HITRUST

HITRUST CSF THREAT & MITIGATION ANALYSIS

Q3 2026

Period Covered: 7/1/2026 to 9/30/2026

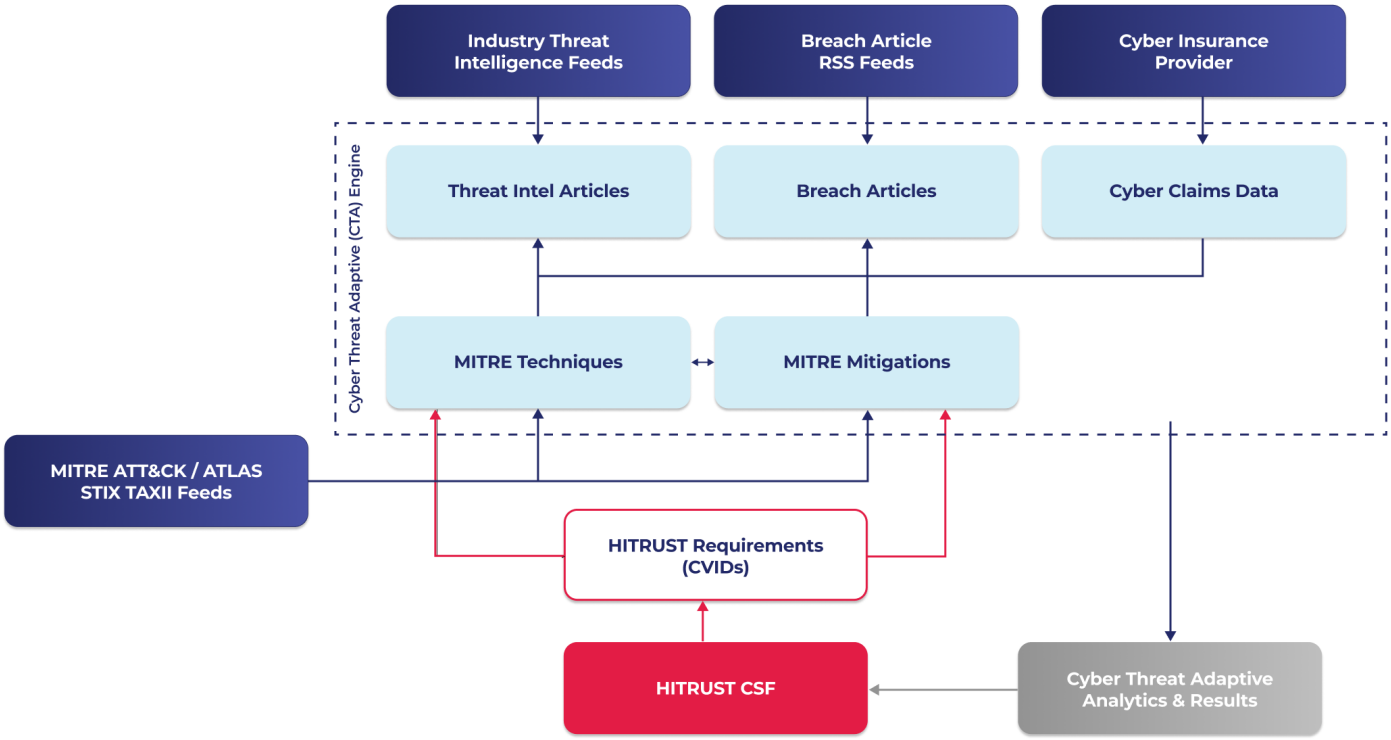
CSF Validation with Real-Time Cyber Threat Intel Analysis

As cyber threats evolve in real time to exploit new vulnerabilities, organizations and their security frameworks must constantly adapt to validate that their control selections still remain effective against rapidly developing threat activity.

For HITRUST, this need is addressed through the Cyber Threat Adaptive (CTA) process in which we continuously analyze current cyber threat intelligence and apply the insights we gain directly to the HITRUST CSF. This threat intelligence analysis provides valuable information that verifies HITRUST's requirements remain relevant and effective at responding to and mitigating active and 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. The threat data we use in our analysis, powered by the Cyber Threat Adaptive Engine, comes from Microsoft through Defender Threat Intelligence (Defender TI), that includes indicators of compromise, research reports, news articles, and blogs. The Engine analyses the sources, identifies, and assigns relevant MITRE ATT&CK and ATLAS technique tags. 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 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 interpreter, 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®

Alongside analyzing possible threats, the CTA process also provides HITRUST with insights into common entry points for attackers through an analysis of threat research articles, showcasing the ways in which attackers might try to exploit a system. Based on the research reviewed during Q3, the five most mentioned entry points are:

Entry Point	Count	% of Articles
General Malware	47	32.19%
Browser Malware	20	13.70%
Phishing	16	10.96%
Backdoor Malware	15	10.27%
Software Supply Chain	12	8.22%

This information allows for an additional layer of consideration for the requirements selected for inclusion in each of our assessment types. **The e1, i1, and r2 all provide robust coverage against threat actors at these five entry points,** with mitigations focused on providing employees with phishing awareness training, implementing and maintaining anti-malware, configuring browser protection mechanisms, vulnerability scanning, and software supply chain safeguards.

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 the review of 9,859 threat articles, 42,602,746 MITRE ATT&CK and MITRE ATLAS technique-level indicators, and 75 real-world breaches, HITRUST's four assessment types confidently provide ample coverage for potential threats.

Coverage of adversarial techniques:

The **e1** with its core 44 requirements is **98.39%**

The **i1** and **r2** have **100%** coverage

AI Security Certification is **97.30%** coverage of AI-focused techniques



Top MITRE ATLAS Techniques and Mitigations

With AI rapidly developing as a technology utilized and exploited by threat actors, AI-related techniques continue to represent a significant share of the observed threat activity in Q3 2026. The two most common AI techniques are listed below:

Commonly Sighted AI Techniques in Q3 2026	MITRE Mitigations	HITRUST CVIDs	Total Indicator Count	% Indicator Volume
Phishing (AML.T0052) *Initial Access, Lateral Movement*				
Phishing uses deceptive messages, links, or other content to persuade a person to reveal information, open malicious content, or take an action that benefits an attacker. It remained the leading ATLAS and overall technique in Q3, showing that AI-enhanced social engineering is here to stay and continues to scale as an effective attack method.	**AML.M0018** User Training **AML.M0034** Deepfake Detection	2071.0 2316.0 3040.0	5,704,240	62.14%
User Execution (AML.T0011) *Execution*				
User Execution depends on a user account to perform an action that allows malicious content to run, such as opening a file, following a link, or installing a package. It remained one of the most prominent ATLAS techniques in Q3 and commonly complements phishing, underscoring how often successful attacks still rely on human interaction.	**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 3040.0 3048.0 3066.0	3,389,669	36.93%

Phishing and User Execution are consistently at the top of the AI-technique charts for indicator count. Notably, these techniques are not distinctly AI-based, reinforcing a recurring theme: **AI is most successful at increasing the speed and scale of familiar human-centered attack methods, as opposed to creating new attack paths.** As a note, we limited our discussion of AI-techniques to the Top 2 due to the sharp decline in technique indicators for the remaining AI-techniques. The third most prevalent AI-technique, AML.T0088, had only 43,017 indicators, accounting for only 0.47% of the total AI-technique volume.

Suggested Actions You Can Take To Mitigate These AI Threats

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

- Ensure AI-specific security topics, such as AI-enabled phishing, are included in **employee training** no less than annually. The same dedicated **phishing awareness training** that mitigates traditional phishing is just as vital to protecting your workforce from AI enabled phishing.
    - *See HITRUST CVID 3040.0*
- **Actively filter user inputs** prior to processing, 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 HITRUST CVID 2948.0, CVID 3066.0 and CVID 3048.0*

Top MITRE ATT&CK Techniques and Mitigations

The top five for MITRE ATT&CK techniques for Q3 2026 has remained consistent since our last publication. Listed below are the full top five:

Commonly Sighted AI Techniques in Q3 2026	MITRE Mitigations	HITRUST CVIDs	Total Indicator Count	% Indicator Volume
Phishing (T1566) *Tactic: Initial Access*				
Phishing uses deceptive email, messages, links, or attachments to trick a person into revealing information or taking an action that helps an attacker. It remained the most frequently observed ATT&CK technique in Q3, reinforcing that human-targeted social engineering continues to be a primary route into organizations.	**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) 2071 (e1/i1) 2316.0 (e1/i1) 2365.0 (e1/i1) 2367.0 (e1/i1)	5,199,054	15.56%

continued on the next page

Commonly Sighted AI Techniques in Q3 2026	MITRE Mitigations	HITRUST CVIDs	Total Indicator Count	% Indicator Volume
Exploit Public-Facing Application (T1190) *Tactic: Initial Access*				
Exploit Public-Facing Application targets weaknesses in internet-facing applications, services, web servers, or related systems. Attackers use exposed vulnerabilities as a direct route into an environment, making timely patching, vulnerability management, and limiting unnecessary external exposure especially important. It remained one of the leading ATT&CK and overall techniques in Q3.	**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)	3,261,315	9.76%
User Execution (T1204) *Tactic: Execution*				
User Execution relies on a person to trigger the attacker's next step, such as opening a malicious attachment, following a link, or running a file. It frequently appears alongside phishing and remains a recurring high-volume technique because attackers can bypass technical barriers when a trusted user performs the action for them.	**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)	2,378,080	7.12%
Obfuscated Files or Information (T1027) *Tactic: Stealth*				
Attackers often try to hide malicious files, code, or commands so security tools and analysts have difficulty recognizing them. This can include encrypting, encoding, or compressing malicious content. These techniques are commonly used to evade detection during initial access or after an attacker has gained a foothold, making layered endpoint protection, behavioral monitoring, and analysis of suspicious files important safeguards.	**M1016** Vulnerability Scanning **M1050** Exploit Protection **M1051** Update Software	**0946.0 (i1)** **1369.0 (i1)** **2317.0 (e1/i1)** **2367.0 (e1/i1)**	2,249,069	6.73%

continued on the next page

Commonly Sighted AI Techniques in Q3 2026	MITRE Mitigations	HITRUST CVIDs	Total Indicator Count	% Indicator Volume
Command and Scripting Interpreter (T1059) *Tactic: Execution*				
Attackers often try to hide malicious files, code, or commands so security tools and analysts have difficulty recognizing them. This can include encrypting, encoding, or compressing malicious content. These techniques are commonly used to evade detection during initial access or after an attacker has gained a foothold, making layered endpoint protection, behavioral monitoring, and analysis of suspicious files important safeguards.	**M1049** Antivirus/Antimalware **M1047** Audit **M1040** Behavior Prevention on Endpoint **M1045** Code Signing **M1042** Disable or Remove Feature or Program **M1038** Execution Prevention **M1033** Limit Software Installation **M1026** Privileged Account Management **M1021** Restrict Web-Based Content	0946.0 (i1) 1369.0 (i1) 2317.0 (e1/i1) 2367.0 (e1/i1)	1,995,627	5.97%

Suggested Actions You Can Take To Mitigate These Threats

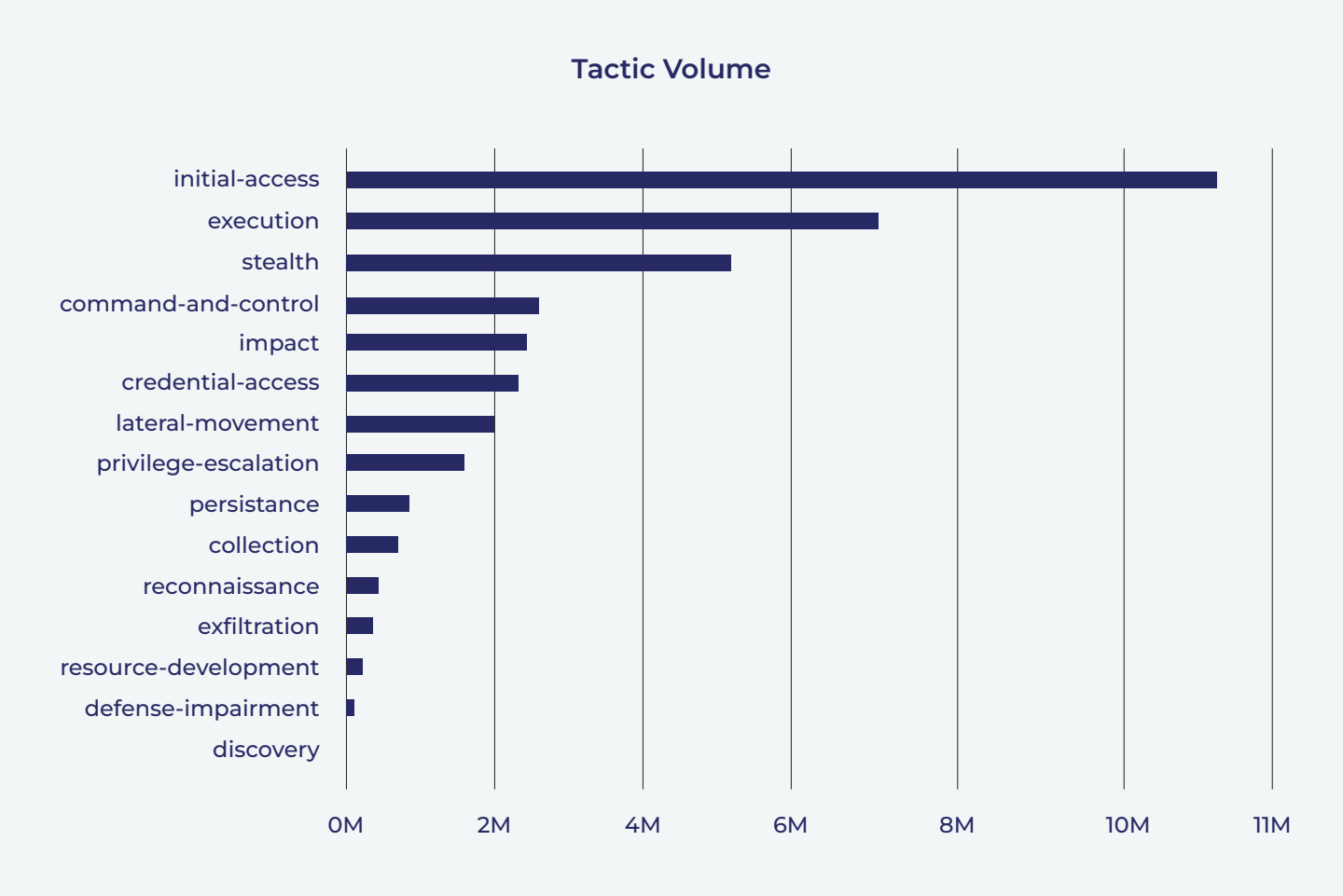
Based on the results of this quarter, we recommend the following:

- 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 effort attacks.
  - *See HITRUST CVIDs 0884.0 (i1) and 0873.0 (i1)*
- Once a potential **technical vulnerability has been discovered**, identify associated risks and actions to be taken and perform those actions within formally documented, risk-tiered remediation timeframes (e.g, patching an entry in the CISA KEV catalog based on CVSS score). Prioritize internet-facing applications, client software, and remotely accessible services where exploitation could enable initial access, execution, and lateral movement.
  - *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)*

Cyber Threat Goal Analysis

To complement the analysis of individual techniques, HITRUST also considers the progression of adversary activity across the MITRE ATT&CK tactics. This perspective illustrates how e1 and i1 requirements provide coverage across the most impactful attack phases. Below, we've ranked the MITRE ATT&CK tactics based on volume.



Focusing on the top 5 tactics (initial-access, execution, stealth, command-and-control, and impact) we can evaluate coverage based on downstream technique to mitigation to requirement mappings.

Top Attack Phases	Threat Volume	e1 Coverage	i1 Coverage
Initial Access	31.13%	0035.0, 0043.0, 0149.0, 0875.1, 1303.0, 2071.0, 2316.0, 2317.1, 2321.0, 2322.0, 2366.0, 2367.0, 3207.0	0035.0, 0043.0, 0149.0, 0189.0, 0269.0, 0316.0, 0343.0, 0427.0, 0875.1, 0884.0, 1303.0, 1369.0, 1375.0, 1398.0, 1908.0, 2071.0, 2316.0, 2317.1, 2321.0, 2322.0, 2366.0, 2367.0, 3207.0
Execution	19.45%	0035.0, 0043.0, 0149.0, 0160.0, 0875.1, 0943.2, 1002.0, 1303.0, 1896.0, 2071.0, 2316.0, 2317.1, 2367.0, 2368.0	0035.0, 0043.0, 0149.0, 0160.0, 0189.0, 0343.0, 0873.0, 0875.1, 0884.0, 0943.2, ,1002.0, 1303.0, 1313.0, 1369.0, 1896.0, 1908.0, 1989.0, 2071.0, 2316.0, 2317.1, 2367.0, 2368.0
Stealth	13.87%	0035.0, 0043.0, 0149.0, 0160.0, 0875.1, 0943.2, 1303.0, 1918.0, 2071.0, 2316.0, 2326.0, 2368.0	0035.0, 0043.0, 0149.0, 0160.0, 0189.0, 0343.0, 0488.0, 0873.0, 0875.1, 0884.0, 0943.2, 1203.1, 1218.0, 1303.0, 1313.0, 1918.0, 1989.0, 2071.0, 2316.0, 2326.0, 2368.0
Command & Control	6.74%	0149.0, 0160.0, 0875.1	0122.0, 0149.0, 0160.0, 0189.0, 0875.1, 0946.0
Impact	6.59%	0160.0, 0875.1, 0901.0, 0903.0, 1488.0, 2071.0, 2316.0, 2317.1, 2318.0, 2326.0	0160.0, 0189.0, 0343.0, 0569.0, 0875.1, 0884.0, 0901.0, 0902.0, 0903.0, 1092.0, 1289.0, 1313.0, 1369.0, 1488.0, 1506.0, 1508.0, 1514.0, 1542.0, 1954.0, 1989.0, 2071.0, 2316.0, 2317.1, 2318.0, 2326.0

The tactic-level results reinforce that HITRUST's requirements provide coverage across the various goals of an attack, rather than concentrating on isolated techniques. Initial Access, Execution, and Stealth account for 64.45% of observed threat volume, while the five leading tactics collectively represent 77.78%. The e1 establishes essential safeguards across each of these tactics, and the i1 expands that coverage through additional requirements—particularly for detecting, disrupting, and responding to activity associated with the Command and Control and Impact tactics. Together, these results demonstrate a layered defense against the attack activity most frequently observed during the quarter.

CONCLUSION

With a rapidly evolving landscape thanks to the introduction, growth, and usage of AI-based technologies by threat actors, cybersecurity assurance must constantly adapt to the current threats that organizations are actively facing, rather than just implementing the same controls.

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 at a rapid rate.

From the focused, essential assurance provided by e1, to the broader implemented control expectations of i1, to the highly tailorable, risk-based assurance of r2, to the rapidly developing, future-forward, and adaptive assurance of the AI certification, 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 they are also positioned to defend against the attacks most relevant to today's environment.