digiDations

digiDations Solution Mapping to BNM

Mapping the digiDations Platform to the Bank Negara Malaysia's Risk Management in Technology Policy

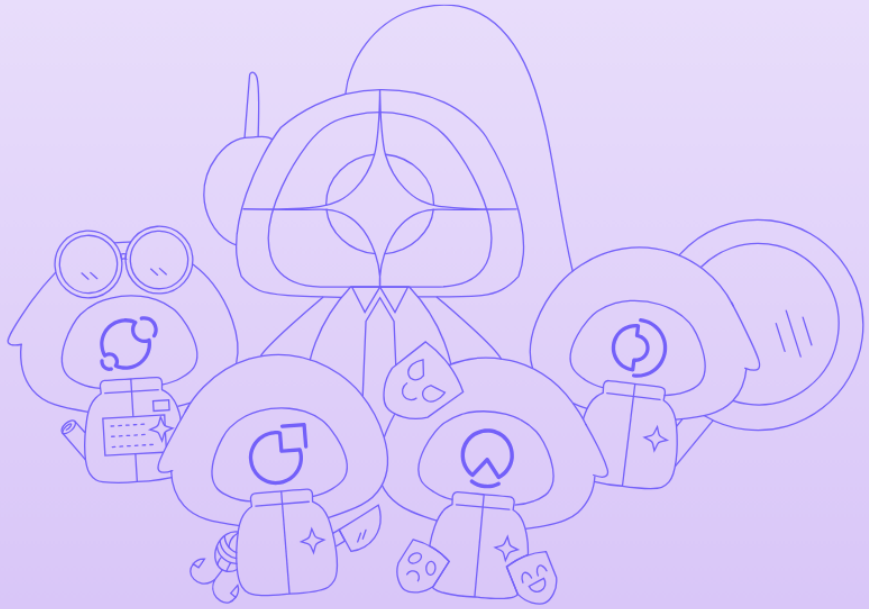

Table of Contents

Executive Summary

Financial institutions in Malaysia operate within an increasingly complex cyber threat landscape. To address these risks, Bank Negara Malaysia (BNM) has issued the Risk Management in Technology (RMiT) Policy Document (BNM/RH/PD 028-98, issued 28 November 2025), which sets out minimum requirements for financial institutions to manage technology risk, including cyber risk. The RMiT applies to licensed banks, investment banks, Islamic banks, insurers, takaful operators, prescribed development financial institutions, approved e-money issuers, operators of designated payment systems, registered merchant acquirers, and intermediary remittance institutions.

A key requirement of the RMiT is for financial institutions 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 digiDations solutions helps financial institutions address the requirements of the BNM RMiT. digiDations offers three separate solution: ATLAS, a continuous adversarial simulation platform that emulates real-world threat scenarios and evaluates the performance of security controls, detection rules, and incident response processes; ORION, a threat intelligence platform that provides IOC, IOA, and IOB coverage including supply chain threats and AI-powered attack techniques; and HELIOS, an External Attack Surface Management (EASM) platform that provides continuous monitoring across public-facing assets and the dark web to detect data breach incidents and threat actor activity targeting the organization.

Together, these capabilities support multiple areas of the RMiT, including the Technology Risk Management Framework, Cybersecurity Management and Cyber Resilience Framework, Red Team simulation requirements, cyber threat intelligence requirements, and the network security, data security, and SOC control measures outlined in Appendix 5 Parts A, B and C. Through continuous validation, threat intelligence, and external exposure monitoring, financial institutions can verify whether their defenses operate as intended, identify control gaps, and improve their ability to detect and respond to emerging threats.

By aligning these capabilities with BNM's regulatory expectations, the digiDations platform enables financial institutions to move beyond theoretical compliance and gain measurable, continuous assurance of their cybersecurity posture, strengthening operational resilience against evolving threat actors targeting the Malaysian financial sector.

RMiT Mapping

The following tables provide a mapping between selected clauses from BNM's Risk Management in Technology (RMiT) Policy Document and the capabilities of the digiDations platform, covering ATLAS, ORION, and HELIOS.

The mapping illustrates how the digiDations solutions supports financial institutions in validating the effectiveness of cybersecurity controls, monitoring mechanisms, and incident response processes referenced in the RMiT. By simulating realistic adversary techniques, providing actionable threat intelligence, and monitoring external exposure, financial institutions can gain measurable insight into the operational effectiveness of their defenses across their entire security program.

The digiDations solutions does not itself establish regulatory compliance. Compliance with the RMiT requires financial institutions to implement appropriate governance, risk management processes, and security controls in accordance with BNM's supervisory expectations. The digiDations solutions supports these efforts by providing continuous validation, threat intelligence, and external attack surface management capabilities that help organizations assess whether their implemented controls and security operations function effectively against realistic threat scenarios.

The mapping focuses on RMiT clauses most closely related to cybersecurity control validation, threat intelligence, and external exposure management, including Section 9 (Technology Risk Management), Section 10 (Technology Operations Management), Section 11 (Cybersecurity Management), and Appendix 5 Parts A, B and C (Network Security, Data Security, and Security Operations Center control measures).

Table 1: Technology Risk Management (Section 9)

BNM RMiT Clause	RMiT Requirement	digiDations Solution Capabilities	Supporting Evidence
RMiT 9.2(c)	The TRMF must include the identification of technology risks to which the financial institution is exposed, including risks from the adoption of new or emerging technology.	ATLAS simulates realistic adversary campaigns and attack techniques based on threat group behavior and emerging threat intelligence. These simulations help identify gaps in defensive coverage, revealing previously unrecognized attack paths and technology-specific risk exposures.	ATLAS simulation findings highlight detection and control gaps, enabling organizations to identify new and emerging risk exposures across their technology environment.
RMiT 9.2(g)	The TRMF must include continuous monitoring to timely detect and address any material risks.	ATLAS can be deployed continuously to execute adversary simulations on demand, enabling organizations to maintain an up-to-date view of the effectiveness of their security controls as the threat landscape evolves.	ATLAS continuous simulation results and control performance metrics provide ongoing evidence of whether security controls remain effective against the latest adversary techniques.
RMiT 9.2(j)	The TRMF must include undertaking scenario analysis to strengthen capacity and readiness to resume critical systems under severe conditions.	ATLAS contains a library of 2,400+ realistic threat scenarios aligned to the latest threat intelligence, including ransomware and APT campaigns. These scenarios allow financial institutions to conduct structured analysis of their defense	ATLAS Scenario Explorer provides detailed scenario information including adversary TTPs, mapped to the latest threat intelligence on APT groups and ransomware campaigns targeting the financial sector. This enables financial institutions to

		readiness under severe cyber conditions.	document and evidence scenario analysis activities, and to simulate those scenarios directly against their live environment, providing measurable assurance of their readiness to resume critical systems under severe conditions.
RMiT 9.2(k)	The TRMF must include effective incident management policies and procedures to minimise the impact of any service disruption by restoring the affected service or system to a secure and stable state as quickly as possible.	ATLAS allows financial institutions to continuously test and validate incident detection and response processes through adversarial simulation. This identifies gaps in incident management workflows that may impair timely recovery.	Simulation results provide detailed timestamps of attack execution, detection and logging, enabling accurate Mean-Time-To-Detect (MTTD) and Mean-Time-To-Response (MTTR) calculation to measure incident management effectiveness.

Table 2: Technology Operations Management (Section 10)

BNM RMiT Clause	RMiT Requirement	digiDations Solution Capabilities	Supporting Evidence
RMiT 10.17	A financial institution must ensure that all systems including digital services are not running with known security vulnerabilities, on outdated platforms or end-of-life (EOL) technology systems, including continuously monitoring and implementing latest patch releases in a timely manner.	ATLAS continuously validates the effectiveness of security controls by executing simulations based on the latest known TTPs and CVEs. This allows security teams to identify whether unpatched or EOL systems remain exploitable under current threat conditions.	ATLAS simulation results indicate whether attack techniques targeting known vulnerabilities are successfully blocked or detected by the cyber defense stack, providing evidence of the effectiveness and prioritization of patch management controls across the environment.
RMiT 10.19	A financial institution must continually monitor the effectiveness and security of the technology in use, incorporating developments in technology that may disrupt existing security controls, and formulate long-term strategy to address anticipated changes including new cyber adversary tactics and techniques.	ATLAS is continuously updated with the latest threat group TTPs and adversary behaviors based on emerging threat intelligence. This allows financial institutions to proactively test their defenses against new and evolving adversary tactics as they emerge.	ATLAS continuous simulation results demonstrate whether updated adversary techniques are successfully detected and blocked, providing measurable insight into whether existing controls remain effective against emerging threats.
RMiT 10.42	A financial institution must ensure sufficient and relevant network	ATLAS includes a log gateway component that collects and stores	ATLAS Web UI provides visibility of the logs collected by the log

	device logs are retained for investigations and forensic purposes for at least three years.	relevant logs from security products (NGFW, NIDS/NIPS, EDR, SIEM, etc.) related to simulations executed. This allows security teams to review and validate the logs generated by network devices during simulated attack activities.	gateway, enabling security teams to verify that network device logging is functioning correctly and that relevant logs are generated during simulated adversary activities.
RMiT 10.49	A financial institution must formulate a roadmap to achieve continuous monitoring of a third party service provider's cybersecurity posture to obtain real-time insights for effective incident management, including adopting security policies and controls to mitigate product-specific third party risks and ensuring incident response plans incorporate protocols with third party service providers to detect and contain security vulnerabilities.	ATLAS can be used to validate the effectiveness of security controls and detection mechanisms that monitor third party connectivity and data flows. This helps financial institutions identify gaps in their ability to detect and respond to adversary activity propagating through third party systems.	ATLAS simulation results indicate whether anomalous activity across third party interfaces is detected and logged by monitoring systems, supporting continuous assurance of third party cybersecurity posture.
RMiT 10.57	A financial institution must ensure that anomalies are flagged for prompt investigations to contain any cyber incidents, and that user	ATLAS simulations generate timestamped adversary activity across critical systems, allowing security teams to validate that	ATLAS simulation results display the relevant security product logs and OS audit logs generated during each simulation, enabling teams to

	activities in critical systems are logged for audit and investigations, maintained for at least three years and regularly reviewed.	monitoring systems correctly detect and log anomalous activities. The log gateway component of ATLAS enables correlation of simulation activity against logs from security products.	validate that user activities are being captured and that logging is functioning correctly across the environment.

Table 3: Cybersecurity Management (Section 11)

BNM RMiT Clause	RMiT Requirement	ATLAS Validation Capability	Validation Evidence
RMiT 11.2	A financial institution must develop a Cyber Resilience Framework (CRF) which clearly articulates its governance for managing cyber risks, its cyber resilience objectives and its risk tolerance, with objectives including ensuring operational resilience against extreme but plausible cyber-attacks. The CRF must support effective identification, protection, detection, response, and recovery (IPDRR) of systems and data from internal and external cyber-attacks.	ATLAS supports the operationalization of the CRF by providing continuous adversarial simulation capabilities to validate identification, protection, detection, response and recovery controls. ATLAS simulates extreme but plausible cyber-attack scenarios based on current threat intelligence to test the effectiveness of the institution's cyber defenses.	Simulation results provide measurable evidence of control effectiveness across the IPDRR lifecycle, supporting ongoing validation that the CRF objectives are being achieved in practice.
RMiT 11.3(c)	The CRF must include identification of cybersecurity threats, vulnerabilities and countermeasures to secure digital services delivery against cyber-attacks.	ATLAS contains 26,000+ TTPs mapped to threat intelligence on 440+ APT groups and 220+ ransomware gangs. This enables financial institutions to identify relevant threats and evaluate the effectiveness of countermeasures	ATLAS contains: 26,000+ TTPs; 6,000+ Detection Rules; 2,400+ Scenarios; 440+ APT Groups tracked; 220+ Ransomware Gangs tracked.

		against specific adversary behaviors targeting the financial sector.	
RMiT 11.3(e)	The CRF must include timely detection of cybersecurity incidents through continuous surveillance and monitoring.	ATLAS supports continuous validation of detection capabilities by executing adversarial simulations and measuring whether monitoring systems generate the expected alerts within an acceptable timeframe. Beyond confirming that incidents are detected, ATLAS specifically measures whether they are detected in a timely manner, a critical distinction under this clause. The log gateway component correlates simulation activity against logs from security products, allowing security teams to identify not only gaps in detection coverage but also delays in detection that may indicate monitoring systems are not operating with sufficient speed to meet the institution's cyber resilience objectives.	ATLAS simulation results provide detailed timestamps for each payload executed, including execution start time, end time, and detection time. This enables precise calculation of Mean Time to Detect (MTTD) for each simulated incident, giving security teams measurable evidence of whether cybersecurity incidents are being detected in a timely manner across all monitored systems.

RMiT 11.3(f)	The CRF must include detailed incident handling policies and procedures and a crisis response management playbook to support the swift recovery from cyber incidents and contain any damage resulting from a cybersecurity breach.	ATLAS can execute scenario-based simulations aligned to crisis response playbook scenarios, enabling financial institutions to test and validate the effectiveness of their incident handling procedures and response playbooks under realistic conditions.	ATLAS simulation results provide timestamped evidence of attack execution, detection and response, enabling teams to measure response effectiveness and identify gaps in incident handling procedures.
RMiT 11.3(i)	The CRF must establish a cyber risk management function to analyse actual and potential cyber threats, providing risk assessments and timely escalation of high-risk cyber threats to senior management and the board.	When a financial institution's cyber risk management function identifies a potential high-risk threat through their threat intelligence processes, ATLAS allows the security team to validate whether that threat is of actual value in their specific environment, by running the corresponding adversary simulation and observing whether it succeeds, is detected, or is blocked. This moves the team from theoretical threat analysis to evidence-based risk assessment. Where a threat is confirmed as high-risk and exploitable, the security team can	ATLAS generates detailed simulation reports (high-level PDF summary and detailed CSV export) containing payload information, TTP mappings, execution timestamps, and blocked and detected status. These reports provide the tangible evidence base required to support a credible risk escalation to senior management.

		use ATLAS to execute targeted simulations and generate a structured simulation report — including payload details, attack techniques, blocked and detected status — that provides concrete, demonstrable evidence to support timely escalation and informed decision-making by senior management and the board.	
RMiT 11.5 / Appendix 5	A financial institution must adopt robust control measures as outlined in Appendix 5 to enhance its resilience to cyber-attacks, including network security (network segmentation, firewall, IPS), data security (DLP, customer information breach safeguards), and SOC capabilities.	ATLAS validates the operational effectiveness of the control measures required under Appendix 5 Parts A, B and C, including: network security controls (simulating malicious network traffic to validate firewall, IPS and network segmentation effectiveness); data security controls (simulating data exfiltration and unauthorized access techniques to validate DLP and customer information breach safeguards); and SOC capabilities (generating realistic adversary	Simulation results display whether simulated network traffic, malware techniques, data exfiltration attempts, and adversary behaviors are blocked and logged by the relevant security controls, providing direct and continuous evidence of Appendix 5 Parts A, B and C control effectiveness.

		activity to validate log collection, SIEM correlation, behavioral detection, and threat detection coverage across critical systems).	
RMiT 11.6	A financial institution must conduct a realistic 'Red Team' simulation attack on its infrastructure at least once every three years to proactively identify and manage potential vulnerabilities.	ATLAS supports the planning and execution of red team simulation exercises by providing a comprehensive library of threat intelligence-based scenarios and realistic adversary TTPs. ATLAS can be used to continuously validate controls between formal red team engagements, ensuring the organization's cyber defenses remain effective on an ongoing basis.	ATLAS Scenario Explorer provides detailed red team scenarios and TTPs. Simulation results provide evidence of control effectiveness, blocked and detected status, and detailed payload logs to support red team exercise reporting.
RMiT 11.8	A financial institution must establish clear responsibilities for cybersecurity operations which shall include implementing appropriate mitigating measures corresponding to all phases of the cyber-attack lifecycle: reconnaissance, weaponisation, delivery, exploitation,	ATLAS simulates adversary techniques across all phases of the attack lifecycle, enabling security teams to validate that detection and response controls are in place for each stage. Simulations cover techniques including data exfiltration, C2 communications,	Simulation results indicate whether techniques at each phase of the attack lifecycle are blocked and detected, identifying gaps in defensive coverage across the kill chain.

	installation, command and control, and exfiltration.	lateral movement, persistence, and malware execution, allowing financial institutions to evaluate their defensive coverage across the full kill chain.	
RMiT 11.9	A financial institution must ensure continuous and proactive monitoring and timely detection of anomalous activities in its technology infrastructure, including establishing a Security Operations Center (SOC) equipped with necessary tools for proactive monitoring, ensuring monitoring covers all critical systems, and conducting regular VAPT in line with Appendix 5.	ATLAS supports continuous SOC validation by generating realistic, adversary-based activities that test whether monitoring systems detect anomalous behavior. The log gateway component of ATLAS collects and correlates logs from security products, enabling security teams to validate SOC detection capabilities and identify gaps in monitoring coverage across critical systems.	Simulation results display relevant security product logs and OS-based audit logs generated during each simulation, enabling SOC teams to validate detection rules and SIEM correlation use cases, and identify gaps in monitoring coverage. Detailed timestamps for each simulation payload enable precise Mean Time to Detect (MTTD) measurement.
RMiT 11.10	A financial institution must establish a process to collect, analyse and evaluate cyber threat intelligence in relation to its environment to promptly detect cyber threats, including data breach incidents and	ORION provides comprehensive Threat Intelligence feed & report. It allow security operation team to collect, analyze, and contextualize threats identified. ORION transforms raw threat data into actionable	ORION provides comprehensive threat intelligence capabilities covering Indicators of Compromise (IOC), Indicators of Attack (IOA), and Indicators of Behavior (IOB), including emerging threat vectors such as supply chain threats and AI-

	spread of misleading information over the Internet.	intelligence that the security team can prioritize and act on ATLAS is continuously updated with the latest threat intelligence on APT groups and ransomware gangs targeting the financial sector. This allows security teams to leverage ATLAS to validate whether their current defenses are effective against the specific threats identified through their cyber threat intelligence programme. HELIOS provides External Attack Surface Management (EASM) capabilities, continuously monitoring the open internet for known data breaches, information and public facing asset regarding the financial institution.	powered attack techniques. This enables security operations teams to continuously collect, analyze, and detect threats within their existing internal environment. ATLAS Scenario Explorer maps threat intelligence to specific adversary TTPs and scenarios, enabling security teams to validate their defenses against identified threat actors. TARA AI provides detailed threat intelligence analysis within ATLAS. HELIOS provides continuous monitoring across public-facing assets and the dark web, giving security teams comprehensive visibility into the organization's external exposure, data exfiltration disclosures, and threat actor communications targeting the organization. This enables early detection of data breach incidents

			and identification of vulnerabilities in public-facing assets before they can be exploited.
RMiT 11.12	A financial institution must establish comprehensive cyber crisis management policies and procedures that incorporate cyber-attack scenarios and responses in the organization's overall crisis management plan, escalation processes, business continuity and disaster recovery planning. This includes developing a clear communication plan for engaging shareholders, regulatory authorities, customers and employees in the event of a cyber incident.	ATLAS supports the validation of cyber crisis management procedures by executing realistic adversary simulations based on extreme but plausible cyber-attack scenarios — including ransomware campaigns, APT intrusions, and data exfiltration attacks. By running these simulations against live environments, financial institutions can verify that their crisis management processes, escalation workflows, and incident response procedures are triggered correctly and operate as expected under real attack conditions. ATLAS simulation results provide measurable evidence of whether detection, escalation and containment processes function during actual adversary activity, identifying gaps in crisis response before a real incident occurs.	Simulation results provide timestamped evidence of attack execution, detection and escalation trigger points, enabling teams to verify that crisis management procedures are activated at the correct thresholds. Scenario-based simulation reports can be used to evidence that cyber-attack scenarios have been incorporated and tested within the institution's crisis management plan.

RMiT 11.13	A financial institution must establish and implement a comprehensive Cyber Incident Response Plan (CIRP) covering: Preparedness; Detection and Analysis; Containment and Eradication; Recovery; and Post-incident Activity.	ATLAS enables financial institutions to test all phases of the CIRP through realistic adversarial simulation. Simulations validate detection and analysis capabilities (MTTD), containment and eradication effectiveness, and recovery readiness. Post-incident analysis is supported by detailed simulation logs and TARA AI remediation recommendations.	Simulation results provide timestamped evidence across each phase of incident response, enabling teams to measure MTTD and MTTR and validate the effectiveness of CIRP procedures. TARA AI provides detailed remediation guidance to support post-incident improvement.
RMiT 11.16	A financial institution must conduct an annual cyber drill exercise to test the effectiveness of its CIRP including out-of-band communication methods, based on various current and emerging threat scenarios, with involvement of key stakeholders. The test scenarios must include scenarios designed to test escalation, internal and external communication, and decision-making processes, as well as the readiness	ATLAS contains realistic simulation scenarios based on current and emerging threat intelligence related to APT groups and ransomware campaigns. These scenarios can be used to design and execute annual cyber drill exercises, enabling financial institutions to test CIRP effectiveness under realistic conditions with involvement of key stakeholders.	ATLAS supports both built-in and custom scenarios and playbooks. It can generate simulation reports (high-level PDF summary and detailed CSV) to support documentation and reporting of cyber drill outcomes to the board and senior management.

	of CERT and relevant third party service providers.		

Table 4: Cybersecurity Control Measures – Network, Data & SOC (Appendix 5, Parts A, B & C)

BNM RMiT Clause	RMiT Requirement	ATLAS Validation Capability	Validation Evidence
RMiT App.5 Part A, Section 1	A financial institution must ensure technology networks are segregated into multiple zones according to threat profile. Each zone shall be adequately protected by various security devices including but not limited to firewall and Intrusion Prevention System (IPS). This must include network for delivery of digital services and wireless networks.	ATLAS simulates realistic malicious network traffic across network zones based on the latest threat intelligence, enabling security teams to validate whether firewall and IPS controls correctly detect and block adversary traffic at each network boundary, including digital services and wireless network segments.	Simulation results display whether simulated malicious network traffic traversing each network boundary is blocked and logged by the respective firewall and IPS controls, providing direct evidence of network segmentation effectiveness.
RMiT App.5 Part B, Section 5(a)	A financial institution must ensure adequate security controls are in place to safeguard against customer information breach (CIB), including conducting continuous review to ensure that CIB does not occur in the IT environments of the financial institution, its intermediaries, or third	ATLAS executes adversary simulations that include data exfiltration techniques, enabling security teams to validate whether controls protecting customer information effectively. ATLAS simulations can be scoped to perform data exfiltration of customer	Simulation results indicate whether simulated data exfiltration techniques targeting customer information repositories are blocked and detected. These results directly support the security validation exercises required to detect potential accidental exposure of

	party service providers. The financial institution shall incorporate scanning or screening of customer information into the scope of periodic security assessments (e.g. penetration testing, red teaming, or other security validation exercises) to detect accidental exposure of customer information on financial institution's systems.	information via different tunnels or protocol, validating that data loss prevention and access controls correctly detect and prevent customer information breach scenarios.	customer information across the institution's IT environment.
RMiT App.5 Part B, Section 2	A financial institution must design internal control procedures and implement appropriate technology to enforce Data Loss Prevention (DLP) policies covering: data in-use (data being processed by IT resources); data in-motion (data being transmitted on the network); and data at-rest (data stored in storage mediums).	ATLAS simulates data exfiltration techniques across all three DLP domains, including techniques that attempt to extract data in transit over the network (data in-motion), access and copy data from storage systems (data at-rest), and abuse running processes to access sensitive information (data in-use). This allows security teams to validate whether DLP controls effectively detect and block adversary-driven data exfiltration attempts across all layers.	Simulation results display whether simulated exfiltration techniques targeting data in-motion, data at-rest, and data in-use are detected and blocked by the DLP controls in place, providing evidence of DLP policy effectiveness across all required categories.

		The simulation can simulate data exfiltration via covered tunnel, such as DNS, ICMP, financial institution could monitor the abnormal traffic by IPS or NDR, the simulation can validate the measures' effectiveness.	
RMiT App.5 Part C, Section 1	A financial institution must ensure its SOC has adequate capabilities for proactive monitoring of its technology security posture. This shall enable the financial institution to detect anomalous user or network activities, flag potential breaches and establish the appropriate response supported by skilled resources based on the level of complexity of the alerts.	ATLAS generates continuous, realistic adversary activity across the institution's environment, providing the SOC with a controlled stream of known attack techniques to validate whether monitoring systems detect anomalous behavior, flag potential breaches, and trigger the appropriate response. This enables security teams to continuously measure and improve the SOC's detection, correlation and response capabilities against realistic threat scenarios.	Simulation results display whether anomalous and context-based activities generated by ATLAS are detected by SOC monitoring systems and trigger the appropriate alerts. Detailed timestamps for each simulation payload enable MTTD measurement to assess the timeliness of SOC detection.
RMiT App.5 Part C, Section 2(a)	The SOC must be able to perform adequate log collection and the implementation of an event correlation engine with parameter-	ATLAS includes a log gateway component that collects and stores relevant logs from security products (NGFW, NIDS/NIPS, EDR, SIEM, etc.)	ATLAS Web UI provides visibility of the logs collected by the log gateway, enabling SOC teams to verify that relevant security product

	driven use cases such as Security Information and Event Management (SIEM).	related to attack simulations executed. This enables security teams to validate whether the SIEM and log correlation engine correctly ingest, correlate, and generate alerts for adversary activity detected during simulations.	logs are generated during simulated adversary activities and that SIEM correlation rules are functioning as intended.
RMiT App.5 Part C, Section 2(f)	The SOC must be able to provide situational awareness to detect adversaries and threats including threat intelligence analysis and operations and monitoring Indicators of Compromise (IoCs). This includes advanced behavioral analysis to detect signature-less and file-less malware and to identify anomalies that may pose security threats including at endpoints and network layers.	ORION provides comprehensive Threat Intelligence feed & report. It allow security operation team to collect, analyze, and contextualize threats identified. ORION transforms raw threat data into actionable intelligence that the security team can prioritize and act on. ATLAS simulates signature-less and file-less malware techniques, advanced persistent threat behaviors, and IoC-generating attack patterns based on the latest threat intelligence. This enables the SOC to validate whether behavioral analysis capabilities, endpoint detection	ORION provides comprehensive threat intelligence capabilities covering Indicators of Compromise (IOC), Indicators of Attack (IOA), and Indicators of Behavior (IOB), including emerging threat vectors such as supply chain threats and AI-powered attack techniques. This enables security operations teams to continuously collect, analyze, and detect threats within their existing internal environment. ATLAS simulation results indicate whether advanced behavioral techniques, including file-less malware, living-off-the-land

		tools, and IoC monitoring mechanisms correctly identify these advanced adversary techniques without relying solely on signature-based detection.	techniques, and IoC-generating attacks are detected by the SOC's monitoring systems, validating the effectiveness of behavioral analysis capabilities at both endpoint and network layers.
RMiT App.5 Part C, Section 2(g)	The SOC must have a well-documented and standardized playbook that covers common and plausible cyber threat scenarios, such as ransomware attacks.	ATLAS contains a library of 2,400+ realistic threat scenarios based on the latest threat intelligence related to ransomware gangs and APT groups. These scenarios can be used to design and validate SOC playbook coverage, ensuring that documented response procedures are tested against realistic attack patterns. TARA AI, built into ATLAS, provides detailed payload explanations and recommended detection rules to support playbook development and refinement.	ATLAS Scenario Explorer provides detailed scenario and TTP information for ransomware and APT campaigns. TARA AI generates detection rules and mitigation recommendations that can be incorporated directly into SOC playbooks, supporting continuous playbook improvement based on current threat intelligence.
RMiT App.5 Part C, Section 3	A financial institution must ensure that the SOC provides monthly threat assessment report, which shall include at a minimum: trends and	ATLAS generates detailed simulation results that include categorised attack types, targeted systems, payload details, and TTP information	ATLAS can generate a high-level summary report and a detailed CSV export containing payload information, attack categories,

	statistics of cyber events and incidents categorised by type of attacks, target and source IP addresses, location of data centers and criticality of applications; and intelligence on emerging and potential threats including Tactics, Techniques and Procedures (TTP).	mapped to the MITRE ATT&CK framework. This data support and ensure that the SOC capabilities are continuously validated.	timestamps, blocked and detected status, and TTP mappings. This structured data directly supports the monthly threat assessment report requirement set forth by RMiT

Bank Negara Malaysia Risk Management in Technology (RMiT)

The Bank Negara Malaysia (BNM) Risk Management in Technology (RMiT) Policy Document (BNM/RH/PD 028-98), issued on 28 November 2025, provides a comprehensive framework for financial institutions to manage technology risk and strengthen cyber resilience. The policy document supersedes the previous RMiT issued on 1 June 2023 and comes into effect immediately upon issuance.

The RMiT applies to a broad range of financial institutions operating in Malaysia, including licensed banks, investment banks, Islamic banks, insurers, takaful operators, prescribed development financial institutions, approved issuers of electronic money, operators of designated payment systems, registered merchant acquirers, and intermediary remittance institutions.

Overview of BNM RMiT

The RMiT sets out minimum requirements for financial institutions to manage technology risk, including cyber risk. The policy document is structured around the following key areas: Governance (Section 8), Technology Risk Management (Section 9), Technology Operations Management (Section 10), Cybersecurity Management (Section 11), Digital Services (Section 12), Technology Audits (Section 13), External Party Assurance (Section 14), Security Awareness and Education (Section 15), and Regulatory Notification and Assessment requirements (Sections 16-18).

The RMiT distinguishes between mandatory standards (marked 'S') and guidance (marked 'G'). Non-compliance with mandatory standards may result in enforcement action. Financial institutions are expected to apply the requirements having regard to the size and complexity of their operations, the level of technology use, and their external stress exposure.

A key requirement of the RMiT is for financial institutions to conduct a realistic Red Team simulation attack on their infrastructure at least once every three years (RMiT 11.6) and to establish a Cyber Resilience Framework (CRF) that supports continuous validation of security controls across the IPDRR (Identify, Protect, Detect, Respond, Recover) lifecycle.

Key Cybersecurity Expectations for Financial Institutions

The RMiT outlines specific cybersecurity expectations that financial institutions are required to implement. Financial institutions must develop a Cyber Resilience Framework (CRF) that governs the management of cyber risks, articulates cyber resilience objectives, and supports operational resilience against extreme but plausible cyber-attacks. Financial institutions are also required to establish a Security Operations Center (SOC), conduct continuous monitoring of their technology security posture, perform regular vulnerability assessments and penetration testing, and maintain a comprehensive Cyber Incident Response Plan (CIRP).

The RMiT further requires financial institutions to conduct annual cyber drill exercises to test the effectiveness of their CIRP, and to establish processes for collecting and evaluating cyber threat intelligence. These requirements underscore the need for financial institutions to continuously validate the effectiveness of their cybersecurity controls against realistic adversary techniques.

The Challenge of Demonstrating Security Control Effectiveness

Financial institutions operating under Bank Negara Malaysia's Risk Management in Technology (RMiT) framework face an expectation that goes well beyond implementing security controls. They are expected to prove those controls actually work.

RMiT sets out mandatory standards covering governance, cybersecurity operations, technology risk management, and incident response. For boards and senior management, the policy elevates cybersecurity from an IT function to a core strategic accountability. Controls must not only be deployed and documented but demonstrated to be operating effectively under real conditions.

This is where many institutions face their greatest challenge. Vulnerability assessments, penetration tests, and periodic audits each serve an important purpose, but they share a common limitation. They offer assurance at a point in time, while the threat environment shifts continuously. RMiT requires quarterly vulnerability assessments, annual intelligence-led penetration testing, and red team simulation exercises on a triennial basis. Yet even this cadence leaves meaningful windows between assessments during which organisations cannot be certain their defences remain effective against current adversary techniques.

For leadership teams, that uncertainty carries real consequence. A control that was effective at the last audit may have drifted, been misconfigured, or been rendered obsolete by an evolving threat before the next assessment cycle begins.

HELIOS External Attack Surface Management Platform

Organizations today face cyber threats that extend well beyond their internal technology perimeter. Adversaries routinely conduct reconnaissance against public-facing assets, exploit exposed vulnerabilities before security teams are aware of them, and trade stolen credentials and sensitive data across dark web forums and marketplaces. To defend effectively, financial institutions require continuous visibility into their external exposure across all of these dimensions.

The HELIOS External Attack Surface Management (EASM) Platform from digiDations provides financial institutions with a fully external, passive monitoring capability that continuously observes the organization's attack surface from the outside in, the same perspective an adversary would take.

HELIOS monitors across three key domains. First, public-facing asset monitoring gives security teams continuous visibility into the organization's externally exposed assets, including web applications, domains, subdomains, IP addresses, open ports, and services. This enables security teams to identify misconfigurations, unpatched vulnerabilities, and shadow IT assets that may be exposed to the internet without the organization's knowledge.

Second, dark web monitoring provides security teams with an additional layer of intelligence by continuously observing dark web forums, marketplaces, and threat actor communications for any references to the organization. This enables early detection of data exfiltration disclosures and threat actor activity targeting the institution, often before the impact is felt internally.

Third, leaked credential monitoring tracks whether employee or customer credentials associated with the organization have been exposed through third party data breaches or threat actor disclosures. Early identification of leaked credentials enables security teams to take prompt remedial action before compromised credentials are leveraged for unauthorized access.

By providing continuous, external visibility across public-facing assets, the dark web, and leaked credentials, HELIOS ensures that financial institutions maintain an accurate and up-to-date understanding of their external exposure, enabling proactive risk reduction before adversaries can act.

ORION Threat Intelligence Platform

Effective cybersecurity depends on understanding the threats that are most relevant to the organization. Without timely and accurate threat intelligence, security teams risk focusing their efforts on the wrong areas, leaving the organization exposed to the specific adversary techniques and attack patterns that are most likely to be used against them.

The ORION Threat Intelligence Platform from digiDations provides financial institutions with a continuous, structured feed of actionable threat intelligence, enabling security operations teams to maintain an accurate and current picture of the threat landscape relevant to their environment.

ORION delivers threat intelligence across three core indicator types. Indicators of Compromise (IOC) provide security teams with evidence of known malicious activity, including file hashes, IP addresses, domains, and URLs associated with threat actors and malware campaigns. Indicators of Attack (IOA) focus on the behavioral patterns and techniques adversaries use during an active attack, enabling security teams to detect threats based on what attackers are doing rather than solely on known signatures. Indicators of Behavior (IOB) provide broader behavioral context, capturing patterns of activity that may signal adversary presence or intent even before a specific attack technique is identified.

Beyond these core indicator types, ORION covers emerging and specialized threat vectors including supply chain threats, which track risks arising from third party software, vendors, and technology dependencies, and AI-powered attack techniques, which monitor the growing use of artificial intelligence by adversaries to conduct more sophisticated and automated attacks.

ORION delivers this intelligence as a continuous feed, enabling financial institutions to integrate threat intelligence directly into their existing security operations workflows and tools. This ensures that security operations teams are always working from the most current and relevant threat picture, enabling faster detection, more accurate prioritization, and better-informed response decisions.

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

Satisfying BNM RMiT's mandatory standards is the baseline. It is not the destination.

RMiT was developed in response to a financial sector threat landscape that had grown significantly in scope, sophistication, and consequence. The policy reflects BNM's expectation that financial institutions do not simply document their security posture, but demonstrate it. Compliance confirms that the right frameworks, processes, and controls are in place. It does not confirm that those measures will hold when a determined adversary puts them to the test.

The gap between compliance and genuine resilience is where risk lives. Threat actors targeting Malaysia's financial institutions invest in understanding how organisations are defended. They probe for weaknesses between audit cycles, exploit misconfigurations that scheduled assessments did not surface, and adapt their techniques to bypass controls that were validated months ago.

For boards and executive leadership, the implication is clear. Security investment must translate into continuous, demonstrable protection, not periodic assurance. Organisations that go beyond scheduled compliance activities to maintain ongoing visibility into the effectiveness of their controls, detection capabilities, and incident response readiness are better positioned to protect their customers, meet regulatory expectations with confidence, and respond decisively when threats materialise.

BNM RMiT defines the obligation. digiDations ATLAS provides the capability to fulfil it continuously.

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 once every few years. 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 digiDations platform supports this approach through three integrated capabilities. ATLAS enables organizations to safely simulate real-world adversary techniques and evaluate how security controls perform during these simulations, providing continuous, measurable evidence of defensive effectiveness. ORION ensures that the security operations team is always working from the most current and relevant threat intelligence, enabling faster detection, more accurate prioritization, and better-informed response decisions. HELIOS provides continuous visibility into the organization's external exposure across public-facing assets, the dark web, and leaked credentials, enabling proactive risk reduction before adversaries can act.

By incorporating all three capabilities 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 against evolving threat actors targeting the Malaysian financial sector.

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.