Industrial Cybersecurity

**Lazarus group conducting cyber espionage against chemical sector, Symantec detects**

APRIL 18, 2022

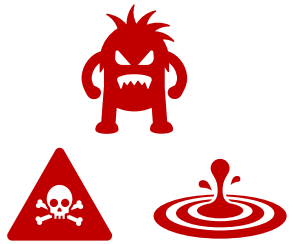
# Vulnerability and Opportunities for Compromise

- Phishing Susceptibility
- Exposed Common Vulnerabilities and Exposures (CVEs)
  - Known Exploited Vulnerabilities
  - Vulnerabilities with Exploits Available
  - Critical and High Severity CVEs
- Prolonged windows of vulnerability exposure
- Exposed vulnerable services and protocols that can facilitate compromise (e.g., RDP)
- End of support and out of date operating systems and software

# A More Proactive, Less Reactive Approach

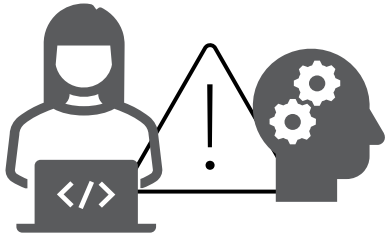
Leverage known threat and consequence information to proactively identify vulnerability exposure among entities and sectors that support national critical functions and provide vulnerability and risk intelligence that enables action to reduce cybersecurity risk.

**BE AWARE OF**



KNOWN THREATS
AND CONSEQUENCES

**IDENTIFY AND ANALYZE**



KNOWN IT AND OT
VULNERABIITY EXPOSURE

**TAKE ACTION**

REDUCE CYBERSECURITY RISK

# Informed Attack Surface Analysis and Vulnerability Hunting

## Objectives

- ✓ Proactively “hunt” and identify known exploited or targeted vulnerabilities
- ✓ Discover sector or regional concentrations of vulnerabilities
- ✓ Identify historical and emerging vulnerability patterns and trends
- ✓ Analyze and compare threat actor and VM Assessments TTPs
- ✓ Detail implications for national critical functions and national security
- ✓ Understand historical incidents to project outcomes and recommend courses of action
- ✓ Notify stakeholders and affected entities of the likely exposure
- ✓ Engage and provide exposed entities with recommendations to mitigate or remediate vulnerabilities

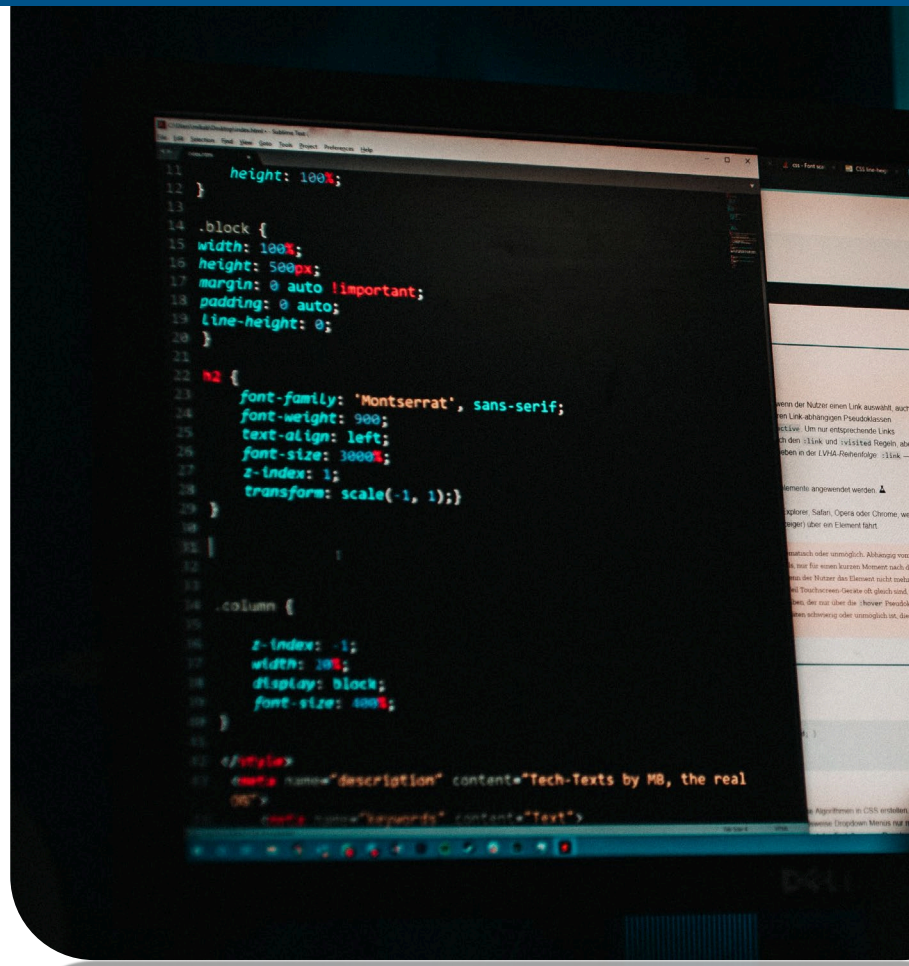
**Concept**: Insights drawn from proactive identification of vulnerabilities within the stakeholder landscape (ecosystem) that may significantly impact a critical infrastructure sector or national critical function if targeted and compromised.

**Goal:** Inform CISA leadership, policymakers, and cybersecurity community partners of active and strategic national cybersecurity vulnerability concerns.

# Identifying External Vulnerability Exposure

If vulnerabilities are exposed to the internet, adversaries can see them.

- Maintain awareness of threat activity and intelligence
- Monitor CVE and ICS-CERT advisories for disclosures
- Leverage open-source search engines (e.g., Shodan, Censys) that can be used to identify IT and OT targets
- Analyze findings from CISA's Cyber Hygiene and commercial vulnerability scanning services to determine vulnerability exposure of IT assets



# Cyber Hygiene Findings in the Chemical Sector

Chemical Sector entities are operating with internet-accessible products, applications, and software that possess vulnerabilities that are actively exploited by threat actors to compromise both public and private entities. These vulnerabilities impact IT assets but there is a roughly even chance that their compromise could spread to OT environments, if not contained, according to analysis of CISA data and open-source research.

- Analysis is derived from the cybersecurity vulnerability information received through the CISA Cyber Hygiene (CyHy) Vulnerability Scanning (VS), Web Application Scanning (WAS) services, Phishing Campaign Assessments (PCA).

CISA offers free services to enable Chemical Sector entities to reduce their internet accessible attack surface. Email vulnerability_info@cisa.dhs.gov for more information and to sign up.

# Reduce Cyber Risk through CISA Services

***Chemical Sector enrollment in CyHy VS increased by 47% from August 2021 to August 2022.***

CISA offers free cybersecurity services to Chemical entities:

- **Vulnerability Scanning**: Chemical entities can identify vulnerabilities and enable their remediation through persistent scanning of internet-accessible systems for weaknesses, configuration errors, and suboptimal security practices.
- **Web Application Scanning**: Chemical entities can assess the "health" of publicly accessible web applications by checking for known vulnerabilities and weak configurations.
- **CISA Assessments**: Chemical entities can enroll in cybersecurity assessments (e.g., penetration testing, and phishing campaign assessments) that provide actionable and tailored risk-informed recommendations.

Email vulnerability_info@cisa.dhs.gov for more information and to sign up.

# Exposed Known Exploited Vulnerabilities

CISA maintains a Known Exploited Vulnerabilities (KEVs) catalog, which identifies a subset of CVEs that are actively used to compromise systems. CISA urges Chemical entities to remediate KEVs as soon as possible after identification to decrease risk of compromise.

KEVs provide adversaries with opportunities to exploit internet accessible hosts and systems that can enable a network-wide compromise through remote code execution, cross site scripting (XSS), authentication by-pass, and information disclosure.

KEVs are used to exploit public and private organizations and are a frequent attack vector for malicious cyber actors of all types. CISA maintains a catalog of KEVs that carry significant risk to Federal agencies and public and private sectors entities: **cisa.gov/known-exploited-vulnerabilities/**

# Common Vulnerabilities of Concern

## Deprecated encryption protocols

Deprecated encryption protocols increase threat actor ease of compromise, especially when exposed for extended periods of time.

- Encryption weaknesses can be due to due to insecure use of TLS, SSL, and SSH protocols.

## Exposed unsupported Windows OSs and other legacy systems

Use of unsupported Windows OSs (Windows 7, Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008)—or other unsupported OSs—exposes an entity to dozens of known and more of unknown or unreported vulnerabilities for unsupported OS that leave organizations and users at risk because vendors cease software security updates.

- According to industry analysis, approximately 95% of ransomware malware identified by VirusTotal targets Windows operating systems, which leaves entities using and exposing unsupported versions to the internet inherently vulnerable.

## Vulnerabilities with exploits available

Vulnerabilities with an exploit available have a tool, script, and/or malware developed against it that enables a threat actor to engage in exploitation of the vulnerability and potentially compromise entities.

# Exposed Vulnerable Services

Services such as SMB, NetBIOS, Kerberos LDAP, and Telnet should never be exposed to the internet and require immediate remediation. Other services should not be exposed to the internet unless there is a valid business use case and appropriate mitigations, such as a read-only configuration for File Transfer Protocol (e.g., SFTP), and continuous monitoring for suspicious activity are in place. Exposed services like FTP, Remote Desktop Protocol (RDP), Telnet, and others enable threat actors to spread malware, including ransomware, gain initial access on victim's networks, exfiltrate sensitive data, and use other known tactics that enable network compromise.

- Organizations should be cognizant of exposing significant encryption vulnerabilities in their email services (SMTP, POP3, and IMAP). Maintaining securely configured email services is critical to protect against business email compromise.
- Exposure of vulnerabilities in Domain Name Services (DNS) increase risk for organizations. DNS servers provide critical network function of mapping IP addresses and domain names, which if compromised by adversaries, could result in denial of service, re-directing user browsing to malicious web sites; and information disclosure of sensitive network information that can be leveraged for reconnaissance.

**Examples of Vulnerable Services**

| | |
|---|---|
| **FTP** | **Kerberos** |
| **RPC** | **SQL** |
| **RDP** | **NetBIOS** |
| **LDAP** | **SMB** |
| **Telnet** | **IRC** |

*CISA's CyHy Vulnerability Scanning routinely reports on exposure of vulnerable services that increase the risk of compromise.*

# Web Application Vulnerabilities

CISA observed a prevalence of vulnerabilities that are due to insecure web applications that are exposed to the internet, according to analysis of CyHy VS and WAS.

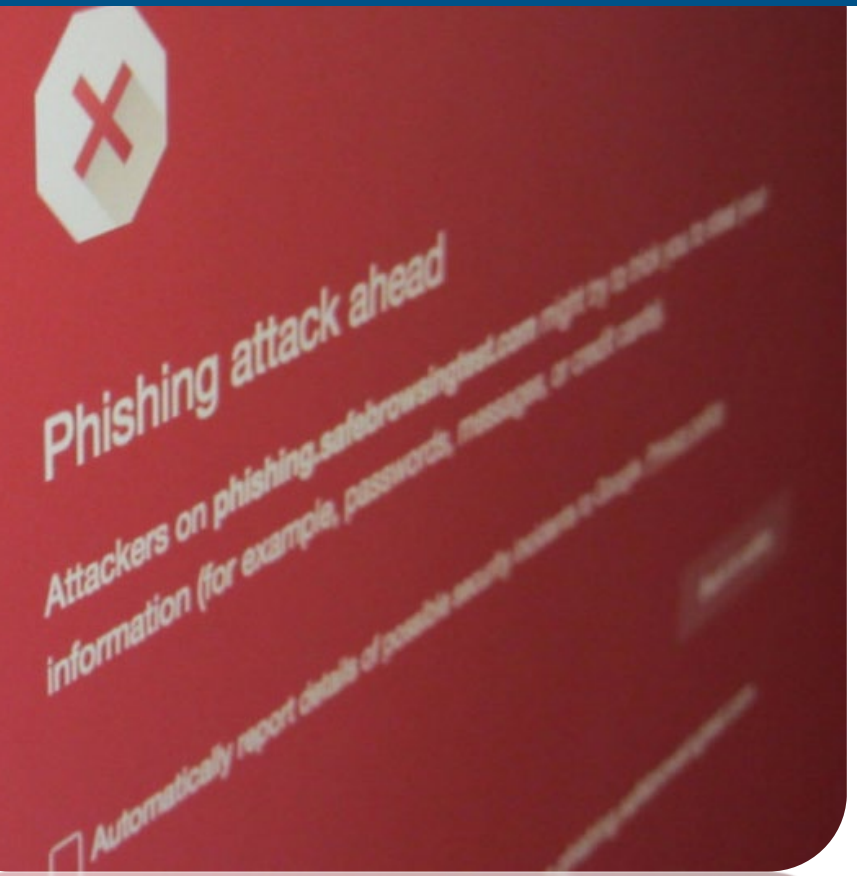
- The most frequently WAS observed weaknesses were due to encryption weaknesses, which can enable adversaries to:
  - Capture valid accounts and credentials
  - Capture critical and sensitive network information through information disclosure and adversary-in-the-middle attacks.
- Broken access control, outdated components, and security misconfigurations were also frequently observed and supported by analysis of CyHy VS.

# Vulnerability Remediation Timeliness

Threat actors are almost certainly increasing time to exploit vulnerabilities of interest. Industry analysis suggests **that attackers typically start scanning for vulnerabilities within 15 minutes of a CVE being disclosed**. Threat actors are also continuing to exploit older unpatched vulnerabilities that almost certainly provide known avenues to compromise Chemical entities.

- Chemical entities that delay remediation of KEVs and critical and high severity vulnerabilities provide extensive windows of exposure for threat actors to exploit high-consequence vulnerabilities.
- Prioritization, based on contextual factors, aligns with the Stakeholder-Specific Vulnerability Categorization (SSVC) model, which considers exploitation as one of the factors entities should consider in the management and prioritization of active vulnerabilities.

# Phishing and Social Engineering Weaknesses



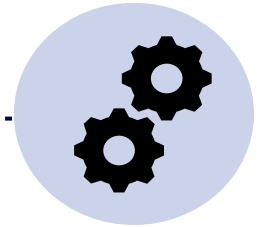

Successful phishing may provide threat actors initial access into a network and can lead to a multitude of damaging consequences for the victim and third parties including but not limited to data breach and data loss, malware infection, and ransomware.

- CISA's analysis of phishing assessments indicates that eight out of every ten entities had at least one individual that falls victim to a phishing attempt.
- Only a few of targeted employees report phishing attempts, which limits the organization's ability respond to the intrusion and alert others to the threat.
- Within the first 10 minutes, many successfully phished individuals click the link, taking the bait, by replying with sensitive information or clicking on a spoofed link or attachment.

Usage of multifactor authentication (MFA) can counter sophisticated phishing attacks and prevent adversary take-over of accounts due to successful phishing and credential theft.

Configuring email servers to utilize protocols designed to verify the legitimacy of email communications, like Sender Policy Framework (SPF), Domain Keys Identified Message (DKIM), or Domain-Based Message Authentication, Reporting and Conformance (DMARC), can help reduce the likelihood of a successful phishing attack.

# Actions to Reduce Cyber Risk

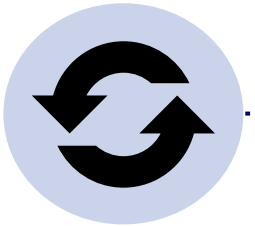


## Routinize Vulnerability Management

- Implement policy to ensure timely patch cycles for all priority applications, and to handle out-of-cycle patching for potentially high-impact vulnerabilities, like KEVs.
- Routinely revalidate secure configurations of system and web applications.
- Maintain and practice incident response procedures to limit impact and remediate malicious activity.

## Reduce Phishing

- Provide user training on phishing detection, reporting, and response.
- Implement reporting procedures for both suspected phishing attempts and verified incidents.
- Implement strong border, host, and end-point protection services as initial barriers to reduce the impact and likelihood of a successful phishing attempt.
- Enforce MFA to secure accounts and resources.



## Maintain Updates

- Inform leadership of the risks associated with operating unsupported software to balance the potential impact.
- Plan for software end of life to allow sufficient time and resources towards migrating to a new version.
- Implement additional security measures for any unsupported software unable to be transitioned out, including segmentation from the corporate network and limiting cross-communications.

## Minimize Vulnerable Service Exposure

- Disable or block unnecessary remote access.
- If business operations require exposure, prioritize patching and updates for timely mitigation of known vulnerabilities on exposed services.
- Implement MFA solutions for all remote access and secure connections by following vendor guidance to configure encryption protocols, or by utilizing a VPN solution.

# Services and Resources

- Cyber Hygiene Services
- CISA's Get Your Stuff off Search
- CISA's Known Exploited Vulnerability Catalog
- CISA's ICS CERT Advisories
- Stopransomware.gov
- Prioritizing Vulnerability Response (Stakeholder Specific Categorization)
- CISA's ICS Infographic


**Cybersecurity Division | Vulnerability Management**

Cyber Risk Summary Questions and Feedback:

CSD_VM_Insights_Intake@cisa.dhs.gov

Cyber Hygiene Services:

https://www.cisa.gov/cyber-hygiene-services

vulnerability_info@cisa.dhs.gov