Practical Cybersecurity Defenses

Frank Harrill

WSU CySER Seminar

March 18, 2025

Discussion Topics

- Threat Landscape Overview
- Risk Assessment and Management
- Use of Security Frameworks and Standards
- Incident Response Planning and Execution
- Employee Training and Awareness
- Advanced Defense Mechanisms
- Insider Threat Mitigation
- Real-World Examples

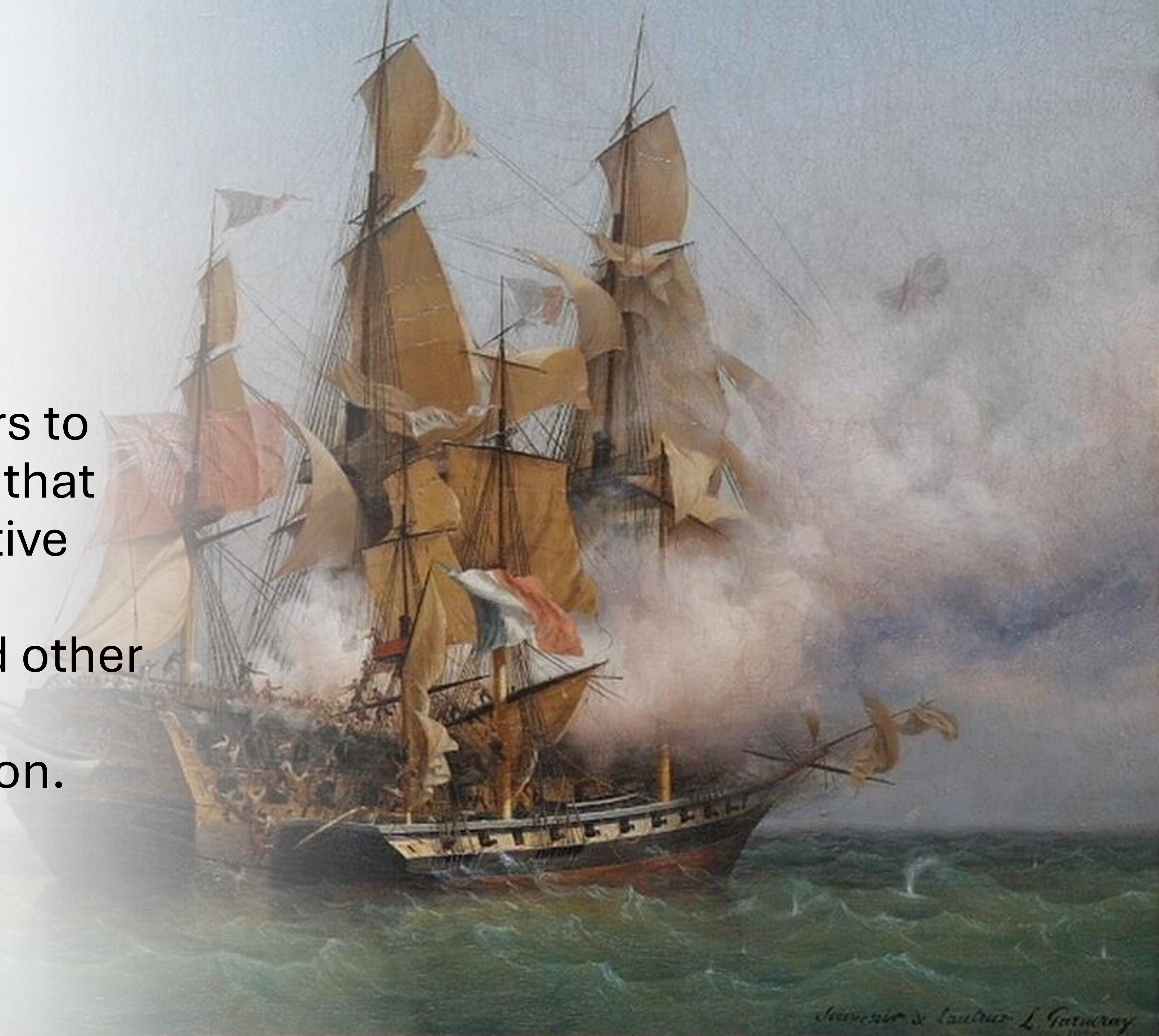
The concepts of deny-by-default, least privilege, and need-to-know should underpin any security program.

The trust we place in each other can be weaponized if fundamental safeguards are not present.

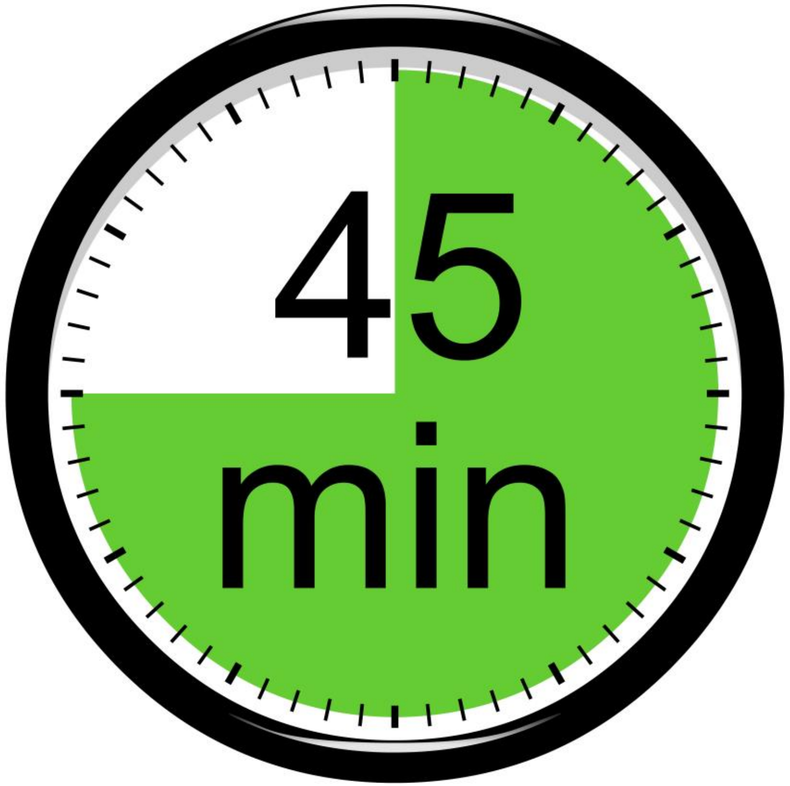
We are all prime targets.

A Return to Privateering

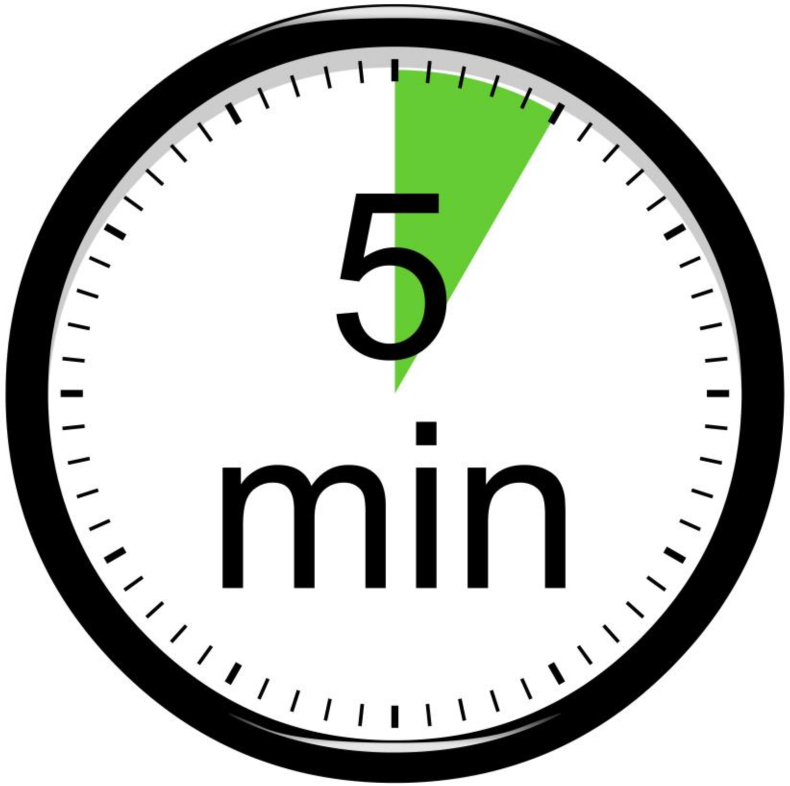
The use of criminal actors to launch crippling attacks that permit the theft of sensitive technical data by hostile intelligence services and other nation-state adversaries demands our full attention.



Attacks are nearly instant

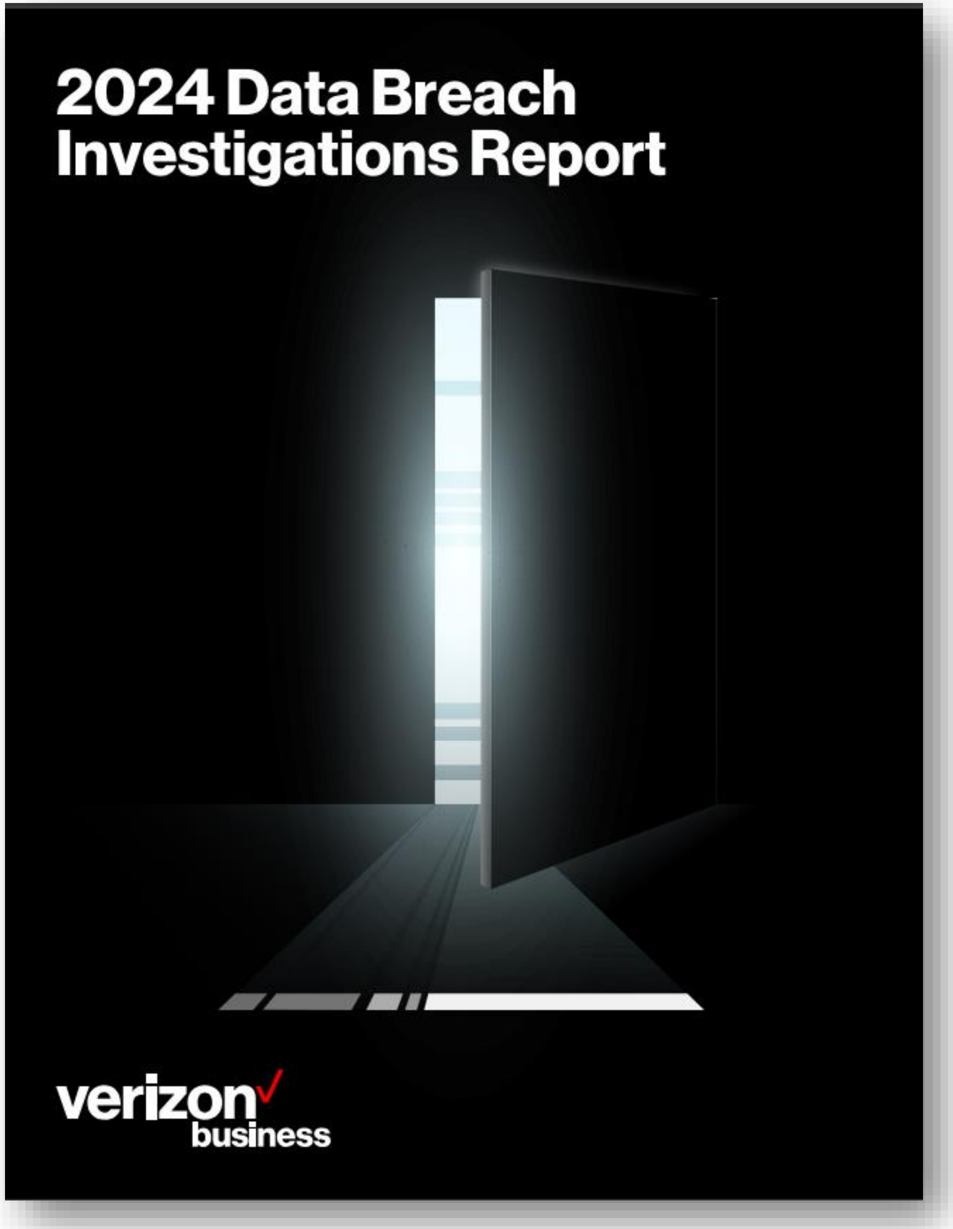


2013



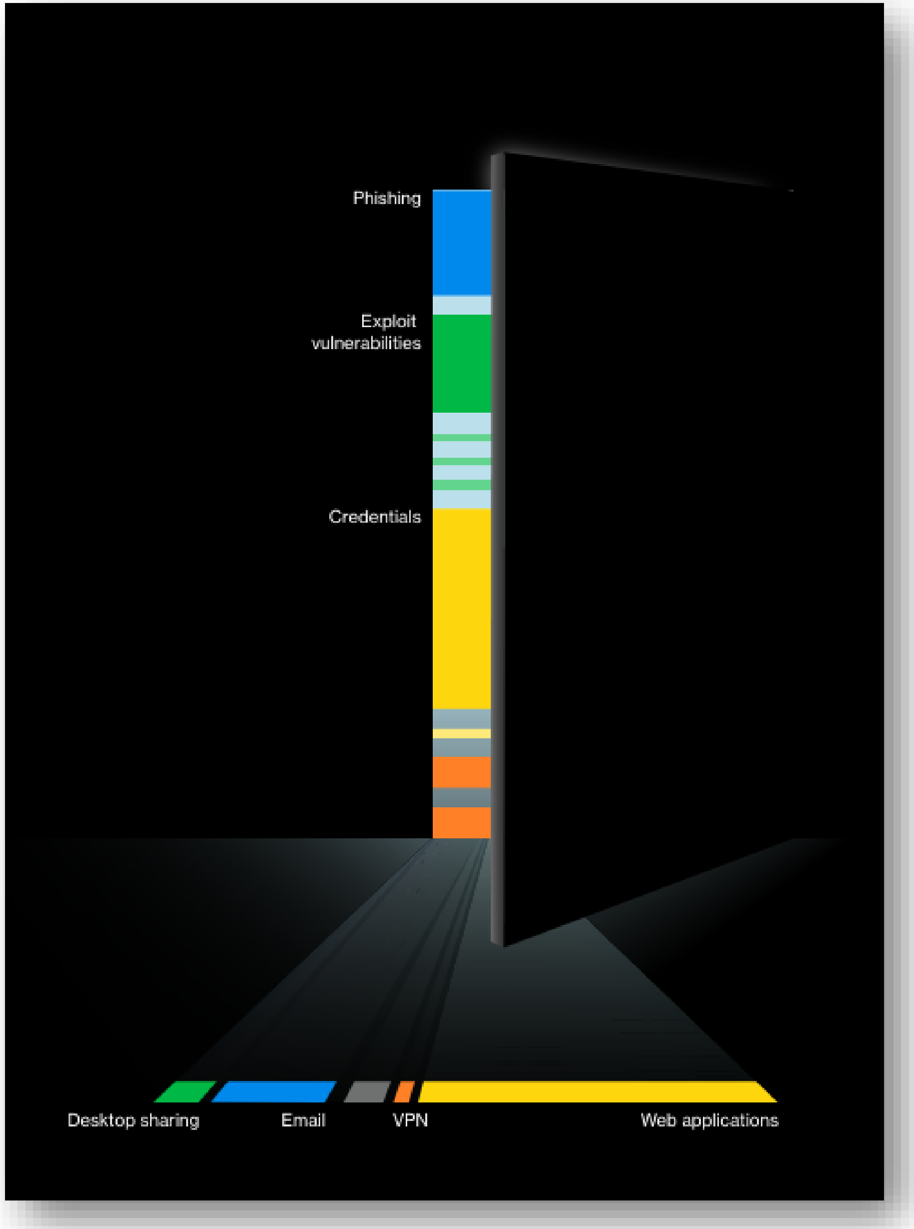
Today

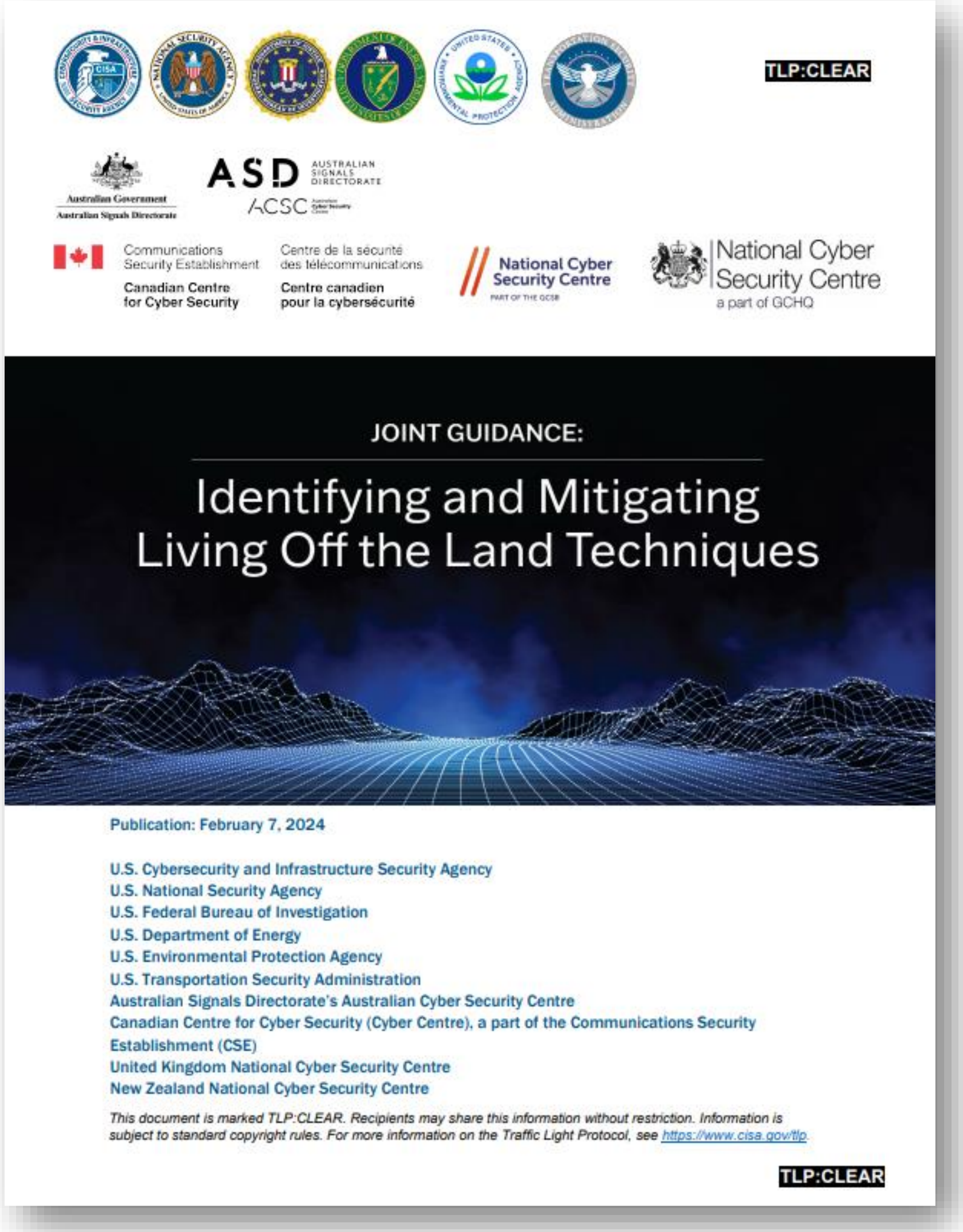
Most intrusions begin with stolen or reused passwords.



2024 Data Breach Investigations Report

verizon business





TLP:CLEAR
Australian Government
Australian Signals Directorate
ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC
Communications Security Establishment
Centre de la sécurité des télécommunications
Canadian Centre for Cyber Security
Centre canadien pour la cybersécurité
National Cyber Security Centre
PART OF THE GCSB
National Cyber Security Centre
a part of GCHQ

JOINT GUIDANCE:

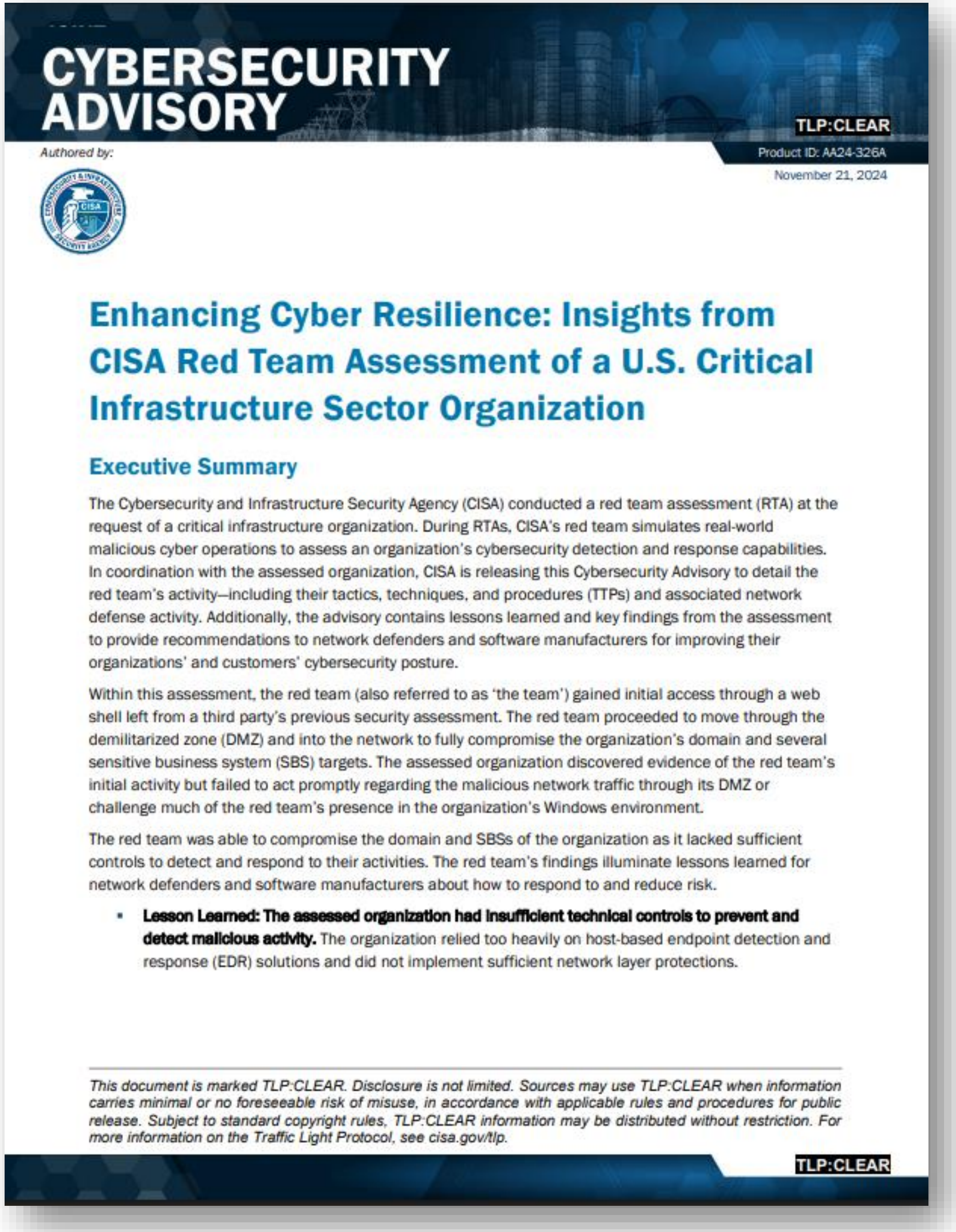
Identifying and Mitigating Living Off the Land Techniques

Publication: February 7, 2024

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
U.S. Federal Bureau of Investigation
U.S. Department of Energy
U.S. Environmental Protection Agency
U.S. Transportation Security Administration
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security (Cyber Centre), a part of the Communications Security Establishment (CSE)
United Kingdom National Cyber Security Centre
New Zealand National Cyber Security Centre

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

TLP:CLEAR



CYBERSECURITY ADVISORY

TLP:CLEAR

Authored by:

Product ID: AA24-326A

November 21, 2024

Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a U.S. Critical Infrastructure Sector Organization

Executive Summary

The Cybersecurity and Infrastructure Security Agency (CISA) conducted a red team assessment (RTA) at the request of a critical infrastructure organization. During RTAs, CISA's red team simulates real-world malicious cyber operations to assess an organization's cybersecurity detection and response capabilities. In coordination with the assessed organization, CISA is releasing this Cybersecurity Advisory to detail the red team's activity—including their tactics, techniques, and procedures (TTPs) and associated network defense activity. Additionally, the advisory contains lessons learned and key findings from the assessment to provide recommendations to network defenders and software manufacturers for improving their organizations' and customers' cybersecurity posture.

Within this assessment, the red team (also referred to as 'the team') gained initial access through a web shell left from a third party's previous security assessment. The red team proceeded to move through the demilitarized zone (DMZ) and into the network to fully compromise the organization's domain and several sensitive business system (SBS) targets. The assessed organization discovered evidence of the red team's initial activity but failed to act promptly regarding the malicious network traffic through its DMZ or challenge much of the red team's presence in the organization's Windows environment.

The red team was able to compromise the domain and SBSs of the organization as it lacked sufficient controls to detect and respond to their activities. The red team's findings illuminate lessons learned for network defenders and software manufacturers about how to respond to and reduce risk.

- **Lesson Learned: The assessed organization had insufficient technical controls to prevent and detect malicious activity.** The organization relied too heavily on host-based endpoint detection and response (EDR) solutions and did not implement sufficient network layer protections.

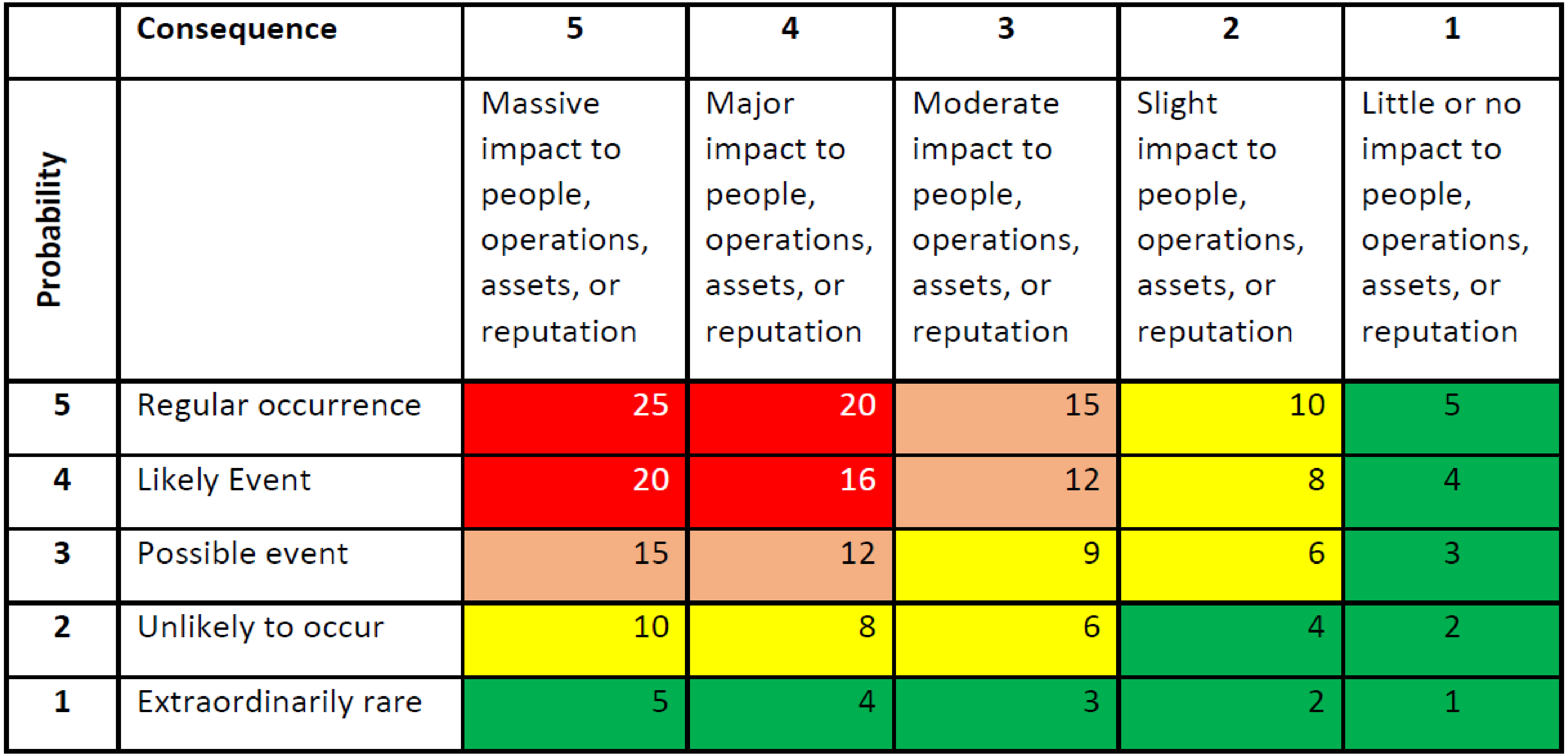
This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

Control Effectiveness

Level	Description	Example
6	Make the operation unnecessary.	Modification to eliminate the operation.
5	Automate the process.	Automation instead of a manual process.
4	Create an error-proof process.	Bounds checking, input sanitization.
3	Use visual aids and checklists.	Visual controls.
2	Verify the output.	Inspections and audits.
1	Train or provide feedback.	Retraining.

Risk Estimation

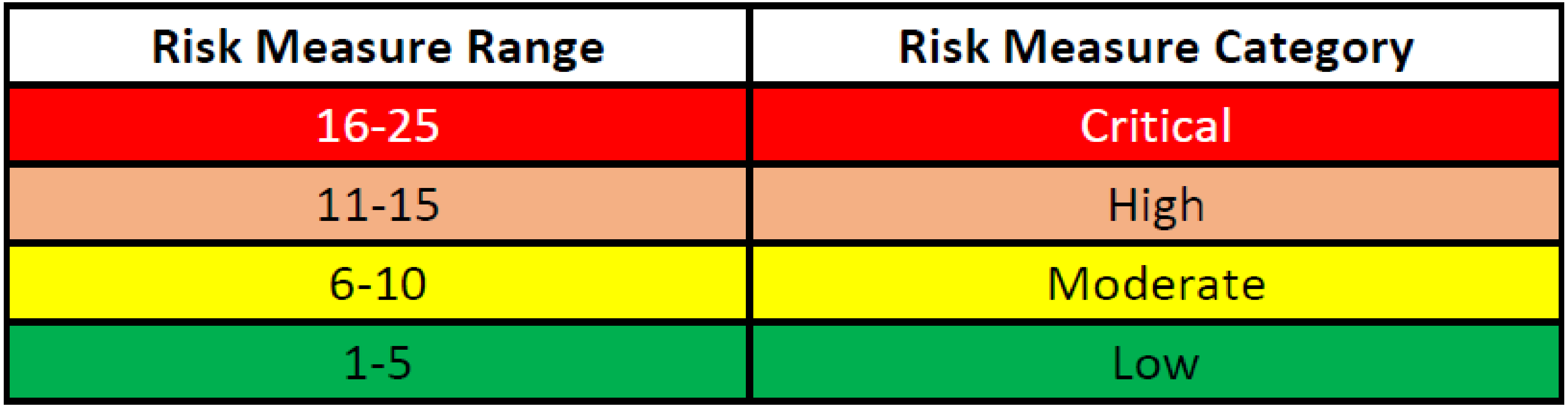


	Consequence	5	4	3	2	1
Probability		Massive impact to people, operations, assets, or reputation	Major impact to people, operations, assets, or reputation	Moderate impact to people, operations, assets, or reputation	Slight impact to people, operations, assets, or reputation	Little or no impact to people, operations, assets, or reputation
5	Regular occurrence	25	20	15	10	5
4	Likely Event	20	16	12	8	4
3	Possible event	15	12	9	6	3
2	Unlikely to occur	10	8	6	4	2
1	Extraordinarily rare	5	4	3	2	1

Residual Risk Categorization

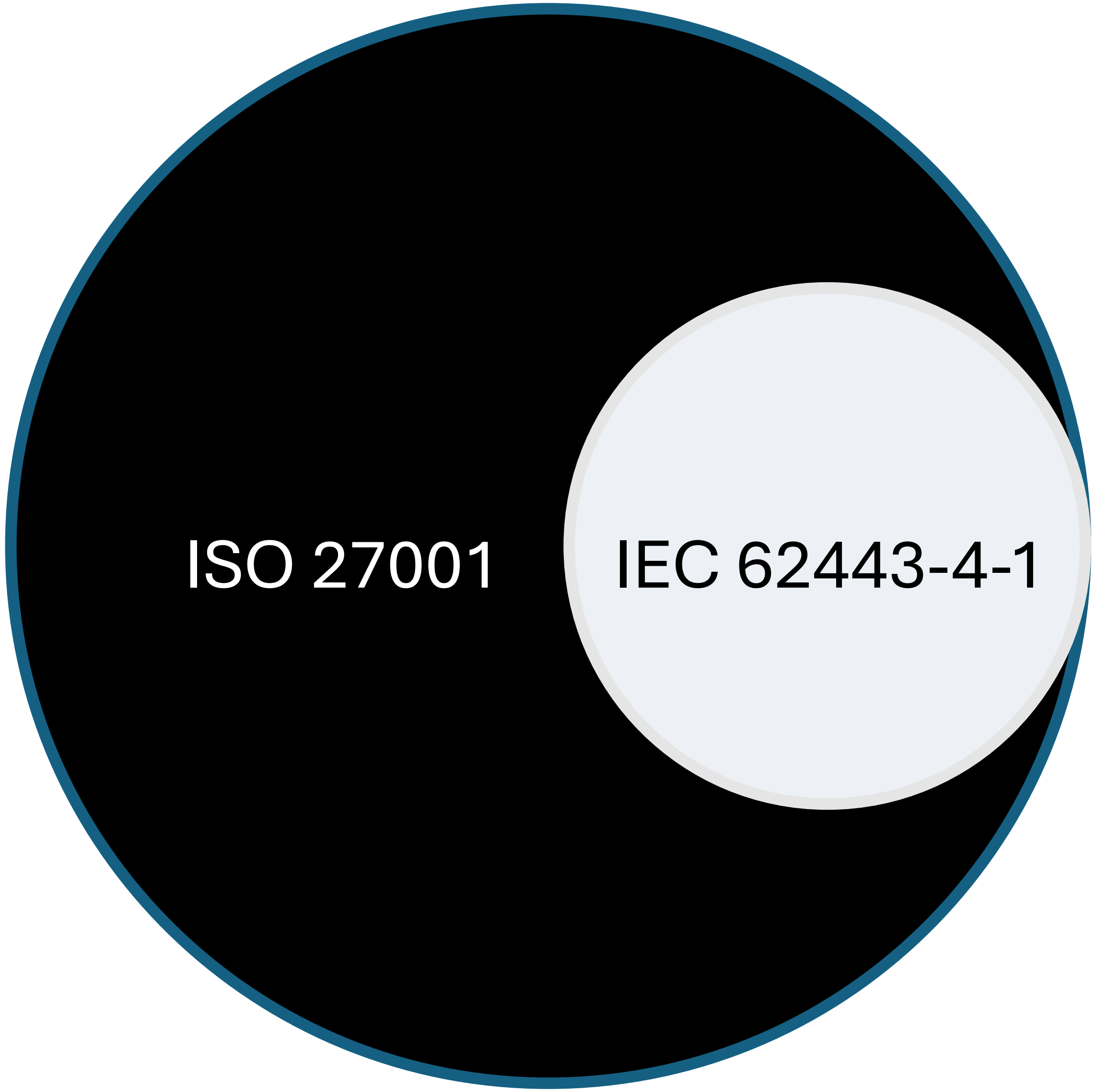
Example: Inherent risk of 20 for a given threat (e.g., DDoS attack)
Mitigating controls are assessed as 70% effective

20 * (1-.7) = 6 (Moderate Risk)



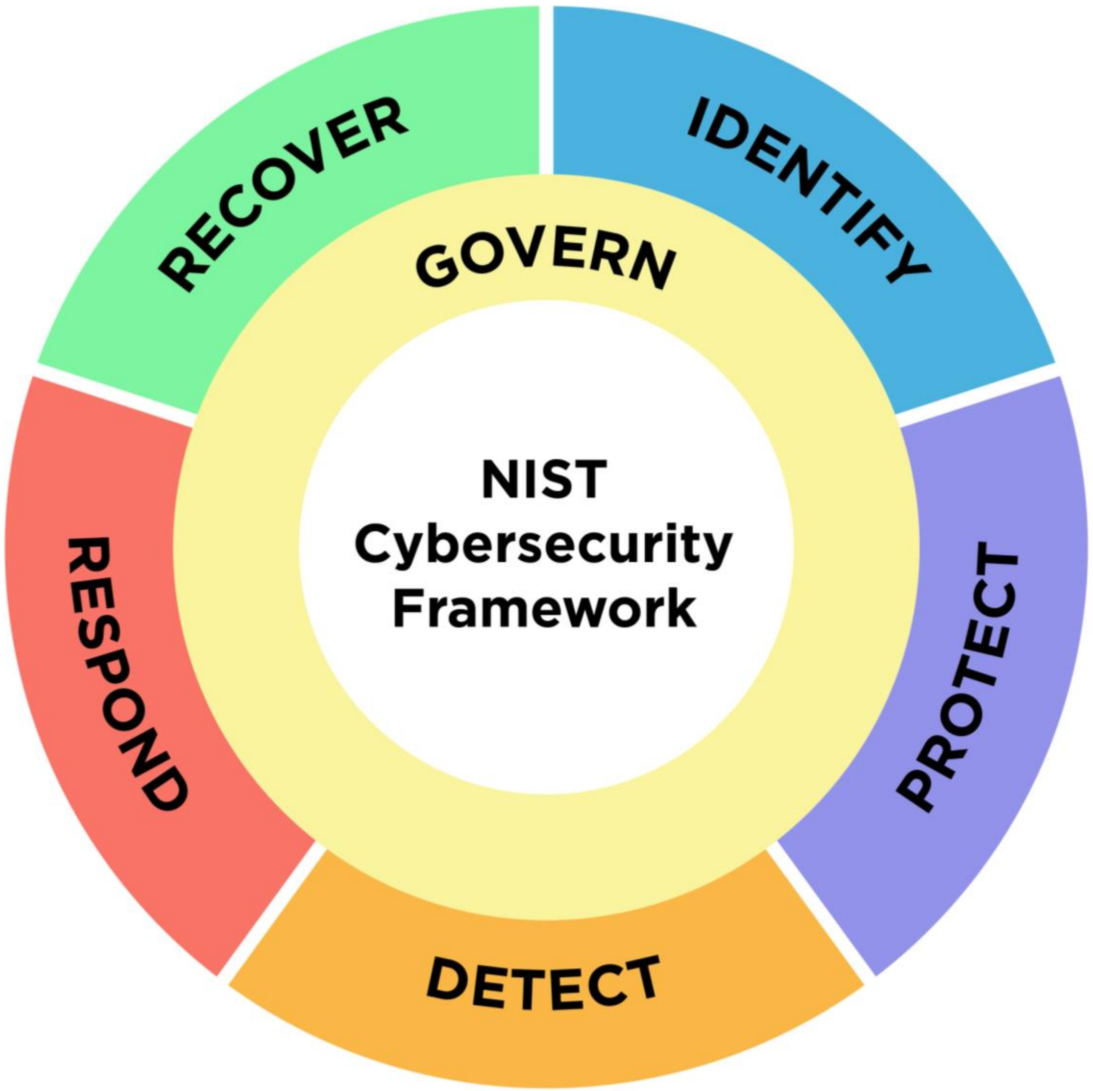
Risk Measure Range	Risk Measure Category
16-25	Critical
11-15	High
6-10	Moderate
1-5	Low

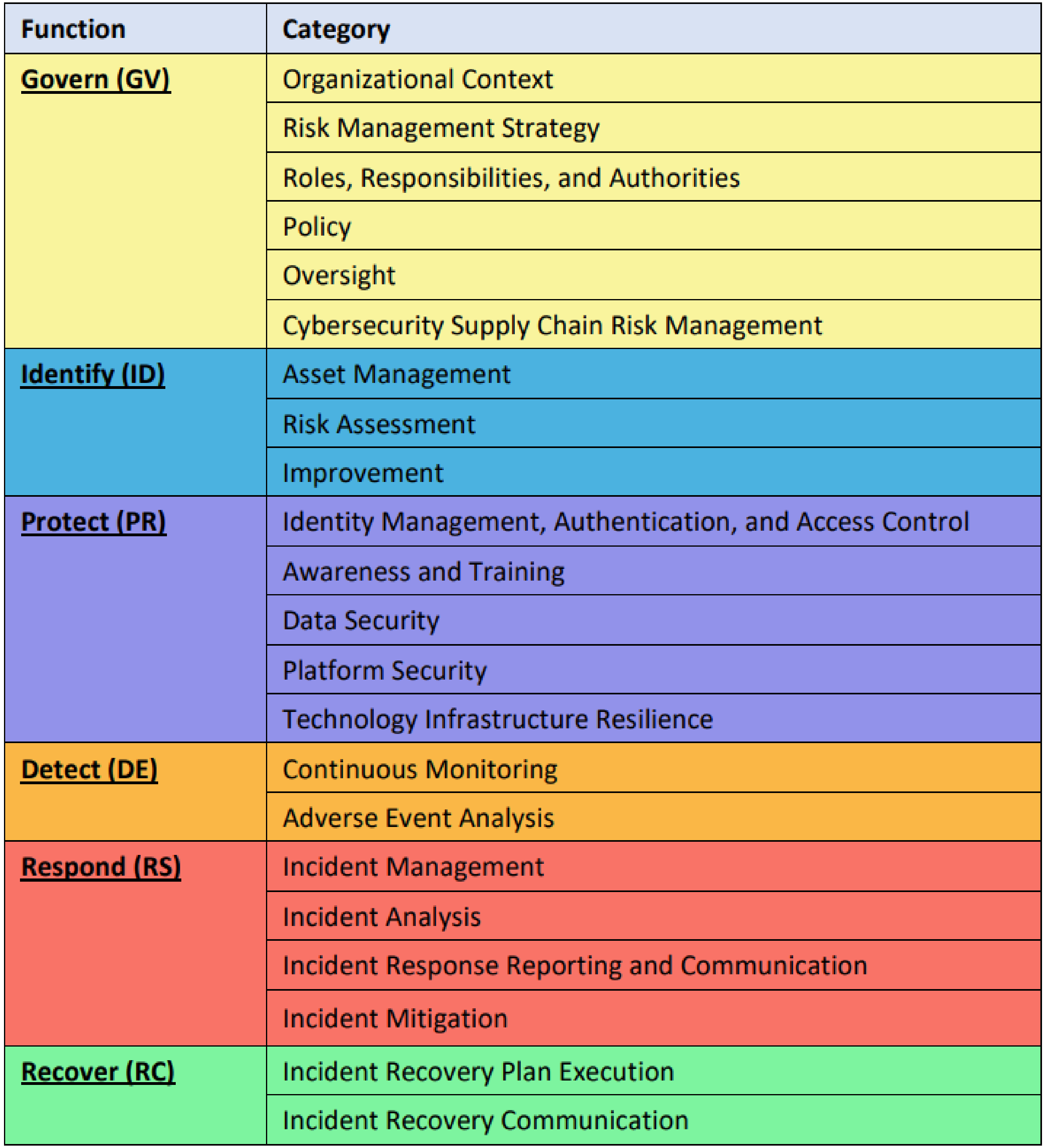
Internationally recognized security standards are auditable and widely accepted.



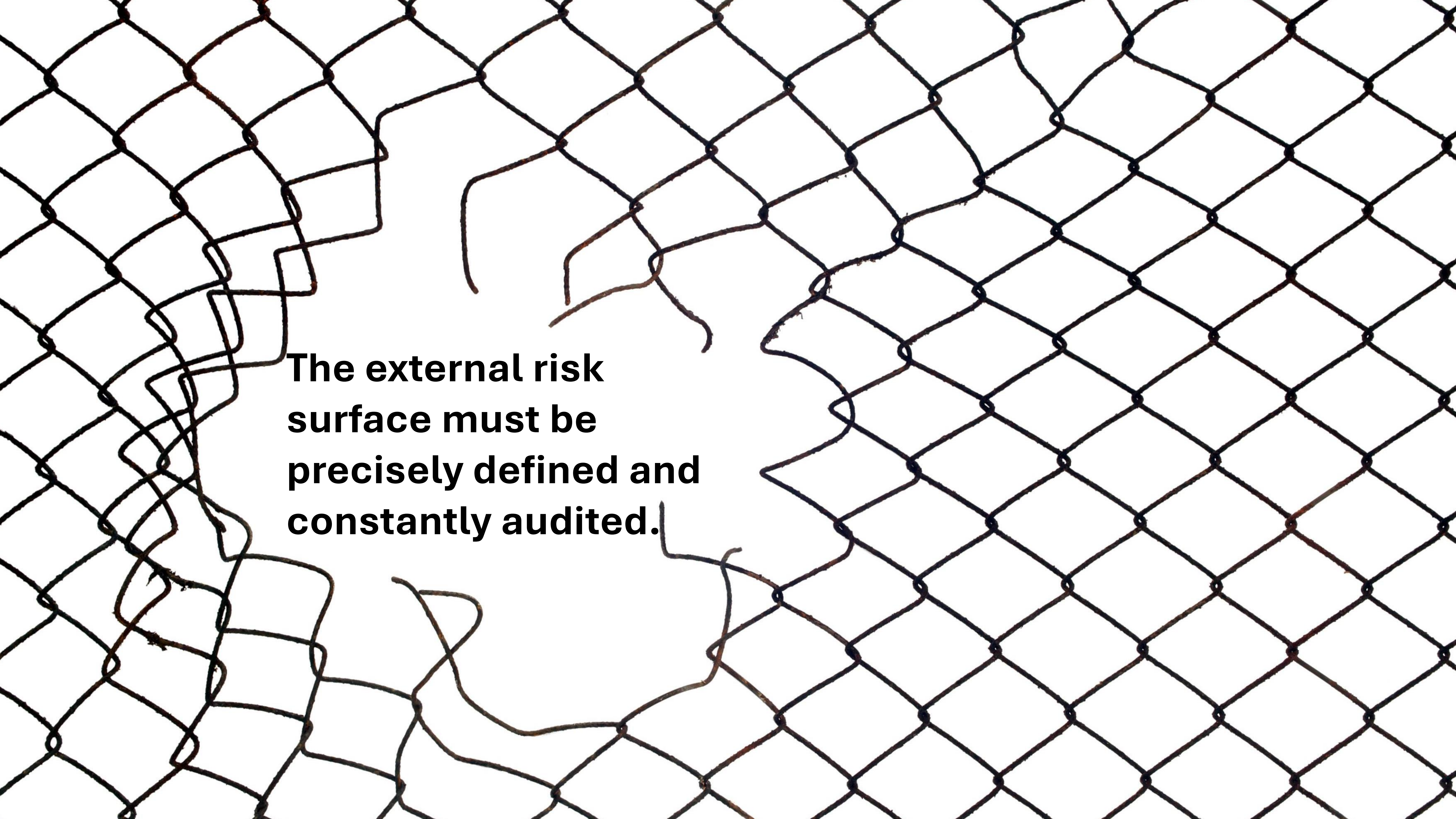
ISO 27001

IEC 62443-4-1

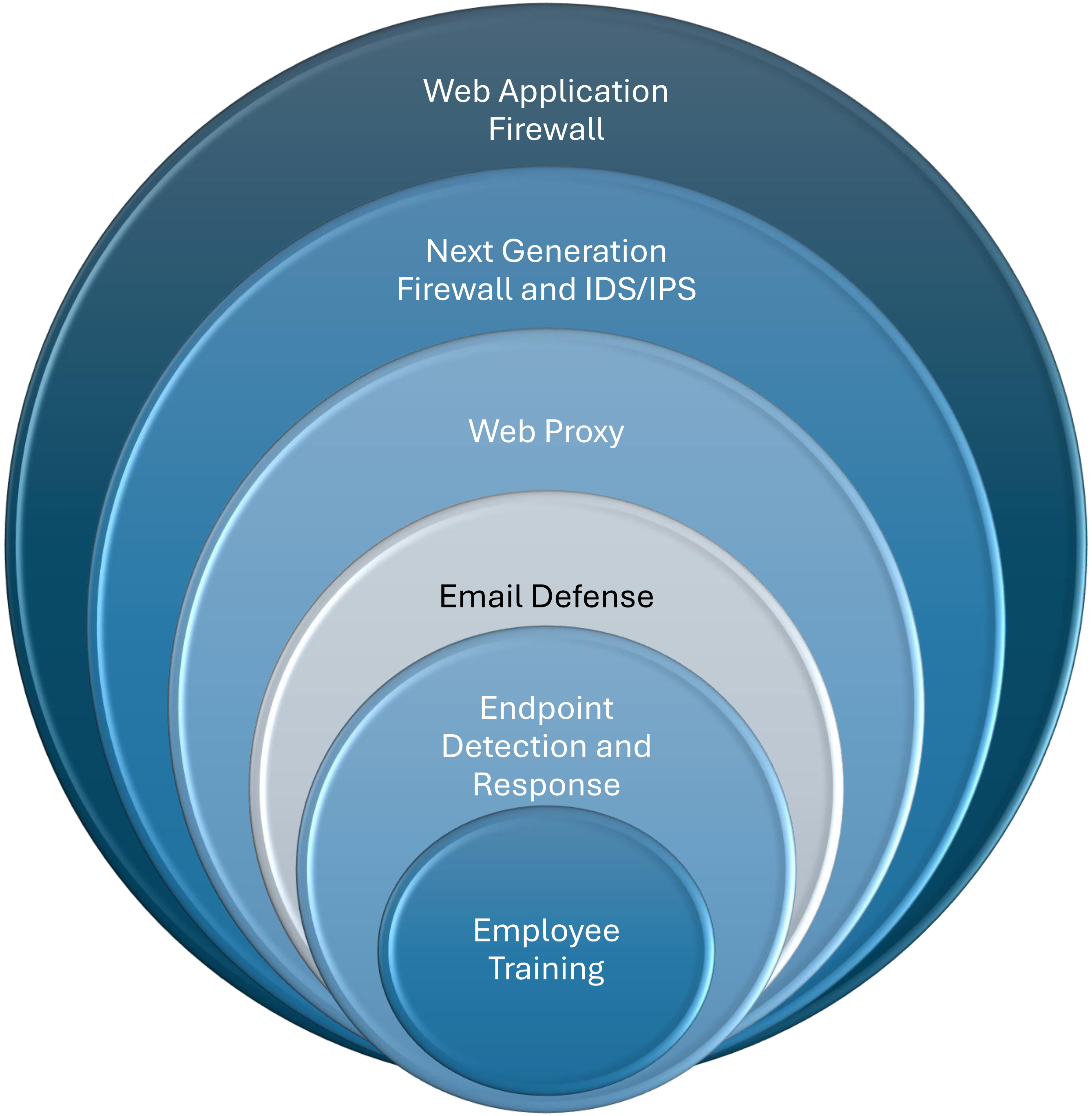




Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication

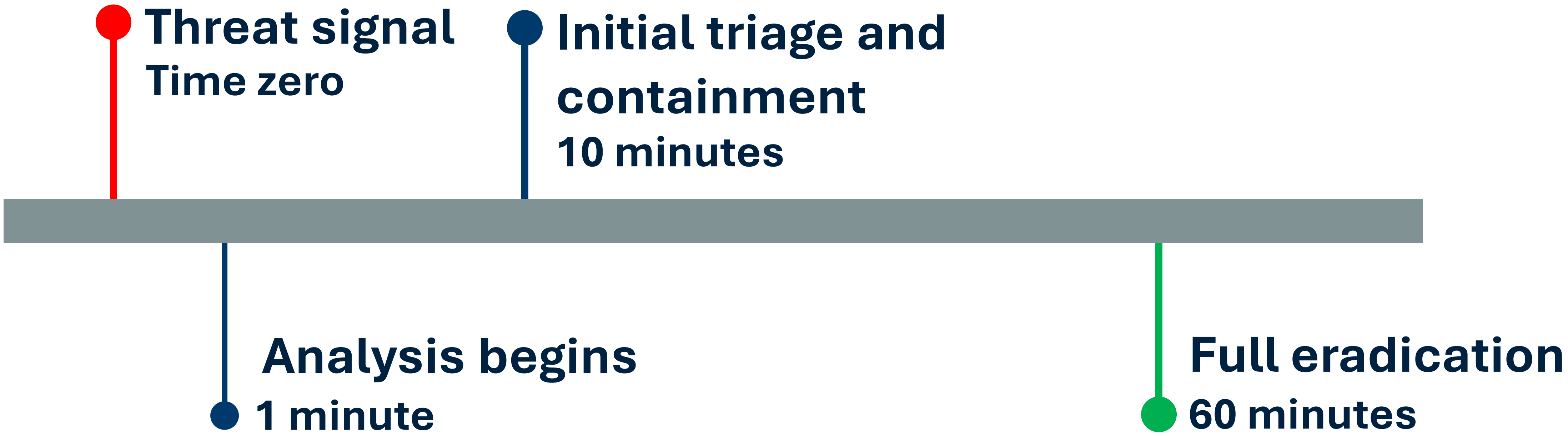


The external risk surface must be precisely defined and constantly audited.


Web Application Firewall
Next Generation Firewall and IDS/IPS
Web Proxy
Email Defense
Endpoint Detection and Response
Employee Training

- Network Segmentation
- Security Operations Center
- Security Incident and Event Management (SIEM) Platform
- Privileged Access Management
- MFA and Conditional Access
- Removable Device Control
- Encryption at Rest and in Transit
- Deception Technology

Constant vigilance is essential



Threat signal
Time zero

Analysis begins
1 minute

Initial triage and containment
10 minutes

Full eradication
60 minutes

The most damaging threats often come from within.

How does an Insider Become a Threat?

Malicious

Negligent

Compromised

Negligence or **Carelessness**

Personal Email

File Sharing/Sync

Mobile Devices

Unapproved Software

Bypassing Security Controls

Recent Incidents

“On February 12, criminals used compromised credentials to remotely access a Change Healthcare Citrix portal, an application used to enable remote access to desktops. The portal did not have multi-factor authentication. Once the threat actor gained access, they moved laterally within the systems in more sophisticated ways and exfiltrated data. Ransomware was deployed nine days later.”

Testimony of Andrew Witty
Chief Executive Officer, UnitedHealth Group
Before the House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
“Examining the Change Healthcare Cyberattack”
May 1, 2024

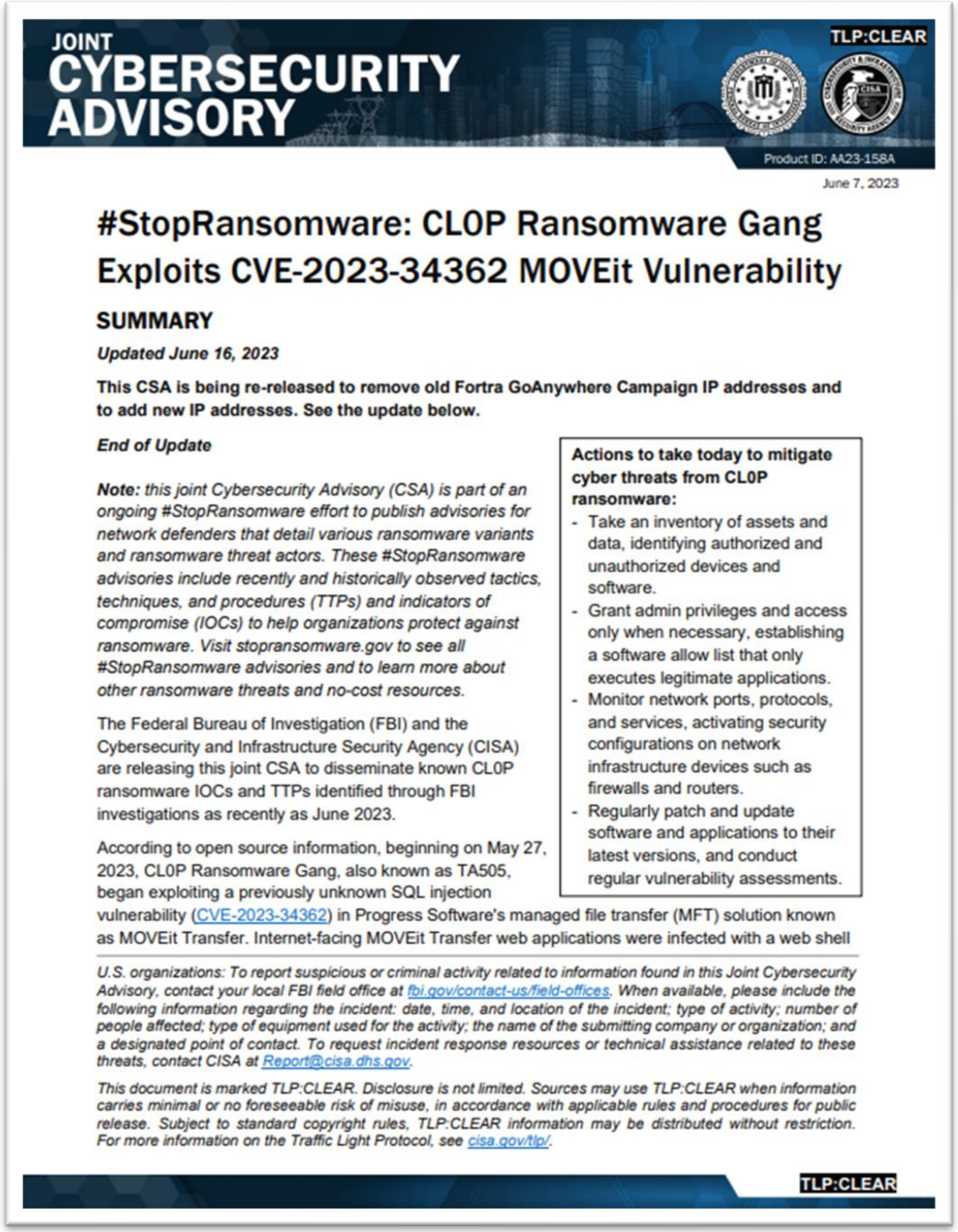
“As chief executive officer, the decision to pay a ransom was mine. This was one of the hardest decisions I’ve ever had to make.

And I wouldn’t wish it on anyone.”

Testimony of Andrew Witty
Chief Executive Officer, UnitedHealth Group
Before the House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
“Examining the Change Healthcare Cyberattack”
May 1, 2024

“As we have previously confirmed, based on initial targeted data sampling to date, we found files containing protected health information (PHI) and personally identifiable information (PII), which could cover a substantial proportion of people in America.”

Testimony of Andrew Witty
Chief Executive Officer, UnitedHealth Group
Before the House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
“Examining the Change Healthcare Cyberattack”
May 1, 2024



JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Product ID: AA23-158A

June 7, 2023

#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability

SUMMARY

Updated June 16, 2023

This CSA is being re-released to remove old Fortra GoAnywhere Campaign IP addresses and to add new IP addresses. See the update below.

End of Update

Actions to take today to mitigate cyber threats from CL0P ransomware:

- Take an inventory of assets and data, identifying authorized and unauthorized devices and software.
- Grant admin privileges and access only when necessary, establishing a software allow list that only executes legitimate applications.
- Monitor network ports, protocols, and services, activating security configurations on network infrastructure devices such as firewalls and routers.
- Regularly patch and update software and applications to their latest versions, and conduct regular vulnerability assessments.

Note: *this joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known CL0P ransomware IOCs and TTPs identified through FBI investigations as recently as June 2023.

According to open source information, beginning on May 27, 2023, CL0P Ransomware Gang, also known as TA505, began exploiting a previously unknown SQL injection vulnerability (CVE-2023-34362) in Progress Software's managed file transfer (MFT) solution known as MOVEit Transfer. Internet-facing MOVEit Transfer web applications were infected with a web shell

U.S. organizations: To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at fbi.gov/contact-us/field-offices. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Report@cisa.dhs.gov.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp/.

TLP:CLEAR

Which of the controls we discussed thwarted exploitation of this zero-day attack?

Questions