HITRUST

HITRUST CSF THREAT & MITIGATION ANALYSIS

Q2 2026

Period Covered: 4/1/2026 to 6/30/2026

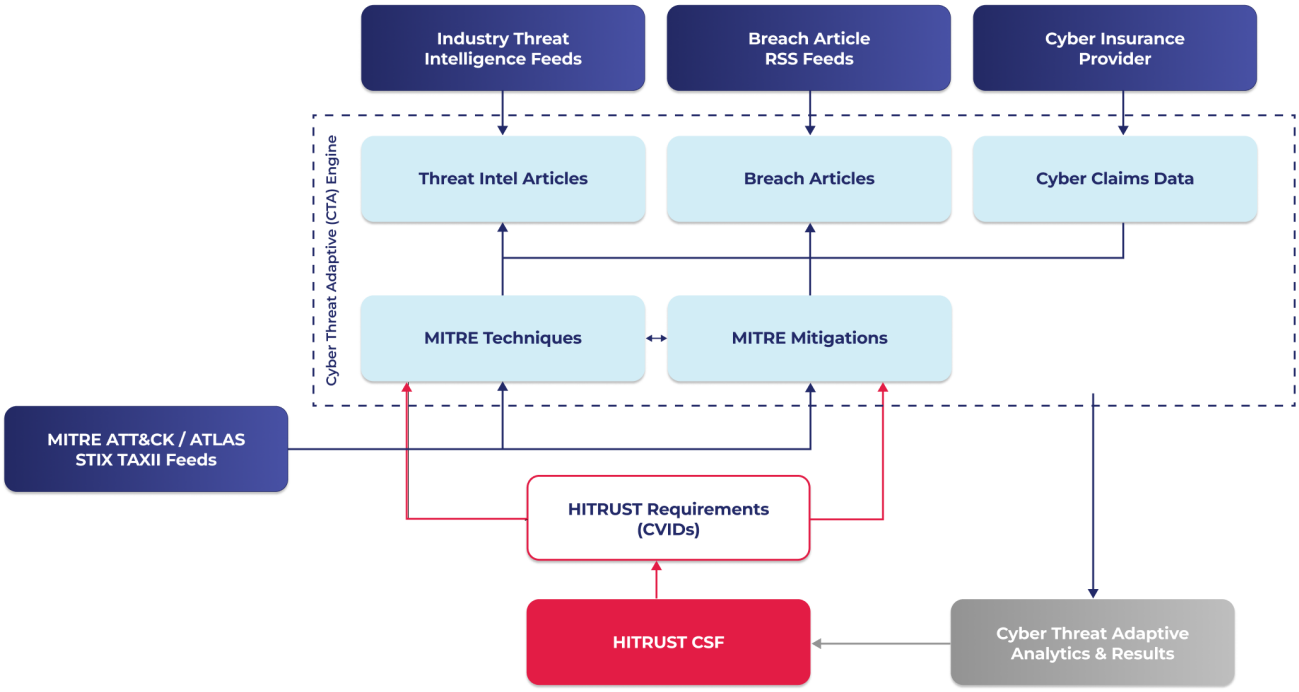
Continued Cyber Threat Analysis to Maintain Proven Mitigation Results.

Cyber threats continue to evolve as organizations adopt new technologies, expand digital operations, and face increasingly sophisticated adversaries. Security programs and frameworks must do more than demonstrate point-in-time alignment; they must continue to validate that control requirements remain effective against real-world threat activity.

HITRUST addresses this need through its Cyber Threat Adaptive (CTA) program. By continuing to analyze current threat intelligence and applying those insights to the HITRUST CSF, HITRUST helps maintain proven mitigation results while ensuring its control requirements remain relevant, effective, and responsive to emerging risks. As a result, organizations with HITRUST certifications can maintain confidence that their security programs are aligned to the evolving threat environment.

Our Approach

HITRUST uses a comprehensive, continuous process to identify threats, align effective mitigations, and help organizations respond with confidence. Through this process, HITRUST regularly reviews and updates the framework to keep pace with the evolving 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. The HITRUST AI Security Certification extends this approach to AI systems by enabling providers to demonstrate that they sufficiently mitigate cybersecurity threats to the AI technologies they have deployed. For more information on the e1, i1, r2, and AI Security Certification, see:

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

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

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

Based on our review of 4,926 threat articles and 435,141 MITRE ATT&CK and MITRE ATLAS indicators, we confirmed that the requirements included in the HITRUST AI Security Certification remain responsive to the evolving AI threat landscape with over 97% coverage of adversarial techniques. Additionally, this review confirms that the e1, i1, and r2 requirement selections continue to be responsive to the current threat landscape with 98.59% coverage of adversarial techniques for the e1 and 100% for the i1 and r2.

Top MITRE ATLAS Techniques and Mitigations

For the second consecutive quarter, AI-related tactics and techniques reflected in MITRE ATLAS continue to proportionately increase. HITRUST saw the volume of AI-specific techniques continue to surpass many traditionally prevalent methods. The top AI-related techniques observed in the second quarter of 2026 are:

Commonly Sighted AI Techniques in Q2 2026	MITRE Mitigations	HITRUST CVIDs
Phishing (AML.T0052) ***Initial Access, Lateral Movement***		
Adversaries leveraging AI to phish their targets has come in as the top overall technique seen in Q2 2026. Generative AI programs can be programmed with a meta prompt in order to phish for sensitive information and create complex schemes including the use of LLMs for synthetic text, visual deepfakes of faces, and audio deepfakes of speech. Using these tools in combination or as a tool to spear phish individuals, companies, and/or industries is becoming increasingly common.	AML.M0018 - User Training AML.M0034 – Deepfake Detection	3040.0 (AISEC)
User Execution (AML.T0011) ***Execution***		
User Execution and phishing often are seen in combination, so it is no surprise to see this ATLAS attack technique come in as the #3 overall and #2 ATLAS technique seen this quarter. In order to gain execution on a target system, adversaries rely on specific actions taken by a user by a user, for example, opening a malicious document or file. The most popular sub-technique reported was the **Malicious Package (AML.T0011.001)**. Creating malicious software packages has always been a successful, albeit time-consuming, technique. With the use of AI, campaigns can be scaled exponentially. Other sub-techniques associated with User Execution include Unsafe AI Artifacts, Poisoned AI Agent Tool, and Malicious Link.	AML.M0011 - Restrict Library Loading AML.M0014 - Verify AI Artifacts AML.M0016 - Vulnerability Scanning AML.M0018 - User Training AML.M0023 - AI Bill of Materials	2870.0 (AISEC) 3048.0 (AISEC) 3040.0 (AISEC) 3066.0 (AISEC)

Suggested Actions

Based on the analysis of AI-enabled attacks of this quarter, we recommend focusing on the following mitigations:

- Ensure AI-specific security topics are included in **employee training** no less than annually for all teams involved in AI software and model creation and deployment, as well as data science and cybersecurity personnel.
  - *See See HITRUST CVID 2948.0 (AISEC), CVID 3066.0 (AISEC) and CVID 3048.0 (AISEC)*
- Prior to processing, **actively filter user inputs,** including attachments for suspicious and/or unexpected values or patterns which could be adversarial or malicious. Consider formulating filters in conjunction with a maintained, **documented inventory of data used to train, test, and validate AI models.**
  - *See CVID 2948.0 (AISEC), CVID 3066.0 (AISEC) and CVID 3048.0 (AISEC)*

Top MITRE ATT&CK Techniques and Mitigations

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

Commonly Sighted Technique in Q2 2026	MITRE Mitigations	HITRUST CVIDs
Phishing (T1566) ***Initial Access***		
Longstanding as the most common initial attack vector, the volume of this indicator validates the importance of anti-phishing training and email security. These three 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.	M1017 – User Training M1021 – Restrict Web-Based Content M1031 – Network Intrusion Prevention M1047 – Audit M1049 – Antivirus/Antimalware M1054 – Software Configuration	0189.0 (i1) 0343.0 (i1) 0599.0 (i1) 0873.0 (i1) 0880.0 (i1) 0884.0 (i1) 0886.1 (e1/i1) 0946.0 (i1) 2316.0 (e1/i1) 2365.0 (e1/i1) 2367.0 (e1/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.	M1016 – Vulnerability Scanning M1026 – Privileged Account Management M1030 – Network Segmentation M1035 – Limit Access to Resource Over Network M1037 – Filter Network Traffic M1048 – Application Isolation and Sandboxing M1050 – Exploit Protection M1051 – Update Software	0035.0 (e1/i1) 0043.0 (e1/i1) 0160.0 (e1/i1) 0943.2 (i1) 0946.0 (i1) 1369.0 (i1) 1398.0 (i1) 2317.1 (e1/i1) 2362.0 (e1/i1) 2367.0 (e1/i1

Continued on the next page

Commonly Sighted Technique in Q2 2026	MITRE Mitigations	HITRUST CVIDs
User Execution (T1204) ***Execution***		
Frequently occurring shortly after initial access, an adversary may rely on a user to complete specific actions in order to execute their malicious payload. This can occur by opening a malicious document file or link. This technique is often seen in combination with Phishing. A full spectrum of mitigating controls from user training to access restrictions to endpoint protection is necessary to thwart T1204.	M1017 – User Training M1021 – Restrict Web-Based Content M1031 – Network Intrusion Prevention M1033 – Limit Software Installation M1038 – Execution Prevention M1040 – Behavior Prevention on Endpoint	0189.0 (i1) 0343.0 (i1) 0873.0 (i1) 0880.0 (i1) 0884.0 (i1) 0875.1 (i1/e1) 0946.0 (i1) 1303.0 (e1/i1) 1313.0 (i1) 1989.0 (i1) 2071.0 (e1/i1) 2316.0 (e1/i1) 2368.0 (e1/i1)
Obfuscated Files or Information (T1027) ***Stealth***		
In combination with aforementioned techniques, malicious files and information may be hidden or obfuscated. Attackers may encrypt, archive or compress their payloads in order to avoid detection and suspicion. In addition to having a vigilant and informed user base, maintaining up-to-date antivirus/antimalware, and a prolific audit program can help avoid falling victim to Obfuscated Files.	M1017 – User Training M1040 – Behavior Prevention on Endpoint M1047 – Audit M1049 – Antivirus/Antimalware	0035.0 (e1/i1) 0873.0 (i1) 0875.1 (e1/i1) 0884.0 (i1) 0896.0 (e1/i1) 1989.0 (i1)
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 M1026 – Privileged Account Management M1033 – Limit Software Installation M1038 – Execution Prevention M1040 – Behavior Prevention on Endpoint M1042 – Disable or Remove Feature or Program M1045 – Code Signing M1047 – Audit M1049 – Antivirus/Antimalware	0035.0 (e1/i1) 0043.0 (e1/i1) 0189.0 (i1) 0873.0 (i1) 0884.0 (i1) 0875.1 (e1/i1) 1263.1 (i1) 1313.0 (i1) 1989.0 (i1) 2362.0 (i1/e1) 2363.0 (e1/i1)

Current Active Attacks

In addition to the above analysis of cyber threat indicator volume, we reviewed 144 real-world breaches reported during Q2 2026 and analyzed the techniques used to carry out those attacks. This analysis once again confirmed phishing-based attacks as the most prevalent during the last quarter. These findings remain consistent with the results of our quantitative threat analysis and continue to reinforce 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 2316.9 (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-xeffort 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 CVIDs 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)*
- Implement and maintain network protection mechanisms such as firewalls and application layer filtering proxy servers. These network protection mechanisms should be used to intercept, inspect and filter internet traffic as well as block malicious URLs, domain names, and IP addresses.
    - *See HITRUST CVID 0189.0 (i1)*

CONCLUSION

Cybersecurity assurance must reflect the threats organizations are most likely to face, not only the controls they have historically implemented. HITRUST's e1, i1, and r2 certifications are designed to account for this reality by using current threat and breach analysis to evaluate whether assessment requirements continue to address relevant attack techniques and effective mitigations. This ongoing review helps keep HITRUST assessments grounded in observed adversary behavior and responsive to changes in the threat environment.

HITRUST's AI Security Certification follows the same threat-informed approach, helping organizations protect AI-enabled services as new attack methods emerge and mature.

From the focused assurance provided by e1, to the broader implemented control expectations of i1, to the highly tailorable, risk-based assurance of r2, each HITRUST certification path benefits from continuous threat analysis. This helps organizations demonstrate that their security programs are not only aligned to recognized assurance requirements, but also positioned to defend against the attacks most relevant to today's operating environment.