HITRUST®

HITRUST CSF CONTROL THREAT ANALYSIS

CYBER THREAT ADAPTIVE QUARTERLY UPDATE

Period Covered: 09/01/2024 to 12/31/2024

Maintaining Relevance of Controls in an Adaptive Framework

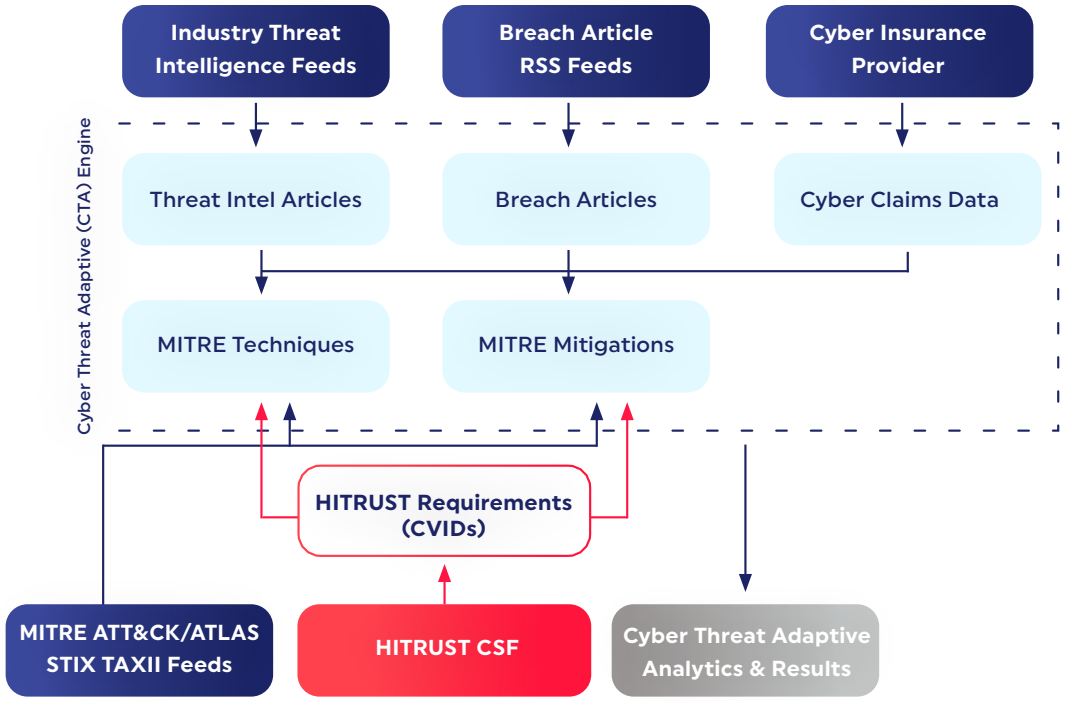
HITRUST is committed to ensuring that our Framework, Assessments, and Certifications remain continuously aligned to the evolving cyber threat landscape. Our **Cyber Threat Adaptive (CTA) program** is how we achieve this — by maintaining maximum relevance in the HITRUST CSF and its associated assurance offerings (e1, i1, and r2). Unlike static frameworks that risk becoming outdated, HITRUST uses CTA to perform regular, in-depth analyses of real-world threat intelligence, breach data, and attack techniques (such as those cataloged in the MITRE ATT&CK framework). This process informs precise modifications — additions, deletions, and refinements — to the HITRUST CSF, ensuring our control specifications reflect what is required to effectively defend against today's threats.

This report summarizes key insights from HITRUST's end-of-quarter CTA analysis covering the period from 09/01/2024 to 12/31/2024. The findings identify which controls remain effective, which need enhancement, and what emerging risks demand new requirements. When coupled with the HITRUST Assurance Program, this proactive approach delivers proven risk mitigation results, as documented in the HITRUST Trust Report.

CTA isn't just an enhancement — it's how HITRUST ensures our security assurances remain meaningful, relevant, and defensible over time.

Our Approach

HITRUST uses a comprehensive and continuous process to identify threats, align mitigations that counter ongoing and new threats, and position the organization to respond effectively. The HITRUST CSF is regularly reviewed and updated as necessary to respond to the constantly shifting threat landscape through this process. The diagram on the right illustrates how we orchestrate this process and use it to progressively update the HITRUST CSF.



Ultimately, the output of this process informs HITRUST on which requirements will be included as part of our e1 and i1 requirement selections. 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, please visit the following links:

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

Throughout this post, 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 our i1, e1, and r2 requirement selections are responsive to the current threat landscape. During this period, we analyzed approximately 129,000 indicators across nearly 4,000 threat articles resulting in approximately 42,000 mappings to MITRE ATT&CK techniques and mitigations. Looking at the most common techniques sighted,[1] the e1 and i1 requirement selections have a high degree of coverage against techniques that were most prevalent in this quarter.

[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.

Top Techniques and Mitigations

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

Commonly Seen Techniques in Q4 2024	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 (i1/e1) 2316.9 (i1/e1)
Command and Scripting Interpreter (T1059) **Execution**		
These techniques enable successful attackers to run arbitrary commands through valid command interpreters and shells. To mitigate these threats, defenders must have solid controls around verifying the legitimacy of code run in their environments. While all shells and script interpreters are a target for this technique, the most referenced target was PowerShell due to its capabilities and prevalence.	M1021 — Restrict Web-Based Content M1045 — Code Signing M1047 — Audit M1049 — Anti-Virus/Anti-Malware	2362.0 (i1/e1) 1263.1 (i1) 0884.0 1316.0 0895.0 0878.0 0793.0 0874.0
Process Injection (T1055) **Defense Evasion, Privilege Escalation**		
Attackers use process injection to run arbitrary code within otherwise approved processes. A strong defense against these attacks includes solid controls around privileged account management and endpoint behavior prevention. This technique is particularly common alongside attacks involving T1053 — Scheduled Task/Job.	M1026 — Privileged Account Management M1040 — Behavior Prevention on Endpoint	2366.0 (i1/e1) 0202.1 (i1/e1) 2913.0 1271.0 1089.0 2022.0

Additionally, we looked at 22 real-world breaches that were reported during this time and analyzed the techniques used to perform those breaches. We identified a consistent trend of phishing-based attacks with the goal of data exfiltration or malware deployment — aligning with the results found in our quantitative analysis of threat data.

Commonly Seen Techniques in Q4 2024	MITRE Mitigations	HITRUST CVIDs
Application Layer Protocol (T1071) **Command and Control**		
Instead of using unusual or suspicious methods to talk to their command center, attackers use normal internet communication methods. This might include protocols like HTTP, HTTPS, or DNS — the same ones your web browser or email uses every day. This allows attackers to hide in plain sight and requires specific controls to check for these anomalies. Organizations should ensure that they have adequate Endpoint Detection and Response (EDR) systems in place and strict outbound traffic controls.	**M1031 — Network Intrusion Prevention** **M1037 — Filter Network Traffic**	**0943.2 (i1/e1)** **0946.0 (i1)** **0189.0 (i1)** **1436.0** **2167.0**
Data Encrypted for Impact (T1486) **Impact**		
Ransomware attacks continue to be common and impactful. Mitigating the risks posed by these attacks requires strong maturity across policy, processes, implementation, management, and measurement of data recovery solutions. Additionally, endpoint protection should be in place to identify ransomware before it enters your organization's network.	**M1040 — Behavior Prevention on Endpoint** **M1053 — Data Backup** **T1486 — Data Encrypted for Impact Mitigation**	**0903.0 (i1/e1)** **0901.0 (i1/e1)** **2326.0 (i1/e1)** **0902.0 (i1)**

Suggested Actions

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

- Ensure that robust **anti-phishing training** policies and procedures are developed, implemented effectively, and their adherence is measured and managed. Phishing attacks will continually become more sophisticated with the increased application of large language model assisted attacks.

  See HITRUST CVIDs 0599.0 (i1), 0880.0 (i1), 0886.1 (i1/e1), and 2316.9 (i1/e1)

- Review policies and procedures surrounding **backups and disaster recovery** to validate they are comprehensive, and your data assets are protected in the event of a successful malware attack. Additionally, test your disaster recovery and data backup mechanisms to ensure they will be operational in the event they are needed.

  See HITRUST CVIDs 0903.0 (i1/e1), 0901.0 (i1/e1), 2326.0 (i1/e1), and 0902.0 (i1)

- In response to threats that seek to leverage your own infrastructure against you or hide among your IT assets, ensure that your organization has controls in place to:
  - **limit attack surface area** by blocking protocols that are not in use;

    See HITRUST CVID 1375.0 (i1)

  - continually **inventorying approved assets, auditing environments** to validate only approved assets exist;

    See HITRUST CVIDs 0626.1 (i1/e1), 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 enter your organization's environment.

  See HITRUST CVIDs 0943.2 (i1/e1) and 1488.0 (i1/e1)

Additional Considerations

While it was not a top threat this quarter, if you are using **artificial intelligence**, ensure that you have a suite of controls in place to address the specific risks related to artificial intelligence. Attackers are beginning to become more sophisticated and aware of attack vectors specific to artificial intelligence, and we anticipate AI-specific techniques to trend upward in the coming year. HITRUST offers two AI-focused assessments that will help identify your organization's security and risk posture with respect to AI:

AI Security Assessment | Comprehensive Controls for Securing AI Technologies | HITRUST®

AI Risk Management Assessment | Comprehensive Insights | HITRUST®

CONCLUSION

In an era of increasingly diverse cyberattacks, having a security assessment that matches 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.