HITRUST®

HITRUST CSF THREAT & MITIGATION ANALYSIS

2025 Q3

Period Covered: 7/01/2025 to 9/30/2025

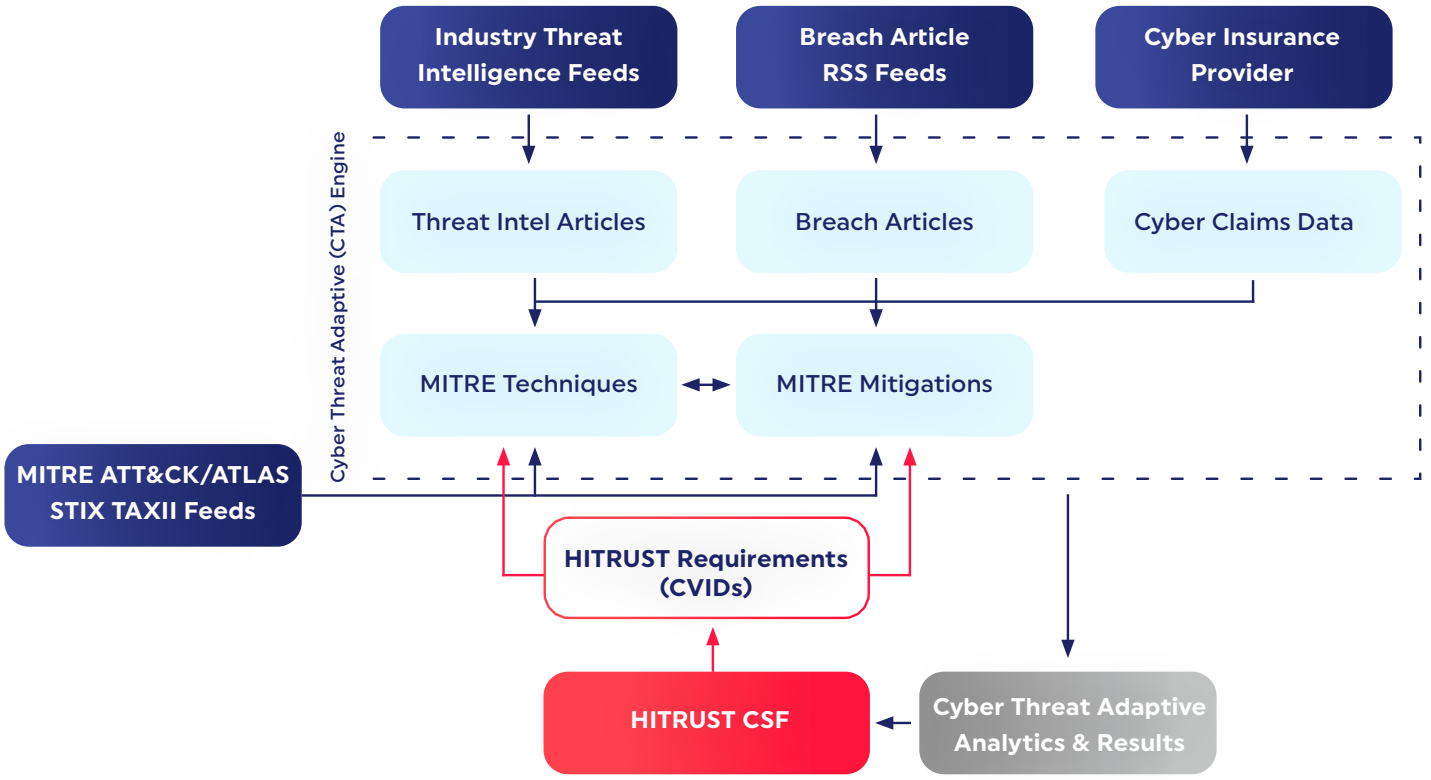
Static Security Programs Can't Keep Up. HITRUST Can.

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:



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® 1-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 quarter, our research confirms that the i1, e1, and r2 requirement selections remain responsive to the current threat landscape. During this period, we analyzed 226,831 indicators across 4,445 threat articles resulting in approximately 4,000 mappings to MITRE ATT&CK techniques[1] and mitigations. Analysis of the most common techniques confirms that the e1 and i1 assessments have a high degree of coverage against techniques that were most prevalent in this quarter.

Top Techniques and Mitigations

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

Commonly Sighted Technique in 2025 Q3	MITRE Mitigations	HITRUST CVIDs
Phishing (T1566) ***Initial Access***		
Longstanding as the most common initial attack vector, this quarter was no exception and further validates the importance of anti-phishing training and email security. This quarter 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 M1031 — Network Intrusion Prevention M1054 — Software Configuration M1017 — User Training	0599.0 (i1) 0880.0 (i1) 0886.1 (e1/i1) 2316.0 (e1/i1)
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 plug-ins 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 M1050 – Exploit Protection M1021 – Restrict Web-Based Content M1051 – Update Software M1017 – User Training	0884.0 (i1) 0946.0 (i1) 0189.0 (i1) 0873.0 (i1) 1989.0 (i1) 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 M1050 – Exploit Protection M1035 – Limit Access to Resource Over Network M1030 – Network Segmentation M1026 – Privileged Account Management M1051 – Update Software M1016 – Vulnerability Scanning	0884.0 (i1) 0946.0 (i1) 0117.0 (i1) 0160.0 (e1/i1) 0297.0 (i1) 0035.0 (e1/i1) 1369.0 (i1) 2317.1 (e1/i1) 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 2025 Q3	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 and further lateral or escalation movement can be mitigated.	M1048 – Application Isolation and Sandboxing M1042 – Disable or Remove Feature or Program M1050 – Exploit Protection M1030 – Network Segmentation M1026 – Privileged Account Management M1019 – Threat Intelligence Program M1051 – Update Software M1016 – Vulnerability Scanning	0884.0 (i1) 1303.0 (e1/i1) 1313.0 (i1) 0946.0 (i1) 0160.0 (e1/i1) 0297.0 (i1) 0035.0 (e1/i1) 0488.0 (i1) 1369.0 (i1) 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 helps mitigate exploitation risk.	M1026 – Privileged Account Management M1051 – Update Software	0297.0 (i1) 0035.0 (e1/i1) 1369.0 (i1) 2317.1 (e1/i1)

Current Active Attacks

Additionally, we looked at 192 real-world breaches that were reported during Q3 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 quarter, 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 2316.0 (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) 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 Q3 2025	MITRE Mitigations	HITRUST CVIDs
Input Injection (T1674) ***Initial Access***		
The largest proportional increase of the period was the use of Input Injection. A classic technique in which adversaries can simulate keystrokes by various means to execute malicious actions on a target host. A common approach includes the use of malicious USBs to emulate keystrokes, so limited removable media within a network is recommended to thwart such attacks. Denying scripting and use application control is also recommended to prevent execution.	M1034 – Limit Hardware Installation M1038 – Execution Prevention	1908.0 (i1) 0884.0 (i1)
ESXi Administration Command (T1675) ***Execution***		
An attacker may be able to gain access to a system through the abuse of ESXi administrative services on machines within virtual environments. ESXi-hosted virtual machines can be a medium for adversaries to leverage various tools capable of executing malicious commands and scripts. The best mitigating action is to limit the access to such ESXi-hosted virtual machines, especially restricting guests operations.	M1018 – User Account Management	0035.0 (e1/i1)
Gather Victim Network Information (T1590) ***Reconnaissance***		
This technique is often combined with gathering large amounts of victim information whether through open source intelligence (OSINT) or private means. Due to its broad and typically legal nature, there are limited mitigating controls to apply. MITRE applies its 'Pre-compromise" mitigation which confirms this technique cannot be easily mitigated with preventative controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.	M1056 – Pre-compromise	0886.1 (e1/i1) 1024.0 (i1) 2316.0 (e1/i1)
Remote Service Session Hijacking (T1563) ***Lateral Movement***		
Once a foothold is obtained within a target environment, it is a common technique to attempt to move laterally through remote services. Existing sessions are often targeted in order to remain undetected and maintain a continuous connection. By disabling or removing unnecessary programs, enforcing strong password policies, network segmentation, and both user and privileged user account management, remote services can be locked down to appropriate users and levels of access.	M1018 – User Account Management M1026 – Privileged Account Management M1027 – Password Policies M1030–Network Segmentation M1042 – Disable or Remove Feature or Program	0035.0 (e1/i1) 0297.0 (i1) 0108.0 (i1) 0160.0 (e1/i1) 1303.0 (e1/i1) 1313.0 (i1)
Traffic Signaling (T1205) ***Defense Evasion, Persistence, Command and Control***		
Defense evasion and persistence within a target network is as if not more important than gaining initial access. Adversaries may turn to traffic signaling in order to hide open ports or other potentially vulnerable functionalities that may be exploited. The best way to thwart these types of attack techniques is to identify features and programs that are not being used and disable and remove them. Wake-on-LAN specifically is prominently linked to this technique ID. Filtering network traffic through stateful firewalls can also help to mitigate some variants of Traffic Signaling.	M1037 – Filter Network Traffic M1042 – Disable or Remove Feature or Program	0946.0 (i1) 0189.0 (i1) 1303.0 (e1/i1) 1313.0 (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.