HITRUST CSF THREAT & MITIGATION ANALYSIS H2 2025

Period Covered: 7/01/2025 to 12/31/2025

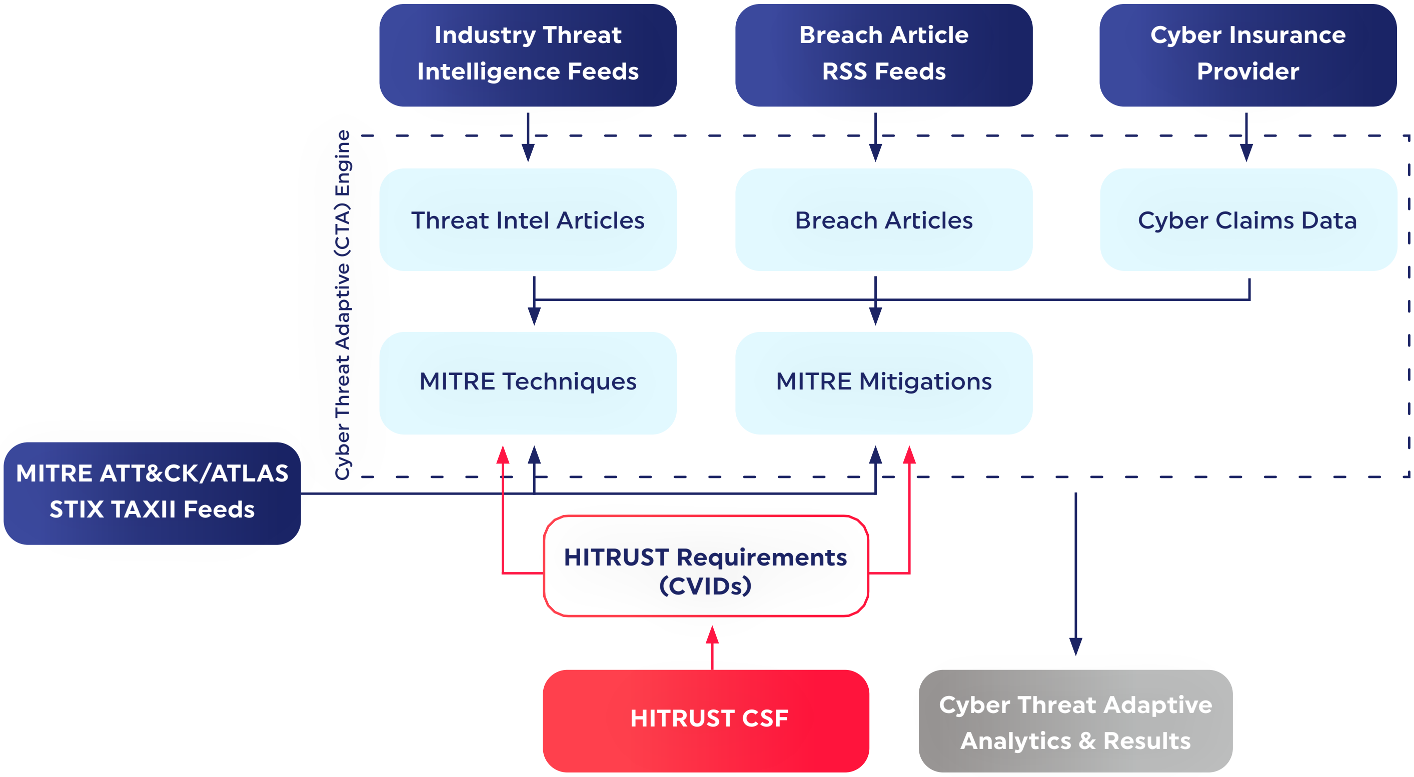
Static Security Programs Can't Keep Up. HITRUST Can.

As cyber threats evolve rapidly, static or slow-moving security frameworks often fail to remain effective. Attackers exploit vulnerabilities and weaknesses faster than organizations can react. The result is security controls that may look effective on paper but fail to respond to a changing threat landscape.

HITRUST addresses this challenge with its Cyber Threat Adaptive (CTA) program. This innovative solution stress-tests the HITRUST framework, the HITRUST CSF, with real-world threat intelligence, ensuring our controls remain highly relevant and effective against emerging risks and support organizations' ongoing compliance obligations. This means that organizations with HITRUST certifications are prepared to face evolving threats.

Our Approach

HITRUST uses a comprehensive and continuous process to identify threats, align mitigations that counter them, and position the organization to respond effectively. Through this process, HITRUST regularly reviews and updates the framework to respond to the constantly shifting threat landscape. The diagram below illustrates how we orchestrate this process and use it to progressively update the HITRUST framework:


Industry Threat Intelligence Feeds
Breach Article RSS Feeds
Cyber Insurance Provider
Cyber Threat Adaptive (CTA) Engine
Threat Intel Articles
Breach Articles
Cyber Claims Data
MITRE Techniques
MITRE Mitigations
MITRE ATT&CK/ATLAS STIX TAXII Feeds
HITRUST Requirements (CVIDs)
HITRUST CSF
Cyber Threat Adaptive Analytics & Results

The output of this process informs which requirements are included in HITRUST's e1 and i1 assessments and certifications. In general, the e1 is a streamlined baseline of security practices for organizations starting their HITRUST journey, with an important emphasis on cyber essentials, while the larger i1 offers a more comprehensive level of assurance and serves as the basis for our tailorable 2-year r2 assessment. The e1 addresses many of the most common entry points for attackers such as phishing, command and scripting, and process injection while the i1 introduces more robust controls around network traffic management, application allow listing, and more. For more information on the e1, i1, and r2 assessments see:

- HITRUST® 1-year (e1) Validated Assessment | HITRUST®
- HITRUST® 1-year (i1) Validated Assessment | HITRUST®
- HITRUST® 2-year (r2) Validated Assessment | HITRUST®

Throughout this report, you will see references to *MITRE ATT&CK techniques and mitigations* which can be found here: MITRE ATT&CK®.

You will also see *HITRUST Cross Version Identifiers (CVIDs) for HITRUST CSF* requirements. To see the full text of the requirement statements, download the HITRUST CSF for free.

Summary of Findings

For this half, our research confirms that the i1, e1, and r2 requirement selections remain responsive to the current threat landscape. During this period, we analyzed 588,588 indicators across 4,650 threat articles resulting in 46,175 mappings to MITRE ATT&CK techniques and mitigations. Analysis of the most common techniques[1] confirms that the e1 and i1 assessments have a high degree of coverage against techniques that were most prevalent in this half.

Top Techniques and Mitigations

From this data, we identified the following as the top 5 techniques for this period:

Commonly Sighted Technique in H2 2025	MITRE Mitigations	HITRUST CVIDs
Phishing (T1566) ***Initial Access***		
Longstanding as the most common initial attack vector, this period was no exception and further validates the importance of anti-phishing training and email security. These six months saw an increase in spear phishing campaigns empowered by more advanced AI capabilities – enabling attackers to perform at a scale that was previously not available. These techniques were used in a blend of attacks aimed at either implanting persistent threats such as malware and ransomware, performing intelligence gathering, or achieving financial gain.	M1047 – Audit	0599.0 (i1)
	M1031 – Network Intrusion Prevention	0880.0 (i1)
	M1054 - Software Configuration	0886.1 (i1/e1)
	M1017 – User Training	2316.0 (i1/e1)
Drive-by Compromise (T1189) ***Initial Access***		
An attacker may be able to gain access to a system through a user visiting a website over the normal course of browsing. Multiple methods of exploitation exist including compromising a legitimate website, malicious ads paid for and served through legitimate ad providers, and leveraging built-in application interfaces by inserting malicious scripts. Mitigation of a technique with such a broad attack surface is typically a piecemeal effort. Security best practices such as user training and ensuring browsers and plugins are up to date can go a long way. When combined with technical implementations of exploit protection applications, restricting certain web-based content as a whole, and browser sandboxing, many attacks using this technique can be thwarted.	M1048 – Application Isolation and Sandboxing	0884.0 (i1) 0946.0 (i1)
	M1050 – Exploit Protection	0189.0 (i1)
	M1021 – Restrict Web-Based Content	0873.0 (i1)
	M1051 – Update Software	1989.0 (i1)
	M1017 – User Training	1369.0 (i1) 2317.1 (e1/i1) 2316.0 (e1/i1) 0343.0 (i1)
Exploit Public-Facing Application (T1190) ***Initial Access***		
This technique relies on exploiting a weakness in an internet-facing host or system. This is unique from the Drive-by Compromise detailed above as the focus here is on compromising the host website/web server or database, versus the client endpoint visiting a website. There are several mitigating controls to implement to avoid falling victim to this attack technique, as well as limit impact in case exploitation does occur.	M1048 – Application Isolation and Sandboxing	0884.0 (i1) 0946.0 (i1)
	M1050 – Exploit Protection	0117.0 (i1)
	M1035 – Limit Access to Resource Over Network	0160.0 (e1/i1) 0297.0 (i1)
	M1030 – Network Segmentation	0035.0 (e1/i1)
	M1026 – Privileged Account Management	1369.0 (i1)
	M1051 – Update Software	2317.1 (e1/i1)
	M1016 – Vulnerability Scanning	2367.0 (e1/i1)

[1] In this document, when discussing techniques, we are referring to Techniques defined in the MITRE ATT&CK Framework. MITRE techniques refer to the methods used by adversaries to achieve their tactical goals during cyberattacks. The MITRE ATT&CK framework is a globally-accessible knowledge base that catalogs these techniques based on real-world observations, helping organizations understand and defend against potential threats.

Commonly Sighted Technique in H1 2025	MITRE Mitigations	HITRUST CVIDs
Exploitation of Remote Services (T1210) ***Lateral Movement***		
Once a foothold is obtained within a target environment, it is a common technique to attempt to exploit remote services. Remote services can often be a lower priority for organizations to fully patch and there are older remote communication protocols still in use that contain several well-known vulnerabilities. If an attacker can gain access to a remote service, they can ensure their access is maintained and potentially escalate their privilege. By implementing a threat intelligence program, exploit protection, updating software, disabling or removing unnecessary programs, and regular vulnerability scanning, remote services can be kept secure and difficult to exploit. In addition, by segmenting your network, practicing privileged account management, and application sandboxing, impact, further lateral or escalation movement can be mitigated.	M1048 – Application Isolation and Sandboxing	0884.0 (i1) 1303.0 (e1/i1)
	M1042 – Disable or Remove Feature or Program	1313.0 (i1) 0946.0 (i1)
	M1050 – Exploit Protection	0160.0 (e1/i1)
	M1030 – Network Segmentation	0297.0 (i1)
	M1026 – Privileged Account Management	0035.0 (e1/i1)
	M1019 – Threat Intelligence Program	0488.0 (i1)
	M1051 – Update Software	1369.0 (i1)
	M1016 – Vulnerability Scanning	2317.1 (e1/i1) 2367.0 (e1/i1)
Event-Triggered Execution (T1546) ***Privilege Escalation, Persistence***		
Once an attacker gains access to a system, it is common to piggyback off built in system mechanisms that trigger based on specific events to constantly execute malicious code. For example, every time a logon occurs, an exploit may be run to regain real-time access to the system. It is common to see this technique associated with system or service accounts, so practicing privileged account management is important to ensure escalation of access does not occur. Regularly performing software updates also help mitigate exploitation risk.	M1026 – Privileged Account Management	0297.0 (i1)
	M1051 – Update Software	0035.0 (e1/i1) 1369.0 (i1) 2317.1 (e1/i1)

Current Active Attacks

Additionally, we looked at 425 real-world breaches that were reported during H2 of 2025 and analyzed the techniques used to perform those breaches. We've continued tracking phishing-based attacks as the most prevalent trend in recent periods. Most often, the goal when using a phishing style technique is data exfiltration or malware deployment. This continues to align with the results found in our quantitative analysis of threat data and enforces a major focus of our adaptive assessments.

Suggested Actions

Based on the results of this half, we recommend the following:

- Ensure that comprehensive **role-based security training** policies and procedures are developed, implemented effectively, and their adherence is measured and managed. Phishing and spear phishing attacks are continuously the most common and most effective attack vectors seen and are evolving rapidly with the increased application of large language model assisted attacks. Applying dedicated **phishing awareness training** is a vital step to protecting a workforce.
    - *See HITRUST CVIDs 0343.0 (i1), 0599.0 (i1), 0880.0 (i1), 0886.1 (e1/i1), and 2316.9 (e1/i1).*
- Ensure the **timely installation of anti-malware** protective measures and technologies, including regular updates, upgrades, and software scans. Additionally, **configure malicious code and spam protection** to detect known threats and low-effort attacks.
    - *See HITRUST CVIDs 0884.0 (i1) and 0873.0 (i1)*
- Once a potential technical vulnerability has been identified, **identify associated risks and actions** to be taken. Perform these actions in a timely manner.
    - *See HITRUST CVID 1369.0 (i1)*
- Protect your network perimeter and key points within the network by implementing technical tools such as **intrusion detection systems (IDS)/intrusion prevention systems (IPS)**. Ensure these are implemented on the wireless side of the firewall, and update all engines, baselines, and signatures on a regular basis.
    - *See HITRUST CVID 0946.0 (i1)*

In addition to the CVIDs in which we saw the biggest indicator counts by volume, the following list contains excellent practices continuously seen in relation to mitigating top attack techniques.

- Ensure that your organization has controls in place to:
    - **limit attack surface area** by blocking unnecessary protocols,
        - *See HITRUST CVID 1375.0 (i1)*
    - continually **inventorying approved assets**, **auditing environments**,
        - *See HITRUST CVIDs 0626.1 (e1/i1), 0626.2 (i1), and 0626.2 (i1)*
    - and **monitoring endpoints for suspicious activity**.
        - *See HITRUST CVID 0884.0 (i1)*
    - Additionally, a **robust EDR system and firewall** will help mitigate threats by stopping these techniques before they spread throughout the organization's environment.
        - *See HITRUST CVIDs 0943.2 (e1/i1) and 1488.0 (e1/i1)*

Additional Considerations

While we saw consistency in volume, we can also gain insights from considering utilization of techniques proportionate to their average usage. The following highlights a few techniques which had the highest increase in usage from the prior analysis period.

Largest Usage Increase Technique in H2 2025	MITRE Mitigations	HITRUST CVIDs
External Remote Services (T1133) ***Persistence, Initial Access***		
The largest proportional increase of the period was the use of External Remote Services. With the uptick in remote services and specifically remote access mechanisms, attackers have focused efforts on these gateways. Obtaining credentials or exploiting vulnerabilities in these services creates unauthorized access. Some services may not contain authentication protocols at all. Strong access controls, network segmentation, and keeping an eye on necessary features or programs are important steps to preventing unauthorized access.	M1042 – Disable or Remove Feature or Program	1303.0 (i1/e1) 1313.0 (i1)
	M1035 – Limit Access to Resource Over Network	0117.0 (i1) 2321.0 (i1/e1)
	M1032 – Multi-factor Authentication	2322.0 (i1/e1)
	M1030 – Network Segmentation	0160.0 (i1/e1)
	M1021 – Restrict Web-Based Content	0189.0 (i1) 0873.0 (i1) 1989.0 (i1)
Implant Internal Image (T1525) ***Persistence***		
Once access is established in a system, maintaining that access can be paramount. Embedding malicious code within cloud or container images is a popular way to establish a backdoor. Routine services, platforms, and images are often utilized to avoid detection. Auditing and privileged account management along with implementing code signing for container images are proper mitigations for this technique.	M1047 – Audit	2121.0 (i1)
	M1046 – Code Signing	1488.0 (i1/e1)
	M1026 – Privileged Account Management	0873.0 (i1) 0884.0 (i1) 0297.0 (i1) 0035.0 (i1/e1)
Steal Web Session Cookie (T1539) ***Credential Access***		
Adversaries may steal web application or service session cookies. Stolen cookies can lead to authenticated user access to web apps and services. Malware can be coded to target cookies while a user is active. Due to the nature of web application use, there are many mitigations to ensure a level of protection. Keeping software configured securely and up to date, restricting web-based content when not necessary, training users on phishing schemes, implementing multi-factor authentication, and auditing authentication are all effective mitigations in concert.	M1047 – Audit	2121.0 (i1)
	M1032 – Multi-factor Authentication	1488.0 (i1/e1)
	M1021 – Restrict Web-Based Content	2321.0 (i1/e1)
	M1054 – Software Configuration	2322.0 (i1/e1)
	M1051 – Update Software	0189.0 (i1)
	M1017 – User Training	0873.0 (i1) 1989.0 (i1) 0886.1 (i1/e1) 1369.0 (i1) 2317.1 (i1/e1) 2316.0 (i1/e1) 0343.0 (i1)

CONCLUSION

In an era of increasingly diverse cyberattacks, aligning your security assessment and certification to match your organization's risk profile is essential. HITRUST's e1 and i1 certifications continue to be responsive to the most common techniques and their mitigations. HITRUST regularly reviews updated threat intelligence and breach data to continually refine the control selection in the e1 and i1 assessments. This ensures that the assessments evolve in response to real-world adversarial tactics and remain aligned with emerging threats over time. Whether you're looking to build confidence through a baseline "essentials" approach (e1) or need a more comprehensive, implemented set of controls (i1), both paths—enhanced by HITRUST's continual threat monitoring—help safeguard against the most common and damaging attacks in today's rapidly changing threat landscape.