digiDations

ATLAS Security Validation for CCoP 2.0

Mapping the ATLAS Security Validation Platform™ to the CSA Cybersecurity Code of Practice for CII 2.0 (CCoP 2.0)

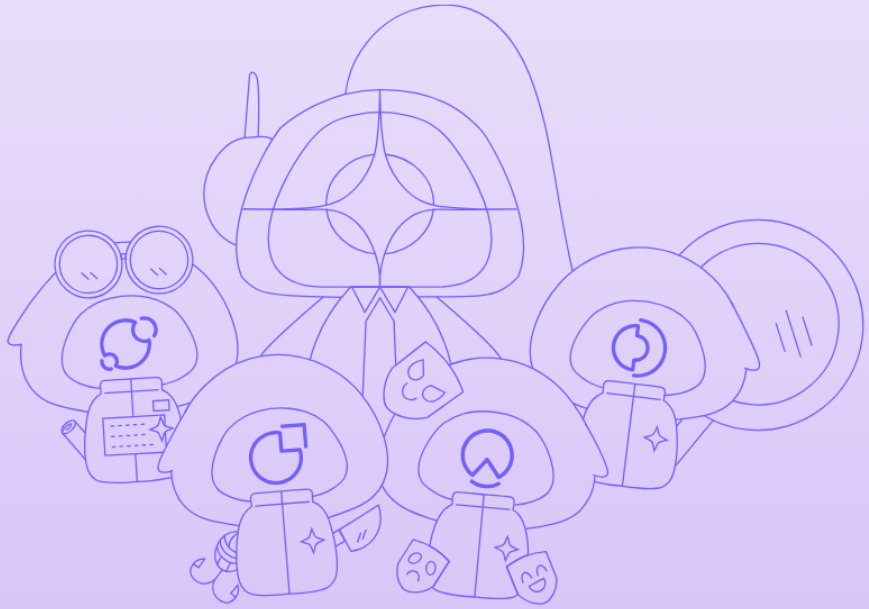

Table of Contents

Executive Summary **3**

Table 1: Protection Requirement (Clause 5) 5

Table 2: Detection Requirements (Clause 6) 9

Table 3: Response and Recovery Requirement (Clause 7) 12

Table 4: Operational Technology (OT) Security Requirements (Clause 10) 14

Overview of CSA's Cybersecurity Code of Practice 2.0 15

Key Cybersecurity Expectation for CII owners 16

The Challenge of Demonstrating Security Control Effectiveness 17

ATLAS Security Validation Platform **18**

Overview of the ATLAS Security Validation Platform 18

ATLAS Security Validation Methodology 19

Capabilities Supporting Security Control Validation 20

Going Beyond Compliance **21**

Limitations of Traditional Security Assessments 21

Continuous Security Validation 23

Strengthening Cyber Resilience 24

About digiDations **25**

Executive Summary

As the cyber threat landscape is rapidly evolving, ransomware and advanced persistence threat (APT) groups are getting more prevalent. In addition, due to the nature of Critical Information Infrastructure (CII), they are often a top target. Cyber Security Agency of Singapore (CSA) has established the **Cybersecurity Code of Practice for Critical Information Infrastructure 2.0 (CCoP 2.0)** to specify the minimum requirements that Critical Information Infrastructure Owners (CIIO) should implement to ensure the cybersecurity of its CII.

Under the CCoP 2.0, CIIs are required to demonstrate that their security controls operate effectively against real-world adversary tactics, techniques, and procedures (TTPs). Traditional security assessments such as periodic penetration testing or vulnerability scans often provide only point-in-time insights and may not fully validate whether deployed security controls can detect, prevent, and respond to modern cyber threats.

This white paper explains how the **ATLAS Security Validation Platform**™ from digiDations helps CIIs comply with the requirements of the CCoP 2.0 by continuously validating the effectiveness of their cybersecurity defenses. ATLAS uses adversarial simulation techniques to emulate real-world threat scenarios and evaluate the performance of security controls, detection rules, and incident response processes across the organization's environment.

The platform supports multiple areas highlighted in the CCoP 2.0, including the **Protection Requirement, Detection Requirement, Response & Recovery Requirement and Operational Technology (OT) Security Requirements.** Through continuous security validation, organizations can verify whether their defenses operate as intended, identify control gaps, and improve their ability to detect and respond to emerging threats.

By aligning continuous security validation with regulatory expectations, ATLAS enables CIIs to move beyond theoretical compliance and gain measurable assurance of their cybersecurity posture. This approach strengthens operational resilience and helps organizations better defend against evolving threat actors targeting respective CIIs.

CCoP 2.0 Compliance Mapping Table

The following tables provide a mapping between selected clauses from the **Cyber Security Agency of Singapore Cybersecurity Code of Practice for Critical Infrastructure 2.0 (CCoP 2.0)** and capabilities of the **ATLAS Security Validation Platform**.

The mapping illustrates how ATLAS can support organizations in **validating the effectiveness of cybersecurity controls, monitoring mechanisms, and incident response processes** referenced in the CSA CCoP 2.0. By simulating realistic adversary techniques and evaluating how security controls perform during these simulations, organizations can gain measurable insight into the operational effectiveness of their defenses.

The ATLAS Security Validation Platform **does not itself establish regulatory compliance**. Compliance with the CCoP 2.0 Guidelines requires CIIs to implement appropriate governance, risk management processes, and security controls in accordance with CSA supervisory expectations. ATLAS supports these efforts by providing continuous validation capabilities that help organizations assess whether their implemented controls and security operations function effectively against realistic threat scenarios.

The mapping focuses on CCoP 2.0 clauses most closely related to cybersecurity control validation, including Clauses 5 (Protection Requirement), Clause 6 (Detection Requirements), Clause 7 (Response and Recovery Requirement) and Clause 10 (Operational Technology (OT) Security Requirements).

Table 1: Protection Requirement (Clause 5)

CCoP 2.0 Clause	CCoP 2.0 Requirement	ATLAS Validation Capability	Validation Evidence
CCoP 5.5.3	**The CIIO shall:** **(a) Implement network security mechanisms between the different network segments of the CII to detect and block malicious network traffic and to secure network communications; and** **(b) Establish mechanisms and processes to isolate affected network segments of the CII in the event of a cybersecurity incident.**	ATLAS simulates realistic network traffic based on emerging threat intelligence, allowing network security control to be validated for its effectiveness across different segments.	Simulation result display whether a simulated network traffic across segments is being blocked and logged by the respective network security control.
CCoP 5.6.2	**The CIIO shall ensure that the CII is not connected to any network outside of the CII except where necessary for operating the CII. Where such connections are necessary, the CIIO shall:** **(a) Implement network security mechanisms between the CII and**	ATLAS simulates realistic network traffic based on emerging threat intelligence, allowing network security control to be validated for its effectiveness across different segments.	Simulation result display whether a simulated network traffic across segments is being blocked and logged by the respective network security control.

	the network to detect and block malicious network traffic and to secure network communications; and		
CCoP 5.12.5	**For a CII that includes web application systems, the CIIO shall reference the latest Open Web Application Security Project (OWASP) or equivalent application security guidelines when designing, developing and testing applications to minimise application security risks.**	ATLAS is capable in simulating web attack, including but not limited to the following: - SQL Injection - Cross Site Scripting (XSS) - XML External Entity (XXE) - Cross Site Request Forgery (CSRF) - Server-Side Request Forgery (SSRF) - Latest CVE of Web Framework	Simulation result display whether a simulated web application vulnerability is being executed successfully or not successfully.
CCoP 5.12.6	**For a CII that includes web application systems that are internet-facing, the CIIO shall also implement a Web Application Firewall (WAF) to monitor for, detect and block web application threats.**	ATLAS is capable in simulating web attack, allowing security team to validate the effectiveness of the WAF in place.	Simulation result display whether the WAF can block relevant web attacks.

CCoP 5.16.1	**The CIIO shall establish a red teaming or purple teaming attack simulation plan which identifies, among other things:** **(a) Objectives to be achieved;** **(c) Assessment methodology, including planning and attack preparation, attack execution, clean-up and containment, blue team report and reconciliation, recommendations and remediation;** **(e) Mitigation measures to minimise potential business impact or disruption; and** **(f) Recovery plan.**	ATLAS contains realistic simulation scenario based on latest threat intelligence related to relevant ransomware or APT groups. The payloads utilized for each scenario are clearly displayed on the ATLAS web UI; CIIO can use this information on the ATLAS UI to assist them in planning purple team exercises. To minimize potential business impact, ATLAS comes with the following features: - Components such as validator and isolator allows simulation to conducted in a safe and controlled manner Payloads are pair with respective "rewind" command to ensure action perform are reversible. For example, creating windows registry key command will have respective delete windows registry key command to undo the action	N.A

CCoP 5.16.2	**The CIIO shall conduct a red teaming or purple teaming attack simulation on its CII at least once every 24 months to test and validate the effectiveness of its cybersecurity measures against prevalent cybersecurity threats. The first instance of the attack simulation is to be completed no later than 12 months after the Compliance Date.**	With ATLAS, CIIO can execute simulation as and when required. This allows CIIO to take a proactive measure continuously in defending against latest threat.	N.A
CCoP 5.16.3	**The CIIO shall, if requested by the Commissioner, submit a copy of the report of any completed red teaming or purple teaming attack simulation, along with the CIIO's remediation plans, to the Commissioner within 30 working days of receiving the request.**	ATLAS can generate two types of reports to assist in the preparation of the submission to the commissioner: - A high-level summary PDF detailing the simulation status (e.g blocked status, etc) - A detailed CSV file containing information such as payload run, timestamps and other relevant data.	N.A

Table 2: Detection Requirements (Clause 6)

CCoP 2.0 Clause	CCoP 2.0 Requirement	ATLAS Validation Capability	Validation Evidence
CCoP 6.1.2	**The CIIO shall also generate, collect and store the following categories of logs to provide visibility of network activities within the CII and between the CII and networks outside of the CII:** **(a) Network Firewall logs;** **(c) Web Proxy logs (TBC)** **(d) Network Intrusion Detection/Prevention System (NIDS/NIPS) logs**	ATLAS comes with a log gateway component which store relevant logs from respective security product (NGFW, NIDS/NIPS, EDR, SIEM, etc). This allows CIIO to have a quick overview of the current logs that are generated within their environment. In addition, the log gateway only stores relevant logs related to the components of ATLAS (i.e.Validator and Isolator).	ATLAS Web UI can be used to view the current logs that the log gateway contains.
CCoP 6.2.1	**The CIIO shall establish and implement mechanisms and processes for the purposes of:** **(c) Analysing all such cybersecurity events, including correlating between cybersecurity events, and determining whether**	With ATLAS, CIIO can execute simulation as and when required. This allows CIIO to effectively validate the current mechanisms and processes that are in place.	N.A

	there is or has been any cybersecurity incident; and **(d) Triggering applicable incident reporting, response and recovery plans if there is or has been any cybersecurity incident.**		
CCoP 6.2.2	**For the purposes of monitoring and detecting cybersecurity events, the mechanisms and processes established by the CIIO shall include:** **(a) Scanning for indicators of compromise (IOCs), including IP addresses, Uniform Resource Locator (URL), domains and hashes;** **(b) Establishing the normal day-to-day operational activities and network traffic in the CII, and using this as a baseline against which the CIIO is to monitor for deviations and anomalous activities; and**	With ATLAS, CIIO can execute simulation as and when required. This allows CIIs to effectively validate the current mechanisms and processes that are in place.	N.A

	(c) Ensuring that alerts for further investigation are triggered for all deviations and anomalous activities that are detected.		

Table 3: Response and Recovery Requirement (Clause 7)

CCoP 2.0 Clause	CCoP 2.0 Requirement	ATLAS Validation Capability	Validation Evidence
CCoP 7.1.2	**The CIIO shall ensure that the CIRT is trained and equipped with the necessary resources to respond to cybersecurity incidents.**	With ATLAS, CIIO can run simulation as and when required to ensure that the CIRT is able to response to incident in real time. In this way, CIIO can identify potential gap in the CIRT such as lack of necessary resources.	Simulation result provides detailed timestamp of different payloads ran. Allowing CIIs to measure key indicator such as Mean-Time-To-Detect and Mean-Time-To-Response.
CCoP 7.3.1	**The CIIO shall conduct scenario-based cybersecurity exercises to test and validate the effectiveness of the following plans:** **(a) Cybersecurity Incident Response Plan;**	With ATLAS, CIIO can execute simulation as and when required. This allows CIIO to effectively validate the current mechanisms and processes that are in place.	Simulation result provides detailed timestamp of different payloads ran. Allowing CIIs to measure key indicator such as Mean-Time-To-Detect and Mean-Time-To-Response; These can be used to validate the effectiveness of the Incident Response plan.
CCoP 7.3.3	**In designing the incident response scenarios for the cybersecurity exercises, the CIIO shall include elements that test and validate:**	ATLAS contains realistic simulation scenario based on latest threat intelligence related to relevant ransomware or APT groups. This allow CIIO to simulate a realistic APT/ransomware campaign to test	Simulation result provides detailed timestamp of different payloads ran. Allowing CIIs to measure key indicator such as Mean-Time-To-Detect and Mean-Time-To-Response; These can be used to validate the

	(a) Responses to threats and vulnerabilities identified from threat intelligence; **(c) Continued monitoring for further cybersecurity threats and incidents even during incident response; and** **(d) Adequacy of the CIIO's resources and capabilities to respond to cybersecurity incidents.**	and validate the incident response process.	effectiveness of the Incident Response plan.

Table 4: Operational Technology (OT) Security Requirements (Clause 10)

CCoP 2.0 Clause	CCoP 2.0 Requirement	ATLAS Validation Capability	Validation Evidence
CCoP 10.2.2	**The CIIO shall monitor the data flows from the OT CII to any enterprise network for anomalies and trigger an alert for investigation when any anomaly is detected.**	ATLAS simulates realistic network traffic based on emerging threat intelligence, allowing network security control to be validated for its effectiveness across different segments.	Simulation result display whether a simulated network traffic across segments is being blocked and logged by the respective network security control.

CSA Cybersecurity Code of Practice for Critical Information Infrastructure 2.0

The **Cyber Security Agency of Singapore Code of Practice for Critical Information Infrastructure 2.0**, revised in **December 2022**, provide a code of practice for Critical Information Infrastructure Owner (CIIO) to ensure the minimum requirements needed to ensure the cybersecurity of its Critical Information Infrastructure (CII); The code of practice only specific the minimum requirements, the CIIOs is expected to implement measures beyond those stipulated in the CCoP 2.0 to further strengthen the cybersecurity of the CII based on its own risk profile.

As CIIs across Singapore continue to expand their digital services and interconnected system environments, the complexity of cyber risks and threats has increased significantly. The Cybersecurity Code of Practice (CCoP) 2.0 issued by the Cyber Security Agency of Singapore (CSA) underscores the need for Critical Information Infrastructure (CII) owners to adopt a systematic and risk-based approach to strengthening their cybersecurity posture, ensuring the protection, resilience, and trustworthiness of essential services.

Overview of CSA's Cybersecurity Code of Practice 2.0

The CCoP 2.0 sets out a comprehensive framework of cybersecurity principles and controls to guide CII owners in establishing, implementing, and maintaining robust cybersecurity measures. It covers a broad range of requirements such as Audit, Governance, Identification, Protection, Detection, Response & Recovery, Cyber Resiliency, Cybersecurity Training & Awareness and Operation Technology Security.

Rather than prescribing specific technical solutions, CCoP 2.0 defines baseline cybersecurity requirements and outcomes that CII owners must meet, while allowing flexibility in implementation based on each organization's operational context, technology landscape, and risk profile. This approach helps ensure that cybersecurity measures remain effective, proportionate, and sustainable.

By defining these standards, CSA aims to strengthen the overall cybersecurity resilience of Singapore's critical sectors. This ensures that essential services remain available and secure even in the face of evolving cyber threats, system disruptions, and operational challenges.

Key Cybersecurity Expectation for CII owners

The CCoP 2.0 outlines specific cybersecurity outcomes that CII owners are expected to achieve to protect their infrastructure and data assets. These expectations emphasize the importance of implementing strong preventive, detective, and corrective controls across people, process, and technology domains.

CII owners should maintain secure system configurations, enforce least-privilege access controls, and deploy continuous monitoring mechanisms to detect suspicious or anomalous activities. Cybersecurity operations should be capable of swiftly identifying, analyzing, and responding to incidents, minimizing potential disruptions to essential services.

Continuous monitoring, regular validation of security measures, and ongoing risk assessments are essential to ensure that cybersecurity programs remain effective in the face of emerging threats and technological changes.

The Challenge of Demonstrating Security Control Effectiveness

For owners of Critical Information Infrastructure across Singapore's essential service sectors, cybersecurity is not merely a technical responsibility. It is a core obligation to the public, to regulators, and to the continuity of services that millions depend on.

CCoP 2.0 establishes a structured set of mandatory requirements spanning governance, asset protection, detection, and response. Yet meeting these requirements raises a harder question that compliance frameworks alone cannot answer: are the controls that organisations have put in place actually capable of stopping a determined adversary?

Traditional security assessments, whether vulnerability scans, penetration tests, or scheduled audits, provide valuable but time-limited assurance. They confirm the state of defences at a specific moment, while the threat landscape shifts continuously around them. Sophisticated threat actors invest in understanding how critical infrastructure is defended, and they exploit the windows between assessments to probe for weaknesses that periodic testing may never surface.

CCoP 2.0 recognises this by mandating adversarial attack simulations alongside conventional testing methods. But the cadence of scheduled exercises, typically every 12 to 24 months, means that control effectiveness cannot be assumed between cycles. For boards accountable for essential service resilience, that gap represents unquantified risk that deserves a more continuous answer.

ATLAS Security Validation Platform

Organizations today operate in increasingly complex technology environments where traditional security assessments alone may not provide sufficient visibility into the effectiveness of deployed security controls. As cyber threats evolve, organizations require continuous methods to validate whether defensive technologies, monitoring mechanisms, and response processes operate effectively against modern adversary techniques.

The **ATLAS Security Validation Platform** from digiDations enables organizations to continuously test and validate the effectiveness of their cybersecurity defenses. By simulating realistic adversary techniques in controlled scenarios, the platform provides measurable insight into how security controls detect, prevent, and respond to potential attacks across the organization's environment.

Through continuous validation, organizations can identify gaps in detection coverage, evaluate the effectiveness of monitoring and response processes, and strengthen their overall cybersecurity posture.

Overview of the ATLAS Security Validation Platform

The **ATLAS Security Validation Platform** is designed to evaluate the operational effectiveness of security controls through adversarial simulation. The platform replicates techniques used by real-world threat actors and executes them safely within controlled testing scenarios.

These simulations enable organizations to observe how deployed security technologies — including endpoint protection platforms, network security controls, and security monitoring systems — respond to adversary techniques across different stages of the attack lifecycle.

Unlike traditional security assessments that provide only periodic insight, ATLAS supports **continuous validation**, allowing organizations to regularly test defensive capabilities as infrastructure changes and new threats emerge.

ATLAS Security Validation Methodology

ATLAS follows a structured validation methodology that helps organizations continuously evaluate and improve their cybersecurity defenses.

This validation process can be viewed as four stages:

Verify – Operational Design

Validate baseline configurations and confirm that foundational security controls are functioning correctly.

Evaluate – Security Effectiveness

Simulate realistic adversary techniques to determine whether deployed security technologies detect or prevent malicious activity.

Analyze – Threat Correlation and Security Operations Efficiency

Assess how effectively monitoring systems and analytics platforms correlate alerts and identify potential attack activity across the environment.

Optimize – Incident Response Readiness

Evaluate incident response processes and identify opportunities to improve detection accuracy and response speed.

Through this continuous validation cycle, organizations can measure the effectiveness of their security defenses and strengthen operational readiness.

Capabilities Supporting Security Control Validation

The ATLAS Security Validation Platform provides several capabilities that help organizations validate the effectiveness of their cybersecurity defenses.

First, the platform enables **realistic adversary simulation**, replicating techniques aligned with established attack frameworks such as MITRE ATT&CK. These simulations allow organizations to evaluate how security technologies detect and respond to specific adversary behaviors.

Second, ATLAS supports **continuous validation of security controls**, allowing organizations to regularly test detection mechanisms, monitoring systems, and defensive technologies against simulated attack scenarios.

Third, the platform provides **visibility into detection and response performance**, enabling security teams to identify gaps in monitoring coverage, detection logic, and incident response processes.

By providing continuous insight into how security controls operate under simulated attack conditions, ATLAS enables organizations to strengthen their defensive capabilities and maintain greater confidence in the effectiveness of their cybersecurity controls.

Going Beyond Compliance

Achieving compliance with CCoP 2.0 is a legal obligation for CII owners. It is also just the starting point.

The Code was developed precisely because Singapore's threat environment had outpaced what earlier regulatory frameworks were designed to address. Threat actors targeting critical infrastructure sectors have become more capable, more patient, and more deliberate in their methods. Regulatory requirements, by their nature, reflect the threat landscape at the time of drafting. They cannot anticipate every evolution that occurs between review cycles.

What this means in practice is that an organization can satisfy every clause of CCoP 2.0 and still carry meaningful exposure if its controls have not been validated against current adversary behavior. Compliance confirms that the right measures are in place. It does not confirm that those measures will hold under the pressure of a real attack today.

Senior leadership in CII organizations increasingly recognize this distinction. The true measure of a security programme is not whether it passes an audit, but whether it can protect essential services when it matters most. Organizations that move beyond scheduled compliance activities to adopt continuous, intelligence-driven validation of their defenses are better positioned to detect threats earlier, respond more effectively, and maintain the trust that their role in Singapore's critical infrastructure demands.

The CSA CCoP 2.0 framework defines the obligation. digiDations ATLAS provides the means to fulfil it on a continuous basis.

Limitations of Traditional Security Assessments

Traditional security assessments such as penetration testing and red team exercises have long been used to evaluate an organization's cybersecurity posture. While these assessments can provide valuable insights into vulnerabilities and potential attack paths, they also have several inherent limitations.

Penetration testing engagements are typically conducted over limited timeframes and depend heavily on the expertise and experience of the testers involved. As a result, the range of techniques explored during an engagement may be constrained by time and available resources. In addition, testing activities conducted in production environments often require safeguards to prevent operational disruption, limiting the realism of the assessment.

Similarly, red team exercises simulate adversarial behavior to test detection and response capabilities, but these exercises are often performed infrequently—such as annually or quarterly. Because of their limited duration and scope, they may not provide continuous visibility into how defensive controls perform as systems evolve and new threats emerge.

As a result, these traditional approaches provide **point-in-time insights** rather than continuous assurance of security control effectiveness.

Continuous Security Validation

To address the limitations of traditional assessments, organizations are increasingly adopting **continuous security validation** practices. This approach involves regularly simulating adversary techniques to evaluate how security controls detect and respond to potential attacks across the organization's technology environment.

By replicating realistic attack techniques and observing how defensive technologies respond, security teams can identify gaps in detection coverage, validate the effectiveness of monitoring systems, and measure the readiness of incident response processes.

Continuous validation provides a more comprehensive understanding of an organization's security posture by testing defensive capabilities against a wide range of adversary techniques across multiple stages of the attack lifecycle.

Strengthening Cyber Resilience

Continuous security validation enables organizations to move beyond a purely compliance-driven approach to cybersecurity. Instead of focusing solely on meeting regulatory requirements, organizations can continuously measure and improve the effectiveness of their defensive capabilities.

The **ATLAS Security Validation Platform** supports this approach by enabling organizations to safely simulate real-world adversary techniques and evaluate how security controls perform during these simulations. By incorporating continuous validation into their cybersecurity programs, organizations can strengthen their ability to detect and respond to emerging threats while maintaining greater confidence in the effectiveness of their security defenses.

behavior across different stages of the attack lifecycle. These simulations enable security teams to observe how existing defensive tools and processes respond to real-world attack techniques.

Unlike traditional point-in-time assessments, ATLAS supports continuous validation of security controls across on-premises, cloud, and hybrid environments. The platform orchestrates controlled adversarial simulations and analyzes the resulting telemetry to determine whether security controls successfully detect, block, or respond to simulated attack activities.

The platform architecture includes multiple components that work together to execute simulations and collect validation results, including a centralized management console, simulation agents, telemetry collectors, and sandbox environments for executing high-risk attack behaviors safely. These components enable organizations to validate detection, response, and mitigation capabilities across their entire security architecture.

About digiDations

digiDations is an AI Native cybersecurity company helping organizations replace security assumptions with continuous, measurable validation. The question it answers is not whether an organization has vulnerabilities. It is whether their defenses can keep up with the threats targeting them right now.

Founded by cybersecurity veterans and AI researchers, digiDations built its product portfolio on Digital Mind, a proprietary AI foundation that continuously collects, correlates, and operationalizes real-world attack intelligence. The AI-Driven AEV portfolio includes ATLAS for Security Validation, APOLLO for Continuous Automated Red Teaming, and HELIOS for External Attack Surface Management. ORION for Threat Intelligence extends digiDations' CTEM coverage with adversary intelligence and visibility into emerging attack surfaces.

digiDations is building toward Autonomous Cyber Defense with TARA AI, the Autonomous CTEM Agent that self-directs across all four products: determining which scenarios to run, orchestrating execution, interpreting results, and generating reports, with teams approving decisions rather than defining the workflow.