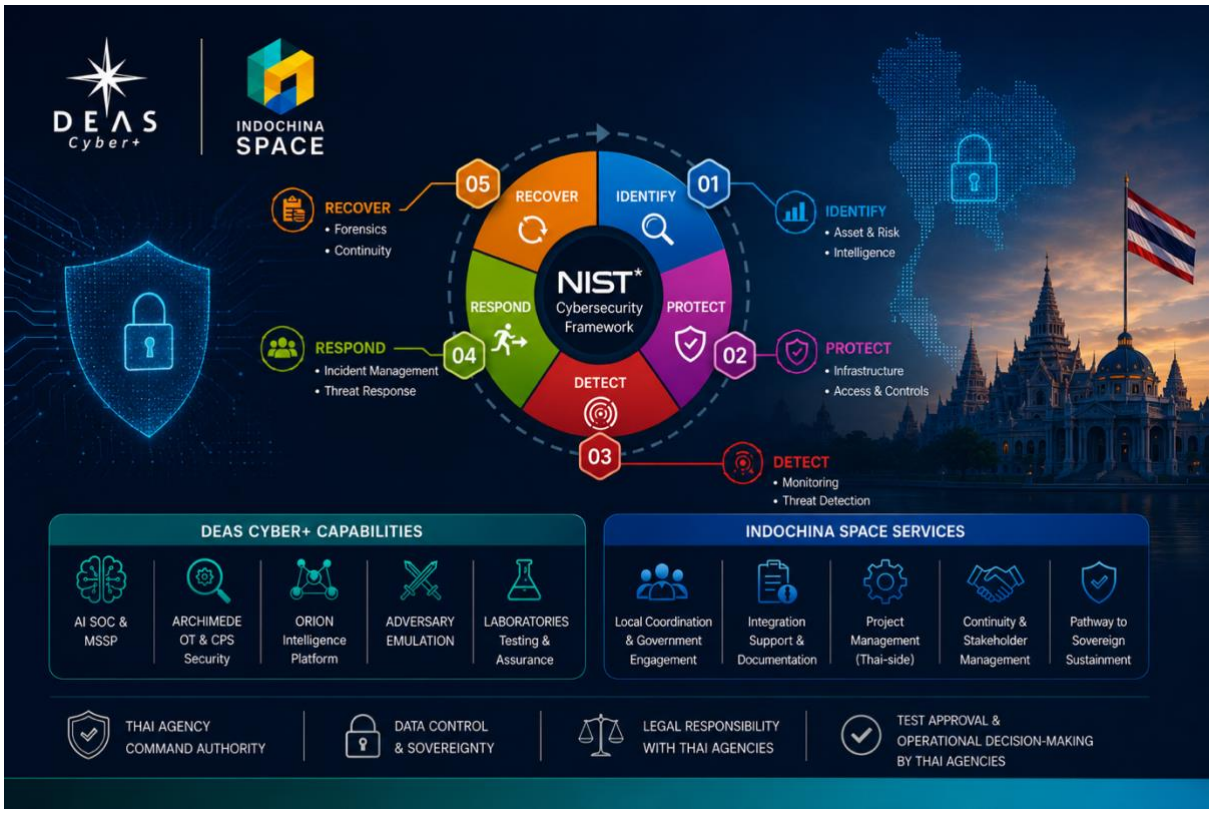
# From Audit to Resilience: A Practical Process to Strengthen Cybersecurity in Thai Government Environments

A white paper on Cybersecurity by Indochina Space for Thai Government agencies.



# Table of contents.


Abstract ..... 3

Strategic Context: Thailand's Cybersecurity Requirement ..... 3

The Core Problem: Fragmented Defence, Expanding Attack Surface ..... 5

A Process for Enhancing Cybersecurity in Thai Government Environments ..... 8

DEAS and Indochina Space Operating Model ..... 9

Capability Modules ..... 11

Archimede: OT and Cyber-Physical Security ..... 11

Orion: Intelligence and Investigative Fusion ..... 12

AI SOC and MSSP: Continuous Monitoring and Managed Response ..... 12

Adversary Emulation: Realistic Resilience Testing ..... 13

Zero Trust and Compliance: Controlled Access and Governance ..... 14

Capacity Building: Training, Transfer, and Sustainment ..... 15

Combined Value of the Modules ..... 16

Application to Thai Government Sectors ..... 16

NCSA and ThaiCERT ..... 16

Defence and Armed Forces ..... 17

CCIB and Anti-Scam Operations ..... 17

MOPH and Health CIRT ..... 18

Power, Utility, and Other CII Environments ..... 18

Cross-Sector Integration ..... 19

Governance, Data Control and Sovereignty ..... 19

Concluding Remarks ..... 21

## Abstract

Thailand's cybersecurity challenge is shifting **from compliance and isolated defensive tools towards operational resilience**. Government agencies now rely on interconnected digital services, shared data platforms, operational technology, telecoms infrastructure, cloud systems, and external providers. These dependencies improve public service delivery, but they also create new pathways for cybercrime, espionage, service disruption, and compromise of critical national functions.

This white paper proposes a structured process for strengthening cybersecurity in Thai Government environments. The process moves from discovery and technical assessment through adversary emulation, remediation, validation, continuous monitoring, intelligence fusion, and capability transfer. Its purpose is to identify real exposure, test realistic attack paths, prioritise operational risk, and verify that corrective action has improved protection.

Indochina Space and DEAS Cyber+ can support this process through a combined operating model. DEAS provides specialist cyber methodology, platforms, and expertise in defence-grade resilience, AI-enabled SOC operations, adversary emulation, operational-technology assessment, and investigative data fusion. Indochina Space provides Thai-side coordination, localisation, implementation support, and continuity. The model preserves Thai command authority, data control, mission ownership, and final decision-making.

The paper applies this approach to national cyber coordination, defence environments, law-enforcement and anti-scam operations, public health systems, utilities, and other Critical Information Infrastructure. Its central conclusion is that Thailand requires a disciplined, Thai-controlled resilience process that protects the systems that matter most and converts cybersecurity investment into verified protection, operational confidence, and sustainable national capability.

## Strategic Context: Thailand's Cybersecurity Requirement

Thailand's cybersecurity requirement has expanded to operate a much broader digital environment in which public administration, defence operations, police investigations, healthcare delivery, financial crime response, utility management, transport, telecommunications, and Critical Information Infrastructure are increasingly connected. The resulting cyber risk now has the potential to affect operational continuity, public trust, national security, financial stability, and the delivery of essential services.

This shift reflects the wider digital transformation of Thai Government operations. Agencies are adopting online services, shared databases, cloud-enabled systems, mobile applications, digital identity mechanisms, remote access, sensor networks, and data-exchange platforms. **These systems improve efficiency and enable faster public service delivery, but they also create more routes through which hostile actors, criminal groups, insider threats, compromised suppliers, or poorly governed external connections can reach sensitive environments**. The more integrated the public sector becomes, the more cybersecurity depends on the security of interfaces between organisations, sectors, platforms, and service providers.

Thailand already recognises cybersecurity as a national priority. The National Cyber Security Agency and ThaiCERT provide national coordination, incident reporting, Critical Information Infrastructure engagement, and technical capacity-building. The Royal Thai Armed Forces and individual service cyber centres are developing cyber capabilities as part of modern multi-domain operations. The Cyber Crime Investigation Bureau and anti-scam centres are responding to high-volume online fraud, cybercrime, digital evidence handling, financial tracing, and transnational criminal networks. The Ministry of Public Health has established a Health CIRT role to coordinate cyber incident handling across the public health sector. These developments show that Thailand's cyber challenge is not caused by institutional neglect. The issue is that **the threat environment is evolving faster than traditional, fragmented, and audit-led cyber approaches can comfortably manage**.

**The requirement is therefore shifting from basic cybersecurity compliance towards operational cyber resilience**. Compliance remains necessary, particularly under Thailand's Cybersecurity Act, the Personal Data Protection Act, and sector-specific requirements. However, compliance alone does not prove that an agency can

withstand a realistic attack, detect compromise early, coordinate a response, protect essential operations, or restore trust after an incident. **A system may pass a formal audit and still contain exploitable pathways, weak segmentation, excessive privileges, insecure remote access, outdated operational technology, vulnerable third-party connections, or insufficient monitoring.**

A more mature cybersecurity requirement must ask which systems matter most to the mission; which interfaces allow outsiders, suppliers, or partner agencies to influence operations; how a capable adversary would move from initial access to operational effect; whether defenders can see that movement; whether response teams can act quickly; whether remediation has been verified; and whether Thai operators can sustain the capability after external support has ended. These are operational questions, not purely technical ones.

This is particularly important in Thai Government environments where information technology and operational technology now intersect. Defence systems depend on radar, communications, logistics, command-and-control networks, satellite links, sensors, and hybrid IT/OT infrastructure. Utilities rely on SCADA, telemetry, substations, field devices, control centres, remote maintenance links, and third-party providers. Hospitals depend on patient databases, connected medical systems, support infrastructure, web portals, and national health platforms. Law-enforcement and anti-scam operations depend on high-volume data fusion across banking, telecommunications, digital platforms, blockchain traces, and international partners. In each case, cybersecurity failure can produce operational consequences beyond the compromised computer.

The strategic requirement is also shaped by scale. National agencies must deal with high volumes of alerts, reports, cases, digital evidence, suspicious accounts, malware samples, exposed services, and cross-sector dependencies. **Manual processes and isolated tools can work at small scale, but they become unreliable when threats are continuous and distributed. This is why Thailand requires stronger automation, better intelligence fusion, clearer prioritisation, and security operations models capable of filtering noise, identifying meaningful patterns, and supporting human analysts rather than overwhelming them.**

A further requirement is **sovereignty of control**. Cybersecurity support for government environments must not imply loss of command authority, data ownership, operational discretion, or national control. Thai agencies must retain approval over testing, access, data handling, reporting, remediation priorities, and operational decisions. External specialist partners can provide methods, tools, training, platforms, and technical expertise, but **the operating model must preserve Thai mission ownership**. This is particularly important in defence, public health, policing, national cyber coordination, and Critical Information Infrastructure, where data sensitivity and public accountability are high.

The practical requirement for Thailand is therefore a structured, repeatable process that can be applied selectively to high-priority government environments. Such a process should begin with discovery and exposure mapping, continue through technical assessment and adversary emulation, convert findings into operationally prioritised remediation, validate that weaknesses have been closed, and then support continuous monitoring, intelligence fusion, incident response, and local capability transfer. The aim is to create a disciplined pathway from risk identification to verified protection.

*In this context, Indochina Space and DEAS Cyber+ can support Thai agencies by combining specialist international cyber capability with Thai-side coordination, localisation, and continuity. DEAS brings expertise in defence-grade cyber resilience, adversary emulation, AI-enabled SOC operations, managed security services, cyber intelligence, operational-technology assessment, and investigative data fusion. Indochina Space can support engagement with Thai stakeholders, project coordination, local integration, documentation, continuity, and capability transfer. Together, the two organisations can help Thai Government bodies move from periodic assessment towards measurable resilience, while maintaining Thai control over systems, data, and operational decisions.*

Thailand's cybersecurity requirement is therefore best understood as a national resilience requirement. It is about protecting the public functions, critical services, military capabilities, investigative systems, and digital trust mechanisms on which modern government now depends. The appropriate response is a controlled process that

identifies real exposure, tests realistic threats, strengthens the systems that matter most, and leaves Thai agencies with greater operational confidence and a more sustainable cyber capability.

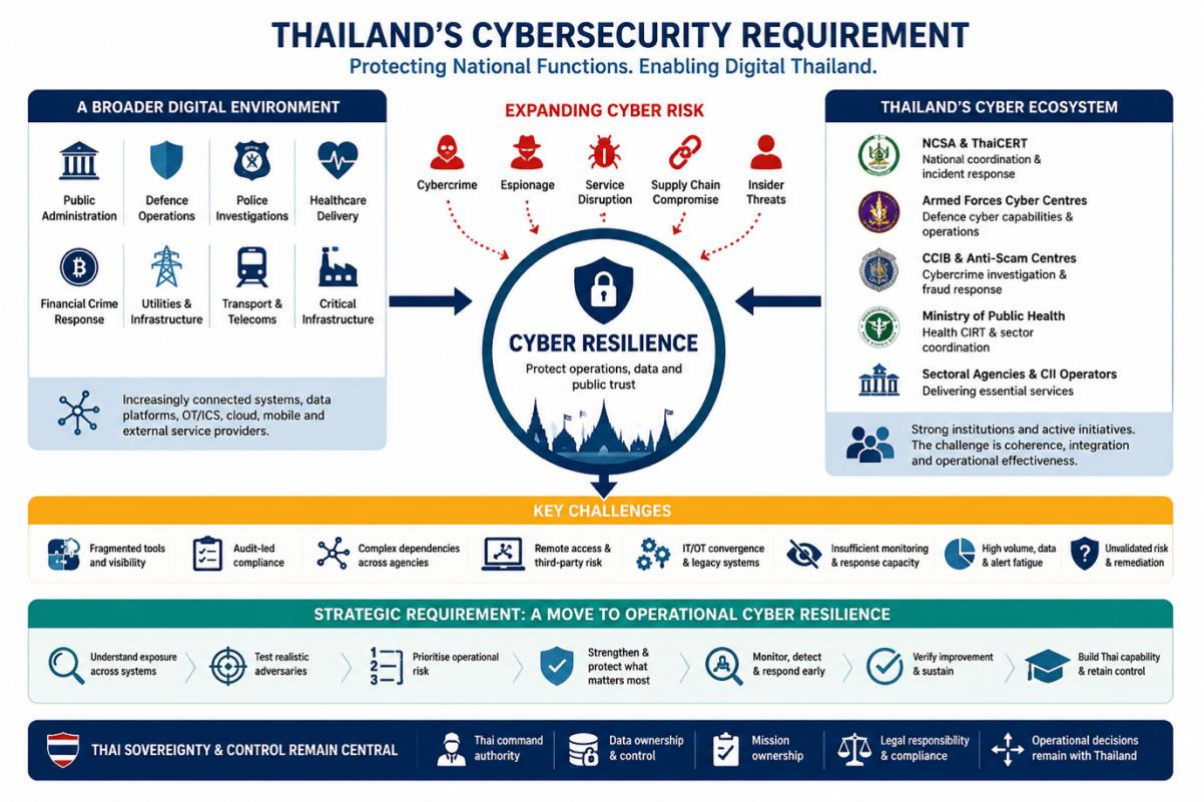



*Figure 1: The Thai cybersecurity landscape.*

## The Core Problem: Fragmented Defence, Expanding Attack Surface

**Thailand's public-sector cybersecurity challenge is that the systems being protected are becoming more connected, while the defensive structures around them often remain divided by agency, sector, platform, procurement history, and operational mandate. This produces a widening gap between the way attackers operate and the way many public organisations are organised to defend themselves.**

A cyber adversary will usually follow the easiest route into a target environment. That route may be a public website, a weak identity process, an exposed cloud service, a contractor VPN, a supplier maintenance channel, an unpatched server, an insecure application interface, a compromised user account, or an operational-technology component that was never designed for hostile digital exposure. The attacker sees pathways. The defender may see departments, systems, contracts, and reporting lines.

This creates a practical problem for government environments. One team may manage enterprise IT. Another may own operational technology. Other groups may control telecoms links, cloud services, digital identity, procurement, public-facing applications, physical infrastructure, or specialist mission systems. External contractors may operate important components under separate support arrangements. Logs may be held in different tools. Alerts may be reviewed by different teams. Incident escalation may follow different chains of command. This structure makes institutional sense, but it can obscure the full attack path.

**Fragmentation weakens defence because cyber incidents rarely remain confined to one technical domain**. A suspicious login, unusual network traffic, endpoint alert, supplier access event, and database query may each appear minor when viewed separately. Combined, they may show reconnaissance, credential misuse, lateral

movement, data staging, or preparation for disruption. Without correlation, an organisation may see disconnected events while the attacker sees a route.

**The attack surface is also expanding at the boundaries between organisations and systems.** Vendor access, inter-agency data exchange, remote support, cloud integration, outsourced operations, shared platforms, and sector-wide reporting mechanisms all create legitimate operational value. They also create dependency and trust relationships that must be controlled, monitored, and periodically tested. Weaknesses at these boundaries can become more important than weaknesses inside a single system, because they provide movement between environments.

Legacy systems add another layer of exposure. Many government and critical-service environments rely on equipment that remains operational for many years because replacement is costly, disruptive, or technically difficult. This is common in operational technology, healthcare systems, utility environments, defence infrastructure, communications systems, and specialised platforms. Such systems may be difficult to patch, sensitive to scanning, dependent on vendor support, or poorly suited to modern monitoring. They cannot be ignored, because they often support essential services.

**The convergence of information technology (IT) and operational technology (OT) makes this risk more serious.** Office systems can often tolerate standard cyber tools, routine scanning, patching cycles, and endpoint controls. Operational environments may involve radar, communications gateways, hospital support systems, industrial controllers, sensors, field devices, substations, shipboard systems, or control-room infrastructure. A cyber incident in these environments can affect service availability, operational readiness, patient safety, public confidence, or physical processes. Assessment methods must therefore be adapted to the environment, rather than copied from ordinary corporate IT.

**A further weakness is the tendency to treat audits as evidence of resilience**. Audits are necessary for governance, legal accountability, and management assurance. They help confirm that policies, controls, and procedures exist. They do not always show whether a capable adversary can chain weaknesses together, whether defenders can detect lateral movement, whether command escalation will work under pressure, or whether remediation has removed the operational risk. A system can satisfy a control checklist and still contain a realistic path to compromise.

Visibility remains one of the main constraints. Many agencies can observe parts of their environment, but lack a consolidated picture of assets, dependencies, remote access, privileged accounts, third-party connections, exposed services, and operational consequences. This limits prioritisation. Teams may spend effort on weaknesses that are visible and easy to report, while less obvious pathways into mission-critical systems remain insufficiently understood.

Scale compounds the problem. National agencies and major public-sector operators face large volumes of alerts, fraud reports, digital evidence, suspicious accounts, malware events, access anomalies, exposed services, and incident notifications. Human analysts cannot interpret this volume manually without correlation, automation, triage, and contextual intelligence. **When tools remain isolated, more data can produce less clarity.**

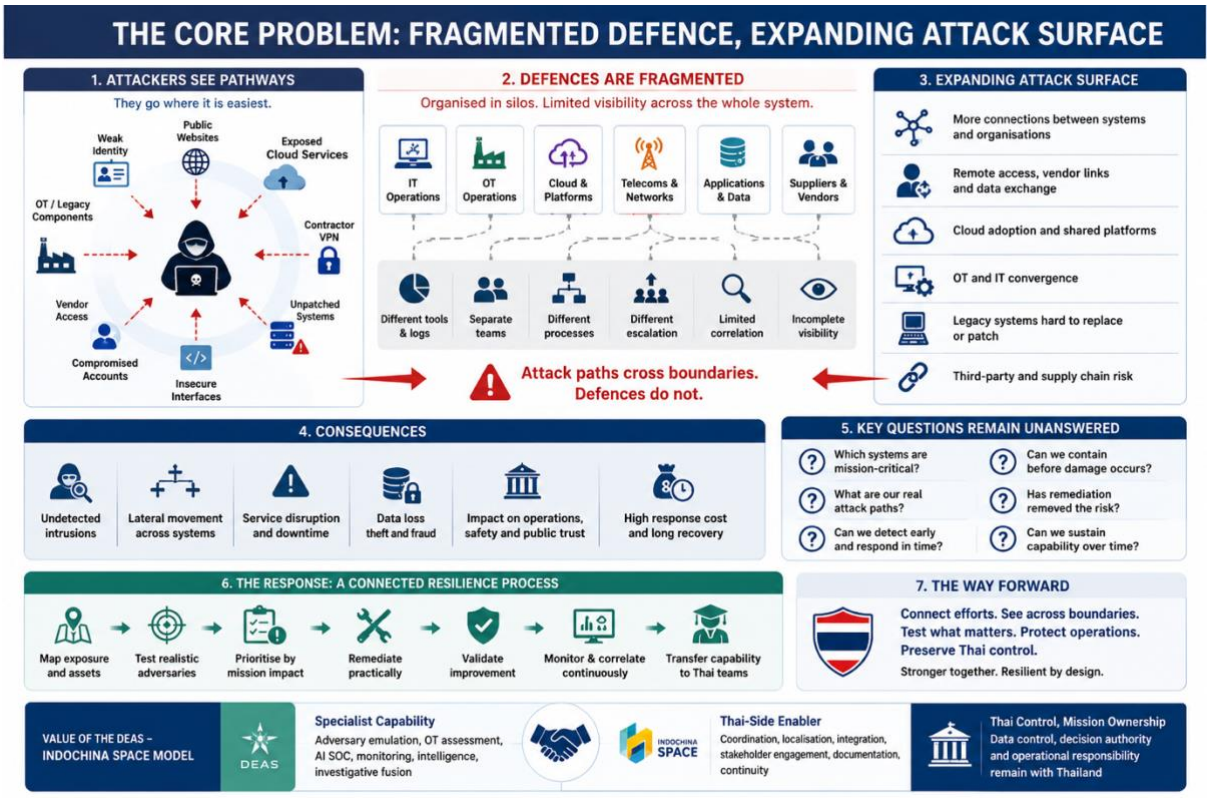



*Figure 2: The issues with a fragmented approach to cybersecurity.*

The result is an active but incomplete defensive posture. Agencies may have capable staff, formal policies, security tools, training programmes, incident processes, and audit regimes, while still struggling to answer essential operational questions. Which systems are genuinely mission-critical? Which external connections create the highest risk? Which weaknesses can be combined into an attack path? Can the organisation detect a capable adversary early? Can it contain compromise before operational damage occurs? Has remediation been validated? Can local teams sustain the process over time?

**The response should be a structured resilience process rather than further accumulation of disconnected tools.** Exposure must be mapped across systems and organisational boundaries. Realistic adversary behaviour must be tested under approved conditions. Findings must be prioritised by mission consequence. Remediation must be practical, documented, and verified. Monitoring must improve from isolated alerts to correlated operational awareness. Training must transfer methods to Thai teams so that capability remains after external support ends.

This is where the DEAS–Indochina Space model has practical value. DEAS can provide specialist capability in adversary emulation, operational-technology assessment, AI-enabled SOC support, managed monitoring, cyber intelligence, and investigative fusion. Indochina Space can provide Thai-side coordination, localisation, integration support, stakeholder engagement, documentation, and continuity. The objective is to connect assessment, remediation, validation, monitoring, and capability transfer into one process.

**The core problem is therefore fragmentation. Thailand has active cyber institutions, capable personnel, legal frameworks, military cyber functions, law-enforcement structures, national coordination bodies, and sectoral response mechanisms. The next requirement is to connect these efforts into a process that sees across boundaries, tests real attack paths, protects operational systems, and preserves Thai control while using specialist external expertise where it adds measurable value.**

# A Process for Enhancing Cybersecurity in Thai Government Environments

Thai Government cybersecurity should be strengthened through a staged resilience process. The objective is to move from partial visibility and periodic assurance towards a repeatable model that identifies exposure, tests realistic threats, closes weaknesses, validates improvement, and leaves Thai teams with sustainable operational capability.

The proposed process has nine stages: discover, assess, emulate, prioritise, remediate, validate, monitor, train, and sustain.

**Discover.** The first stage is to establish a clear view of the environment being protected. This includes identifying critical systems, exposed services, privileged users, external connections, cloud platforms, operational-technology assets, supplier access routes, data flows, and mission dependencies. Discovery should focus on what matters operationally, rather than producing a large inventory with little risk context.

**Assess.** The second stage is to examine the technical and organisational weaknesses that could affect those systems. This includes configuration weaknesses, identity and access-control issues, remote-access exposure, insecure interfaces, insufficient logging, weak segmentation, legacy-system risk, third-party dependencies, and OT/IT convergence points. Assessment should distinguish between ordinary technical findings and weaknesses that could affect essential services, public trust, defence readiness, investigations, healthcare delivery, or Critical Information Infrastructure.

**Emulate.** The third stage is to test realistic adversary behaviour under approved and controlled conditions. Adversary emulation shows how a capable attacker could move from initial access to operational effect. It can test reconnaissance, credential misuse, lateral movement, persistence, data access, service disruption, and response procedures. This stage gives decision-makers a practical view of real attack paths, rather than a theoretical list of vulnerabilities.

**Prioritise.** The fourth stage is to rank findings by mission consequence. Government agencies should not treat every vulnerability as equal. A weakness affecting a public-facing low-risk system is different from one that enables access to command networks, hospital systems, financial-crime data, OT environments, or national coordination platforms. Prioritisation should consider likelihood, exploitability, system criticality, operational impact, public sensitivity, legal exposure, and remediation feasibility.

**Remediate.** The fifth stage is to close the most important weaknesses through practical corrective action. Remediation may include access-control reform, segmentation, secure remote-access design, patching, hardening, logging improvements, supplier-control changes, incident-response workflow updates, monitoring improvements, or compensating controls for legacy systems that cannot be replaced quickly. Remediation should be documented clearly, with responsibility assigned to the appropriate Thai agency, integrator, vendor, or operating team.

**Validate.** The sixth stage is to verify that remediation has reduced risk. Validation may include re-testing, configuration review, attack-path closure checks, detection testing, log verification, and operational exercises. This stage is essential because corrective action has limited value unless it can be shown to have worked. Validation converts cybersecurity activity into evidence of improved protection.

**Monitor.** The seventh stage is to move from periodic assessment to continuous operational awareness. Monitoring should correlate security events, identity activity, network behaviour, endpoint data, remote-access logs, threat intelligence, and operational context. For national or sector-wide environments, monitoring should support triage and escalation rather than producing unmanaged alert volume. The objective is earlier detection, clearer prioritisation, and faster response.

**Train.** The eighth stage is to transfer methods and operational knowledge to Thai teams. Training should be linked to the systems and workflows actually used by the agency. It should include analyst workflows, incident

handling, evidence preservation, OT-specific precautions, adversary techniques, monitoring interpretation, escalation procedures, and post-incident review. Training should build confidence in Thai operators, not dependency on external personnel.

**Sustain.** The final stage is to make the capability durable. Sustainment requires governance, periodic re-assessment, updated threat scenarios, refreshed asset and dependency maps, maintained monitoring rules, tested incident procedures, supplier-control reviews, and clear ownership of the resilience process. The end-state should be a Thai-controlled capability that can be improved over time.

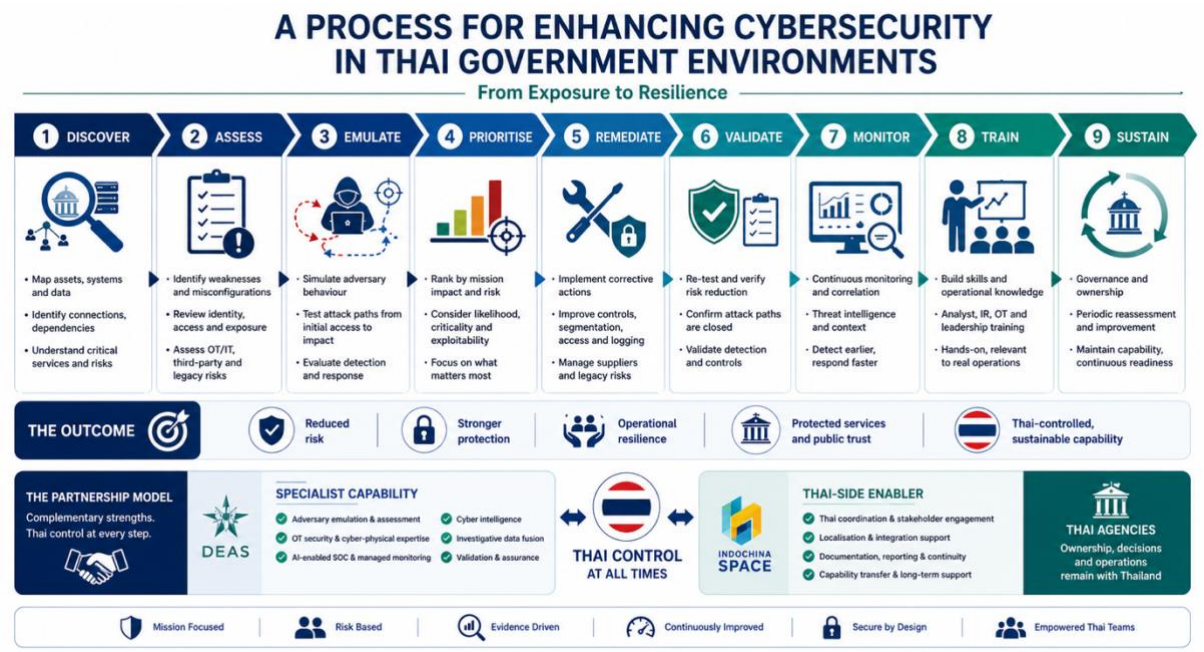



*Figure 3: A staged process for complete cybersecurity resilience.*

**This staged process gives Thai agencies a disciplined route from risk discovery to verified protection.** It also defines where DEAS and Indochina Space can add value. DEAS can provide specialist methods, platforms, adversary emulation, OT assessment, AI-enabled SOC support, cyber intelligence, and validation expertise. Indochina Space can provide Thai-side coordination, localisation, integration support, documentation, stakeholder engagement, and continuity. Thai agencies retain command authority, data control, approval of testing, remediation ownership, and operational decision-making throughout the process.

The value of the model is its sequence. Discovery without assessment produces inventory. Assessment without emulation produces limited assurance. Emulation without remediation produces awareness without improvement. Remediation without validation produces uncertainty. Monitoring without training produces dependency. Training without sustainment produces temporary capability. The full process creates a practical path from exposure to resilience.

## DEAS and Indochina Space Operating Model

The proposed operating model combines specialist international cyber capability with Thai-side implementation, coordination, and sustainment. DEAS Cyber+ provides the technical depth, methods, platforms, and operational cyber expertise. Indochina Space provides the local structure required to make those capabilities usable within Thai Government environments.

*DEAS acts as the specialist capability provider. Its role is to deliver advanced cyber methodology, technical tools, operational platforms, cyber intelligence support, adversary emulation, AI-enabled Security Operations Centre*

*capability, operational-technology assessment, and specialist training. These capabilities are relevant where Thai agencies require assessment beyond ordinary IT security, realistic attack-path testing, stronger monitoring, improved incident response, and protection of critical or cyber-physical systems.*

*Indochina Space acts as the Thai implementation and continuity partner. Its role is to coordinate with government stakeholders, support local project management, assist with integration into Thai operational environments, prepare documentation, manage local communication, and maintain continuity between DEAS specialists and Thai agencies. This role is important because cyber capability must be adapted to Thai institutional structures, approval processes, operational realities, language requirements, and legal responsibilities.*

**The model preserves Thai command authority**. Thai agencies retain control over scope, testing approval, system access, data handling, reporting, remediation decisions, operational priorities, and final use of any findings. DEAS and Indochina Space provide support within approved boundaries. They do not replace agency ownership of mission, data, or decision-making.

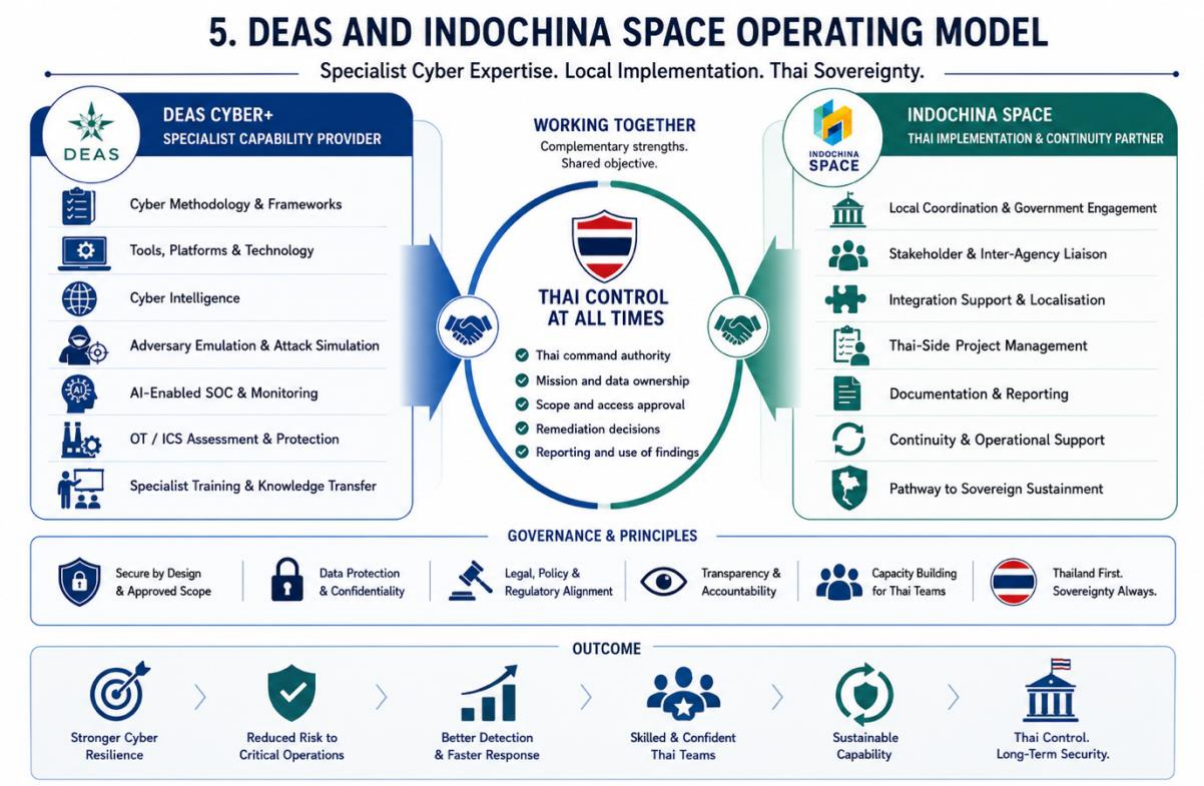



*Figure 4: DEAS and Indochina Space operating model.*

The model also separates specialist delivery from sovereign sustainment. DEAS can introduce advanced methods, platforms, and training; Indochina Space can help embed them into Thai workflows and support their continued use. Over time, the objective is to reduce dependence on external intervention by transferring procedures, operating knowledge, documentation, and practical skills to Thai teams.

This structure is particularly suitable for sensitive government environments. Defence networks, law-enforcement systems, public health platforms, Critical Information Infrastructure, and national cyber coordination functions require technical capability and local accountability at the same time. The DEAS–Indochina Space model provides access to specialist cyber expertise while keeping implementation, continuity, and operational control anchored in Thailand.

The operating model should therefore be treated as a partnership framework, rather than a vendor delivery arrangement. DEAS strengthens the technical and methodological base. Indochina Space provides the local implementation layer. Thai agencies retain authority and ownership. The intended outcome is a practical route from external expertise to Thai-controlled cyber resilience.

## Capability Modules

The proposed process is supported by six capability modules. Each module addresses a different part of the cyber-resilience problem: operational technology exposure, intelligence fusion, continuous monitoring, realistic adversary testing, controlled access and compliance, and long-term capability development.

### Archimede: OT and Cyber-Physical Security

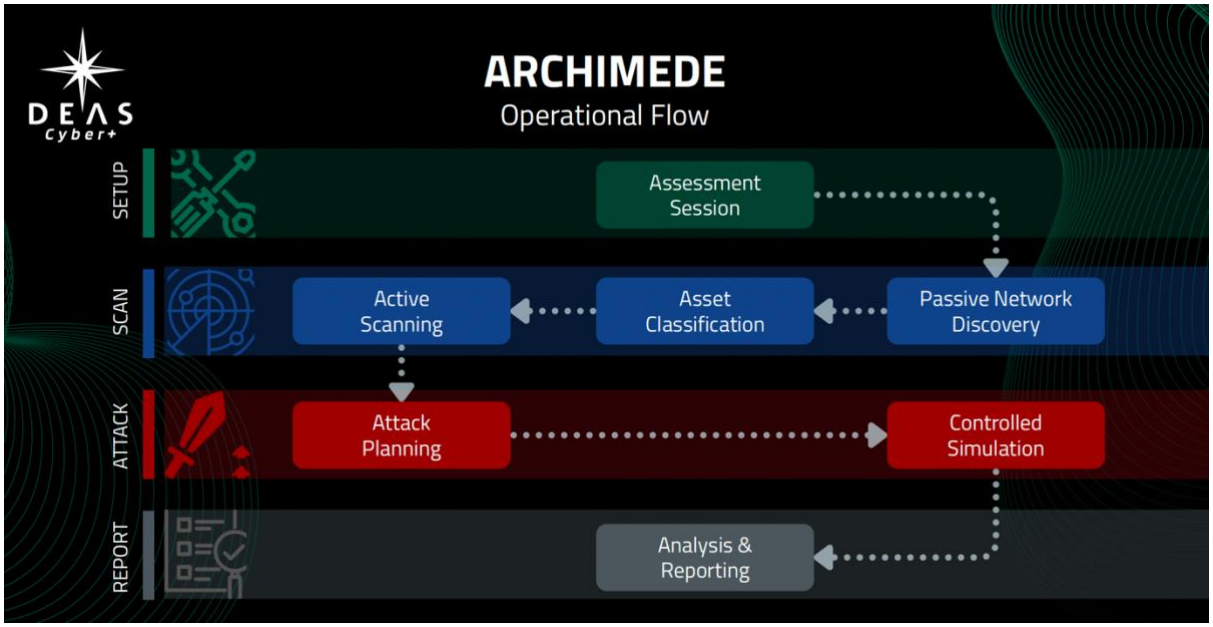



*Figure 5: Archimede operational flow.*

Archimede supports the assessment of Operational Technology, Industrial Control Systems, and cyber-physical environments. These environments include control systems, sensors, radar-related infrastructure, hospital support systems, utility assets, field devices, and other systems where digital compromise can affect physical operations or essential services.

Its value lies in assessing systems that cannot be treated like ordinary office IT. Many OT environments contain legacy devices, fragile protocols, vendor-managed components, long replacement cycles, and strict availability requirements. Standard scanning or intrusive testing can create operational risk if applied without adaptation. Archimede provides a more suitable approach by supporting passive discovery, calibrated assessment, asset classification, controlled testing, and structured vulnerability analysis.

**For Thai Government environments, Archimede is most relevant where operational continuity matters. This includes defence infrastructure, utilities, public health systems, transport systems, communications networks, and other Critical Information Infrastructure.** The objective is to identify exposure, understand dependencies, recommend practical controls, and reduce risk without disrupting the systems being protected.

## Orion: Intelligence and Investigative Fusion

Orion supports intelligence-led analysis by aggregating and correlating heterogeneous data. It is designed for environments where relevant information is spread across different systems, formats, agencies, sources, and investigative workflows.

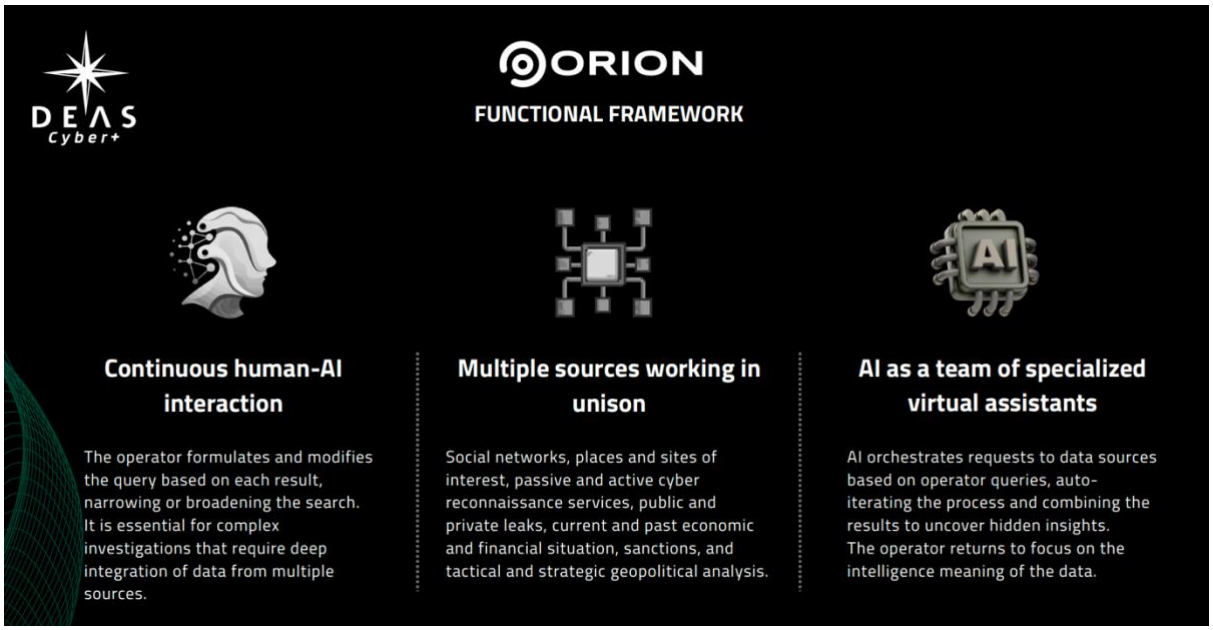



*Figure 6: ORION functionality.*

Its value lies in turning fragmented data into an operational picture. Cybercrime investigations, anti-scam operations, national threat monitoring, fraud analysis, digital evidence review, and cross-sector incident coordination all depend on the ability to connect weak signals. These may include technical indicators, financial traces, telecommunications data, open-source intelligence, leaked data, malware patterns, infrastructure links, and case records.

**For Thai agencies, Orion is particularly relevant to CCIB, anti-scam operations, NCSA, ThaiCERT, defence intelligence support, and sector-level cyber coordination.** It can support analysts by improving correlation, accelerating investigation, identifying hidden relationships, and providing a clearer basis for operational decision-making. It should be used as an intelligence-support capability under Thai data-control and access rules.

## AI SOC and MSSP: Continuous Monitoring and Managed Response

The AI SOC and Managed Security Service Provider model supports continuous monitoring, event correlation, incident triage, and managed protection. It is relevant where agencies face high alert volumes, limited analyst availability, distributed infrastructure, or the need for 24/7 operational awareness.

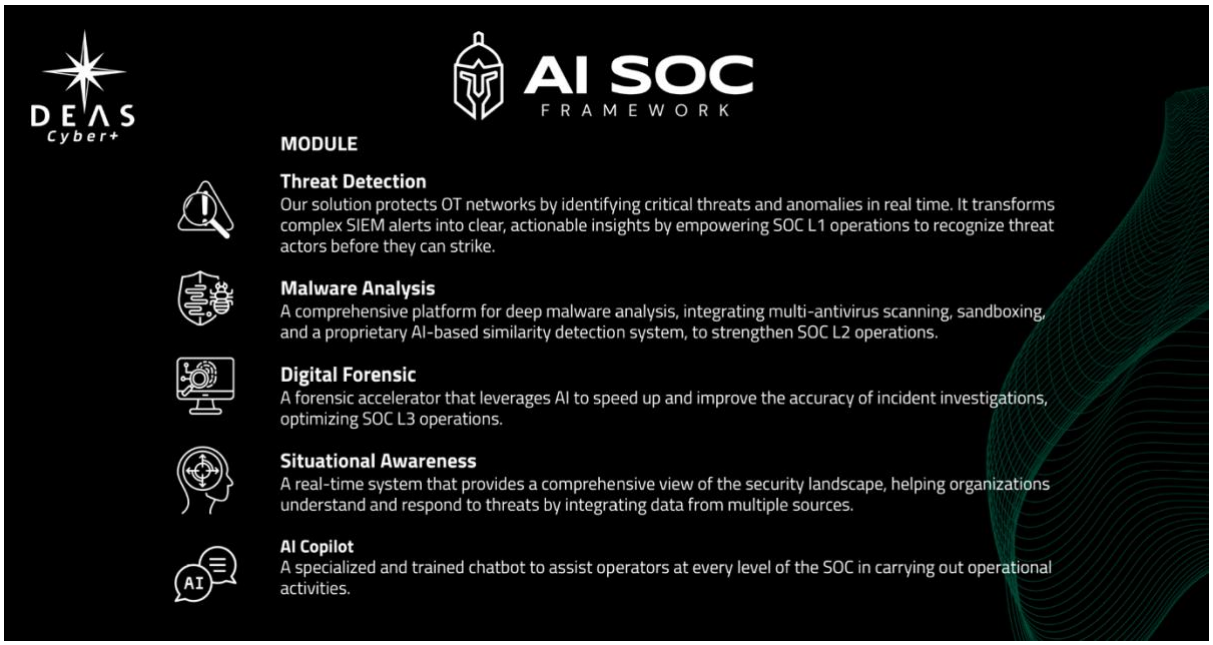



*Figure 7: Security Operations Centre functionality.*

Its value lies in improving detection and response at scale. A Security Operations Centre can integrate signals from network monitoring, endpoints, identity systems, threat intelligence, logs, remote-access channels, and operational systems. AI-enabled workflows can support malware clustering, event prioritisation, analyst guidance, and faster response. Managed services can help agencies maintain coverage while internal capacity is being developed.

**For Thai Government environments, this module is relevant to national cyber coordination, Health CIRT, defence cyber centres, public-sector platforms, and Critical Information Infrastructure operators. It can help move agencies from isolated alert handling towards correlated operational awareness.** Its deployment should be governed by clear rules on data handling, escalation authority, reporting, and Thai agency ownership.

## Adversary Emulation: Realistic Resilience Testing

Adversary emulation tests how a capable attacker could compromise an organisation under authorised and controlled conditions. It goes beyond ordinary vulnerability assessment by examining attack paths, decision points, detection capability, escalation, lateral movement, persistence, data access, and operational consequences.


*Figure 8: DEAS adversary emulation capabilities.*

Its value lies in exposing how weaknesses combine. A single vulnerability may appear manageable when considered alone. Several modest weaknesses can become serious when chained together through identity misuse, weak segmentation, supplier access, exposed services, and poor monitoring. Adversary emulation shows whether existing controls would stop, detect, or delay a realistic attack.

**For Thai agencies, this module is relevant to defence networks, national cyber exercises, CII validation, anti-scam infrastructure, law-enforcement systems, health platforms, and high-value government services.** It should be conducted only with approved scope, agreed rules of engagement, defined safety limits, and clear reporting lines. The output should be practical: attack paths, operational impact, remediation priorities, and validation steps.

## Zero Trust and Compliance: Controlled Access and Governance

Zero Trust provides a governance and architecture model based on continuous verification, least privilege, strong identity control, segmentation, and explicit trust boundaries. It is useful in government environments where users, contractors, suppliers, agencies, cloud systems, and operational platforms interact across complex networks.

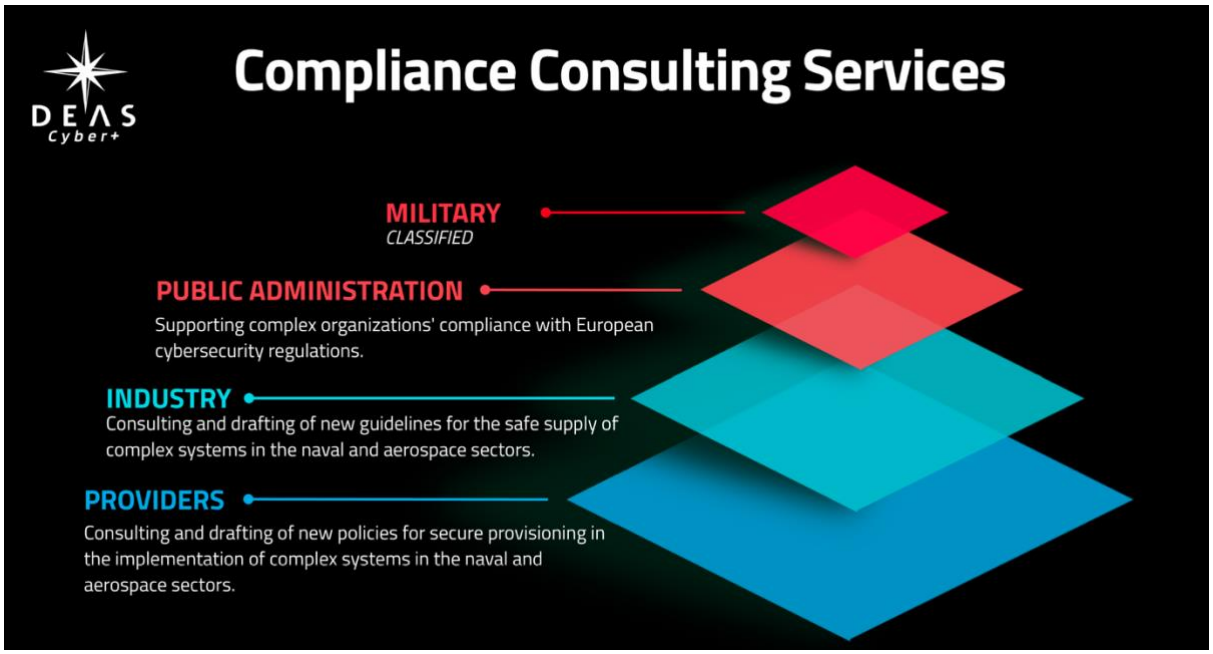



*Figure 9: Cybersecurity compliance services list.*

Its value lies in reducing implicit trust. Many cyber incidents exploit excessive access, weak identity controls, unmanaged remote access, shared accounts, persistent VPNs, poorly segmented networks, or insufficient monitoring of privileged activity. A Zero Trust approach helps agencies define who can access which systems, under what conditions, for what purpose, and with what level of monitoring.

Compliance remains important. Thai agencies must meet legal and regulatory obligations, including cybersecurity, data protection, procurement, sectoral, and audit requirements. The proposed approach treats compliance as governance support for resilience. Policies, standards, and audit evidence should align with operational reality, including tested controls, verified remediation, incident procedures, and documented ownership.

## Capacity Building: Training, Transfer, and Sustainment

Capacity building ensures that cyber improvement remains in Thailand after external support has ended. It should be treated as a core capability module rather than an optional training add-on.

Its value lies in reducing long-term dependency. **Thai teams need practical knowledge of the systems they operate, the threats they face, the tools they use, and the procedures they must execute. Training should therefore be linked to real agency environments, live workflows, approved exercises, incident scenarios, OT-specific precautions, SOC operations, intelligence analysis, evidence handling, and management escalation.**

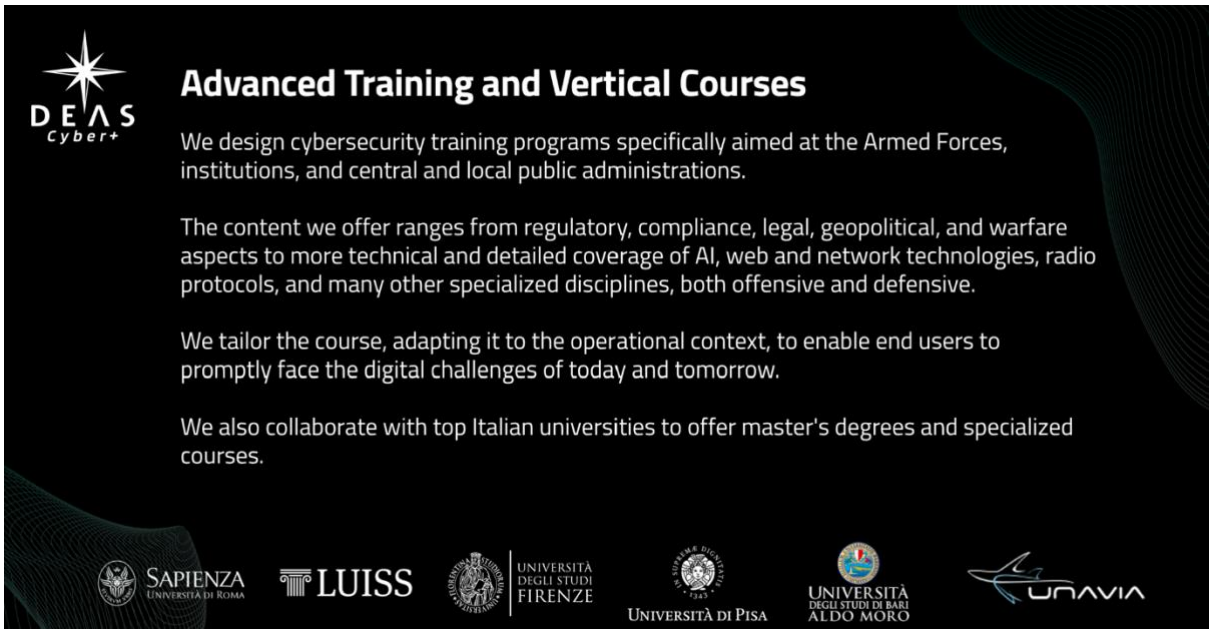



*Figure 10: Advanced training services.*

Capacity building should include technical training, analyst mentoring, exercise participation, documentation, operating procedures, post-incident review methods, and periodic reassessment. Indochina Space can support this process by maintaining local continuity, coordinating stakeholders, preparing documentation, and helping translate specialist methods into Thai operating practice. DEAS can provide the specialist technical content, exercise design, advanced methodology, and platform-specific training.

### Combined Value of the Modules

These modules are strongest when used as part of one process. Archimede identifies OT and cyber-physical exposure. Orion strengthens intelligence fusion. AI SOC and MSSP improve continuous monitoring and response. Adversary emulation tests real attack paths. Zero Trust and compliance provide governance and access control. Capacity building transfers knowledge to Thai teams.

Together, they create a practical capability architecture for Thai Government cybersecurity. The aim is to move from isolated tools and periodic assurance towards a Thai-controlled resilience model that can discover exposure, test threats, close weaknesses, monitor continuously, and sustain capability over time.

## Application to Thai Government Sectors

The proposed capability model can be applied selectively across Thai Government sectors according to mission risk, operational sensitivity, and institutional mandate. Each sector has a different cyber profile, but the same core principles apply: understand exposure, test realistic threats, prioritise operational consequence, improve monitoring, validate remediation, and transfer capability to Thai teams.

### NCSA and ThaiCERT

NCSA and ThaiCERT are central to Thailand's national cyber coordination function. Their role requires broad visibility across Critical Information Infrastructure, rapid incident handling, technical guidance, inter-agency coordination, and support to national cyber readiness.

**The proposed model can support NCSA through national cyber monitoring uplift, CII resilience testing, intelligence fusion, and structured cyber exercises.** AI SOC and MSSP capabilities can help manage high alert

volumes and improve triage. Orion can support cross-agency intelligence correlation. Adversary emulation can test whether existing coordination frameworks work under realistic pressure.

*A practical first step would be a controlled pilot exercise with selected CII operators in a high-priority sector such as energy, finance, telecommunications, or public health. The exercise should test technical defences, reporting channels, escalation procedures, inter-agency communication, and decision-making under realistic conditions. The output should be a validated improvement plan for participating organisations and a reusable exercise model for wider national deployment.*

This approach would strengthen NCSA's ability to move from coordination to measurable resilience. It would also give ThaiCERT better operational context for incident response, threat prioritisation, and national-level reporting.

### Defence and Armed Forces

Thai defence environments require cybersecurity that supports operational readiness. Military networks, command systems, radar infrastructure, communications gateways, logistics platforms, training networks, shipboard systems, air operations infrastructure, and hybrid IT/OT environments must remain available, trusted, and resilient under pressure.

**The proposed model can support the Royal Thai Armed Forces, Royal Thai Air Force, Royal Thai Navy, and other defence bodies through military-grade adversary emulation, operational-technology assessment, defence SOC strengthening, cyber exercise design, and command-chain validation.** Archimede is relevant to radar, sensors, shipboard systems, industrial support systems, base infrastructure, and other cyber-physical assets. Orion can support classified or controlled intelligence analysis, subject to Thai data-control rules. AI SOC capabilities can improve detection, triage, and response in defence networks.

*The strongest initial use case is a Thai adaptation of a military cyber exercise model. This could focus on air defence systems, naval operational networks, logistics infrastructure, or joint command-support systems. The purpose would be to test how cyber incidents affect mission continuity, alert chains, command escalation, sensor confidence, communications, and operational decision-making.*

Defence cybersecurity must remain mission-led. Technical findings should be translated into operational meaning: what could be disrupted, what could be misled, what could be delayed, what could be exfiltrated, and how quickly Thai commanders and operators could respond.

### CCIB and Anti-Scam Operations

Thailand's cybercrime and anti-scam environment is high-volume, data-intensive, and operationally time-sensitive. CCIB, AOC, ASCS, and related police and government structures must process large numbers of reports, digital traces, suspicious accounts, financial movements, telecommunications indicators, social media artefacts, mule-account networks, cryptocurrency trails, and international leads.

**The proposed model can support this environment through intelligence fusion, AI-assisted investigation, malware clustering, digital evidence protection, infrastructure hardening, and resilience testing of investigative systems.** Orion is particularly relevant because cybercrime investigations often require correlation across fragmented sources. AI SOC capabilities can support rapid analysis of technical indicators, malicious infrastructure, phishing campaigns, malware families, and repeated criminal patterns.

Adversary emulation also has value for law-enforcement and anti-scam environments. It can test whether investigative platforms, evidence repositories, reporting systems, and coordination channels are adequately protected against criminal retaliation, insider compromise, credential theft, or targeted disruption. This matters because successful anti-scam operations can make investigative bodies and evidence systems attractive targets.

*A practical first step would be an intelligence-fusion pilot focused on one high-volume scam type, such as phishing, call-centre fraud, mule-account coordination, or cryptocurrency-enabled fraud. The objective would be to improve*

*pattern recognition, case linkage, suspect-network mapping, and operational prioritisation. A parallel resilience review should assess the security of sensitive investigative data and digital evidence workflows.*

The intended outcome is faster case correlation, stronger protection of evidential systems, and improved operational awareness across agencies, banks, telecoms operators, and international partners.

### MOPH and Health CIRT

Thailand's public health sector requires cybersecurity that protects patient data, public health services, hospital operations, connected medical systems, and national digital health platforms. MOPH and Health CIRT operate in a distributed environment where central policy, provincial hospitals, local systems, web platforms, support infrastructure, and clinical services must be coordinated.

**The proposed model can support MOPH through sector-wide monitoring design, Health CIRT strengthening, incident-response workflow improvement, cyber-physical assessment, and resilience testing of public health platforms.** AI SOC and MSSP capabilities can support continuous monitoring across a large and distributed health environment. Archimede can assess hospital support infrastructure, connected medical systems, and OT-like environments where availability and safety matter. Orion can provide threat and incident correlation across the sector.

*A practical first step would be a feasibility study for a coordinated monitoring architecture for Health CIRT. This should define what data should be monitored, which entities should report, how alerts should be prioritised, how provincial systems should escalate incidents, and how MOPH should maintain a national view without over-centralising sensitive data.*

A second step would be targeted assessment of selected hospitals and digital health platforms. This should include identity controls, exposed services, remote access, web applications, backup resilience, incident reporting, connected devices, and support infrastructure. The objective is to protect patient services and data while improving Health CIRT's ability to detect and coordinate response.

### Power, Utility, and Other CII Environments

Power, utility, telecommunications, transport, water, and other Critical Information Infrastructure environments require cybersecurity that protects operational continuity. These sectors depend on interconnected control centres, substations, field devices, telemetry, SCADA, communications links, maintenance providers, external data exchanges, and legacy operational assets.

**The proposed model can support CII operators through OT asset discovery, boundary assessment, remote-access review, segmentation analysis, supplier-interface assessment, incident-response validation, and continuous monitoring.** Archimede is central to this use case because many utility environments contain OT and ICS assets that require careful assessment. AI SOC capabilities can improve visibility and alert correlation. Adversary emulation can test whether an attacker could move from enterprise systems, supplier access, or remote connectivity towards operational impact.

The highest-risk areas are often found at operational boundaries. These include vendor access, third-party maintenance links, inter-control-centre data exchange, insecure remote sessions, poorly governed privileged accounts, weak segmentation between IT and OT, and legacy devices that cannot be patched easily. These areas should be assessed early because they can create routes into critical operations.

*A practical first step would be a **boundary-focused OT resilience assessment** for a selected utility or CII operator. The assessment should map external connections, trust relationships, remote-access mechanisms, segmentation controls, key operational assets, and incident containment procedures. The output should be a prioritised remediation plan and a validation exercise to confirm that the highest-risk pathways have been reduced.*

## Cross-Sector Integration

**The strongest value comes from applying the model across sectors without forcing every agency into the same technical template.** NCSA requires national coordination and CII visibility. Defence requires mission assurance and operational impact testing. CCIB and anti-scam bodies require intelligence fusion and evidential resilience. MOPH requires distributed monitoring and patient-service protection. Utilities require OT resilience and boundary control.

The common requirement is a shared process. Each sector should discover its real exposure, assess weaknesses in context, emulate realistic threats, prioritise by mission impact, remediate practically, validate improvement, monitor continuously, train Thai teams, and sustain capability over time.

This approach allows Thailand to strengthen cybersecurity where it matters most while respecting institutional mandates, data sensitivity, legal authority, and operational command. DEAS contributes specialist cyber capability. Indochina Space supports Thai-side implementation and continuity. Thai agencies retain ownership, control, and decision authority throughout.

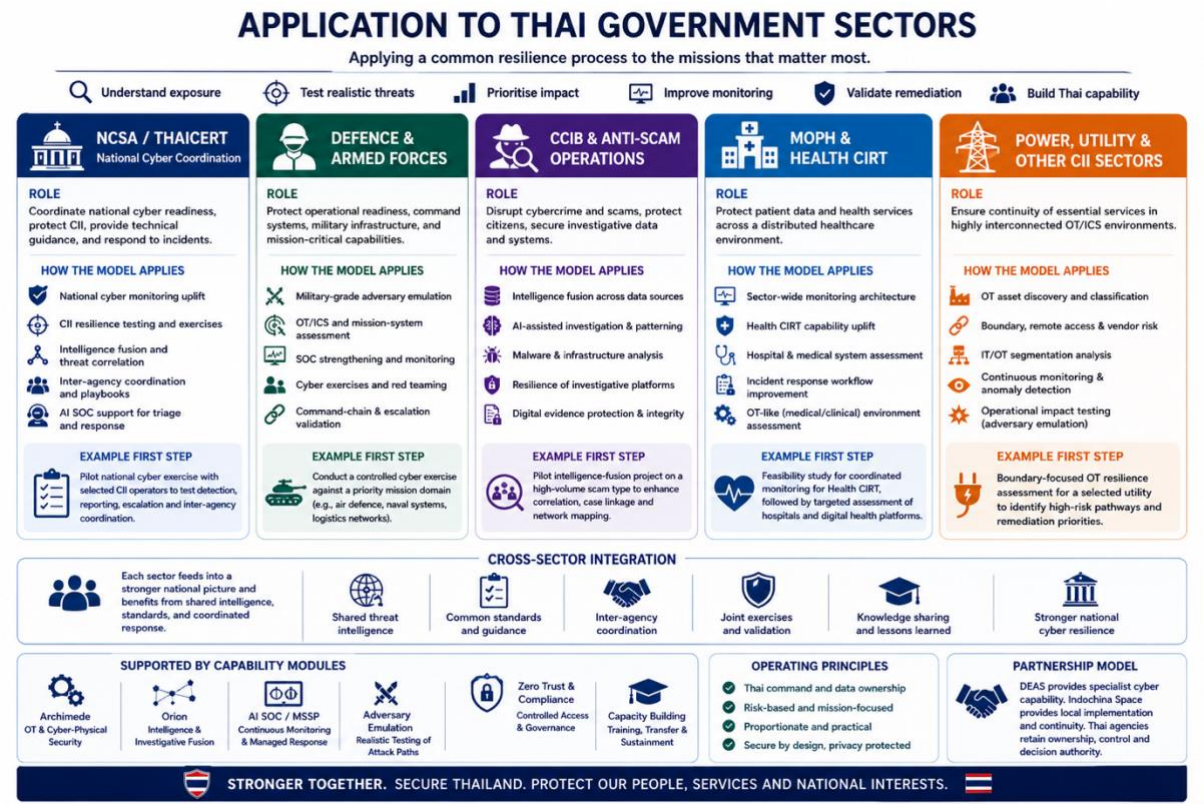



*Figure 11: Application of DEAS solutions to government sectors.*

# Governance, Data Control and Sovereignty

Governance is central to any cybersecurity support model for Thai Government environments. Cybersecurity work in defence, policing, public health, national coordination, and Critical Information Infrastructure involves sensitive systems, sensitive data, legal duties, and public accountability. **The operating model must therefore be built around Thai authority from the start.**

*Thai agencies retain command authority at all times. They define the mission, approve the scope, decide which systems may be examined, set operational constraints, and determine how findings are used. DEAS and Indochina Space*

*provide technical and implementation support within those approved limits. They do not take operational control of government systems or replace agency decision-making.*

**Thai agencies retain mission ownership.** Each organisation remains responsible for the public function, defence mission, investigation, health service, infrastructure operation, or national coordination role that it performs. Cybersecurity support should strengthen that mission, not create a parallel structure outside the agency's chain of authority. Technical work must therefore be aligned with the agency's operational priorities, risk appetite, legal obligations, and internal approval processes.

**Thai agencies retain data control.** Access to logs, network information, digital evidence, system configurations, user records, operational data, patient data, classified material, or investigative information must be governed by agency-approved rules. Data handling arrangements should define what may be accessed, where it may be processed, who may see it, how it is stored, how long it is retained, and how it is deleted or returned. Sensitive data should remain within Thai-approved environments unless explicit authority is granted.

**Thai agencies retain test approval.** Adversary emulation, vulnerability assessment, OT testing, monitoring deployment, evidence analysis, and cyber exercises must operate under agreed rules of engagement. These rules should define authorised targets, permitted methods, timing, escalation channels, safety constraints, reporting requirements, and stop conditions. This is especially important in OT, defence, healthcare, utility, and public-service environments where testing can affect operational availability if poorly controlled.

**Thai agencies retain legal responsibility.** Cybersecurity support must comply with Thai law, agency regulations, procurement requirements, data-protection obligations, confidentiality rules, evidential standards, and sector-specific controls. DEAS and Indochina Space can support compliance through documentation, technical reporting, audit evidence, and structured procedures, but accountability remains with the relevant Thai authority.

**Thai agencies retain operational decision-making.** Findings from assessments, monitoring, intelligence analysis, exercises, or incident response should support Thai decision-makers. They should not dictate operational action. Decisions on remediation priority, service interruption, public communication, legal reporting, disciplinary action, supplier management, evidence handling, or escalation to national authorities must remain with the authorised Thai organisation.

**DEAS and Indochina Space provide controlled support within Thai-approved boundaries.** DEAS contributes specialist cyber methods, platforms, intelligence, assessment capability, adversary emulation, AI SOC support, OT expertise, and training. Indochina Space supports local coordination, documentation, stakeholder engagement, integration, continuity, and Thai-side project management. Their roles are enabling roles. The authority to direct, approve, restrict, pause, or terminate activity remains with the Thai agency.

*The governance model should be formalised before technical work begins. Each engagement should include an approved scope, data-handling plan, access-control plan, rules of engagement, reporting structure, escalation process, confidentiality framework, and responsibility matrix. These documents should be clear enough for senior management, legal teams, technical operators, and external partners to understand their respective roles.*

This approach protects sovereignty while allowing Thailand to benefit from specialist cyber expertise. It gives Thai agencies access to advanced assessment, monitoring, intelligence, and resilience methods without surrendering control over systems, data, missions, or decisions. The intended outcome is a cybersecurity partnership that strengthens Thai capability, supports legal accountability, and leaves operational authority where it belongs: with Thailand.


*Figure 12: All control and governance retained by Thai agencies.*

## Concluding Remarks

Thailand's cybersecurity requirement is now a national resilience requirement. Public administration, defence operations, law enforcement, healthcare, utilities, telecommunications, finance, and Critical Information Infrastructure all depend on systems that are increasingly connected, data-driven, and exposed to external dependencies. **Cybersecurity failure in these environments can affect essential services, public trust, operational readiness, investigations, patient safety, and national security.**

The central task is to **move from fragmented defence towards a structured and repeatable resilience process.** Thai agencies need to understand their exposure, assess weaknesses in context, test realistic attack paths, prioritise risk by mission consequence, remediate practical weaknesses, validate improvement, monitor continuously, train local teams, and sustain capability over time. This process turns cybersecurity from a periodic assurance activity into a disciplined operational function.

*DEAS Cyber+ and Indochina Space can support this transition through a clear division of roles. DEAS provides specialist cyber methodology, platforms, intelligence, adversary emulation, AI-enabled SOC capability, OT assessment, and training. Indochina Space provides Thai-side coordination, government engagement, integration support, documentation, continuity, and project management. Thai agencies retain command authority, mission ownership, data control, testing approval, legal responsibility, and operational decision-making throughout.*

The proposed model is applicable across several high-value environments. NCSA and ThaiCERT can use it to strengthen national monitoring, CII resilience testing, incident coordination, and intelligence fusion. Defence organisations can use it to test mission impact, protect command chains, assess hybrid IT/OT systems, and improve cyber readiness. CCIB and anti-scam bodies can use it to improve investigative fusion, digital evidence protection, and resilience of high-volume cybercrime operations. MOPH and Health CIRT can use it to improve sector-wide visibility, incident response, and protection of health platforms and cyber-physical systems. Power, utility, and

other CII operators can use it to strengthen OT visibility, boundary control, supplier-risk management, and operational continuity.

The policy conclusion is straightforward. **Thailand does not need more disconnected cyber tools. It needs a Thai-controlled process that connects assessment, remediation, validation, monitoring, and capability transfer.** External expertise should strengthen Thai capability, not replace it. The intended outcome is stronger protection for critical systems, faster detection and response, better evidence of risk reduction, and a sustainable national cyber capability that remains under Thai authority.