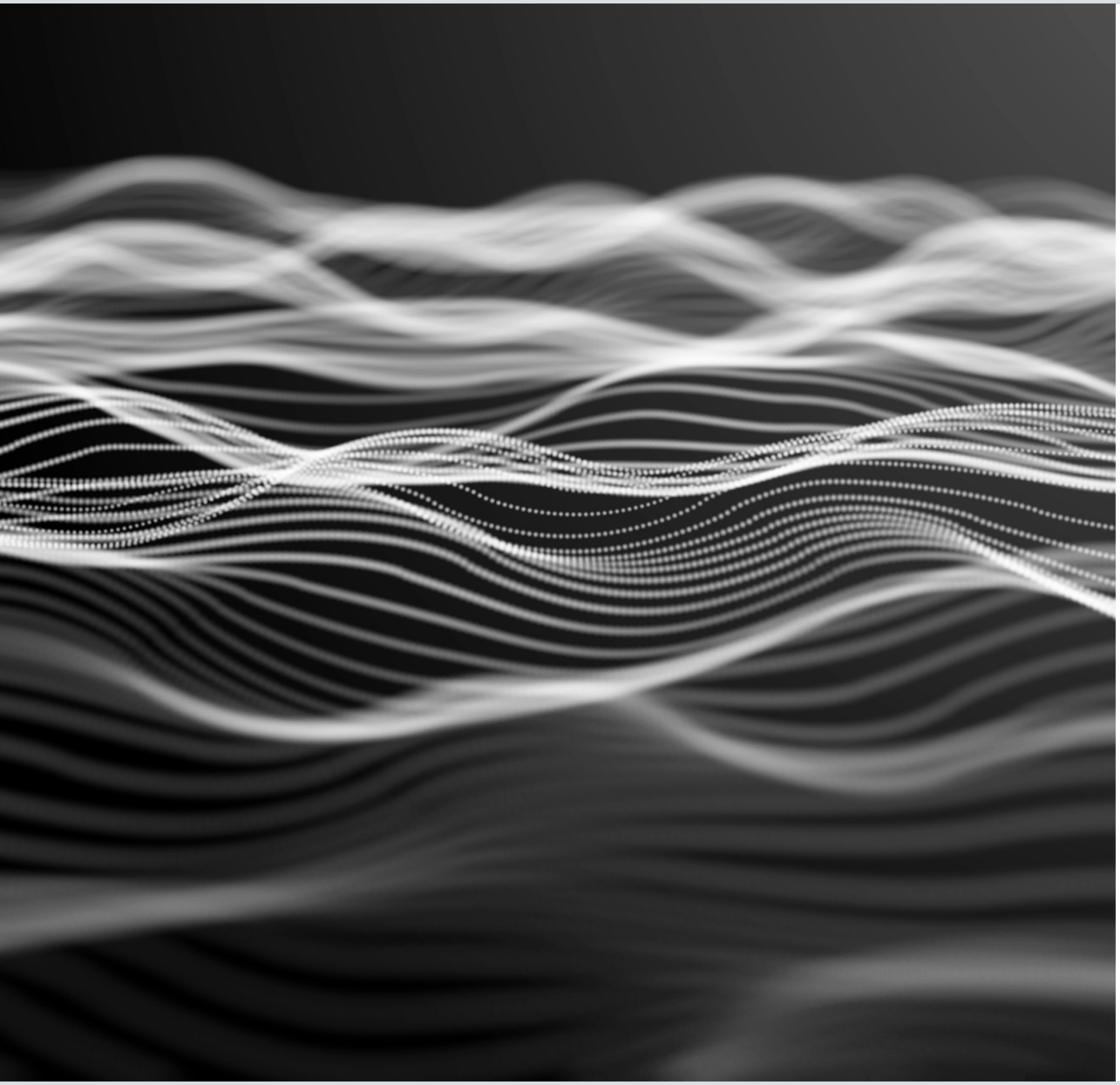


Applying threat-informed approach for fit-for-purpose cybersecurity target maturity setting for organisations

Prepared for CTID Asia-Pacific ATT&CK Community Workshop 2024

26 April 2024

RESTRICTED

Non-exhaustive

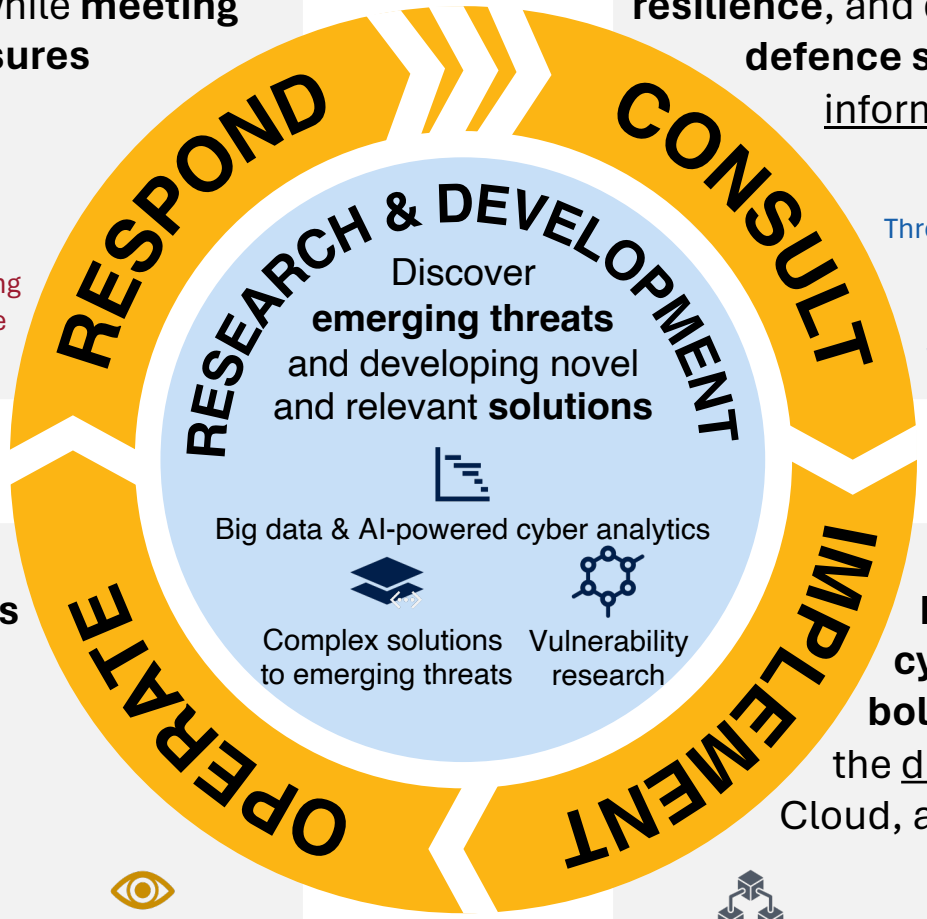
ENSIGN INFOSECURITY

Applying **deep expertise in technologies** including IT, ICS, SCADA, IoT and Cloud to support clients in distress while **meeting urgent timelines and pressures**

- Complete digital forensic tools for all technologies
- Ready-to-deploy expertise supporting regional coverage

Applying expertise to help clients **understand** and **transform** their **cyber-resilience**, and develop **cybersecurity defence strategy** through threat-informed approaches

- Threat Intelligence Analysis
- Advisory
- Security Assessments & Threat Hunting
- Assurance



End-to-end management of cybersecurity operations through advanced threat detection, continuous monitoring, triage, and first-response services

- End-to-end security management
- Cognitive security operations
- Advanced threat detection & response

Architecting and **Implementing cybersecurity solutions** to **bolster the defences** across the digital attack surface (IT, IoT, Cloud, and OT – ICS & SCADA)

- Complete coverage of technology types
- Deep expertise for integration and operational outcomes
- Design and implement advanced SOCs

Asia's largest pure play cybersecurity services company with **over 900 cybersecurity professionals**.

Our clients trust and rely on us to bring our collective capabilities and innovative solutions across **Consulting, Systems Integration, Managed Services** and **Labs** to deliver cyber excellence.

We work with our clients to transform them into cyber-resilient leaders, helping them **Conquer the Unknown**.

Ensign's Threat-Informed Defence Framework (TIDF)

- Works with NIST's Cybersecurity Maturity Framework (CSF) v2.0 to determine the threat informed target maturity level to establish the fit-for-purpose target state rather than to rely on benchmarked data which does not allow for directly relevant target state analysis
- Leverages other reputable cybersecurity frameworks such as MITRE ATT&CK, NIST SP 800-53, Open FAIR Factor Analysis
- Consistent and repeatable use of the maturity scale for observations
- Leverages Ensign's organic Threat Intelligence Analysis capabilities to determine target state cybersecurity maturity level
- Combined with the CSF, the TIDF allows for the identification of Return on Security Investment (ROSI) and quantification of risks.

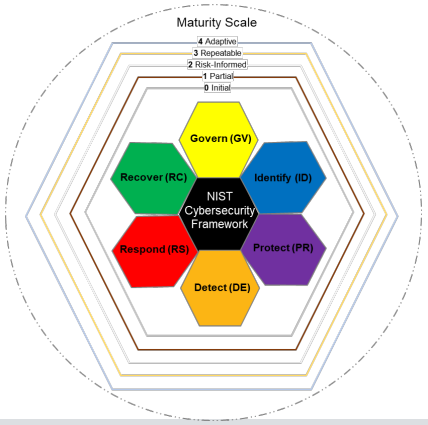
- Identification of **Threat Actors**, **Malicious Software** relevant to the subject organisation(s)
- Establishing the tactics, techniques and procedures (TTPs) affecting the subject organisation(s)
- Using the common taxonomy for threats
- Used to determine the target state maturity leveraging the CSMF

Leverage NIST CSF v2.0, NIST SP 800-53r5, MTIRE ATT&CK *Detections* and *Mitigations*, D3FEND and Engage

- Used to determine expected controls, mitigations and proactive defences to address the threats from technology and procedural angles

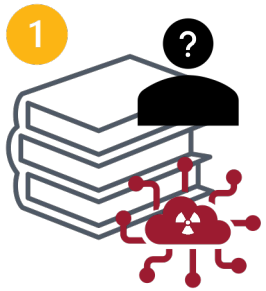
Leverage FAIR and other appropriate risk frameworks to determine risk exposure

- Used to determine the **risk exposure** the subject organisation(s) face



Apply Maturity Assessments for *Assessed State*, *Target State* and *Aspirational Target State*

- Used to present cybersecurity maturity level for the subject organisation(s)
- Helps to determine the fit-for-purpose investment requirements, and aspirational target states (based on proactive defence mechanisms)
- Supports evaluation and strategic planning including Return on Security Investment (ROSI)



PERFORMING THREAT PROFILING OF THE SUBJECT ORGANISATION

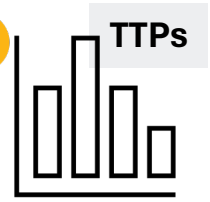
- Conduct research against Ensign Threat Repository for relevant threat groups and malicious software and their associated TTPs
- Relevant threat groups are characterised based on the following:
  - Business activities nature (e.g., sector participation)
  - Territorial exposure / involvement
  - Time currency (6 months / 18 months)

PROFILE THREAT GROUPS AND MALICIOUS SOFTWARE AGAINST ENSIGN THREAT CLASSIFICATION MATRIX

- Profile identified relevant threat groups and malicious software to determine threat "proximity" to subject organisation

ENSIGN THREAT CLASSIFICATION MATRIX	→→→ *Increasing levels of threat to the subject* →→→			
	Insubstantial	**Potential**	**Impending**	**Material**
Capability		●	●	●
Intent	●		●	●
Opportunity	●	●		●

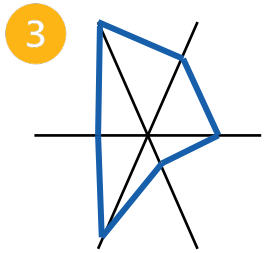
Figure 1: Ensign's Threat Classification Matrix, the criteria and analysis outcomes.



MAP ASSOCIATED TTPs WITH CONTROLS, DETECTIONS, MITIGATIONS, AND PROACTIVE DEFENCES

- Profile the TTPs of relevant threat groups and malicious software into a MITRE ATT&CK Heatmap
- Map TTPs with Detections, Mitigations, Controls (NIST SP 800-53, NIST CSF, ISO 27001) and proactive defences (e.g., MITRE D3FEND and MITRE Engage)

Figure 2: Heatmap of TTPs based on MITRE ATT&CK mapping of TTPs for known threat groups and malicious software.



EVALUATE MATURITY LEVELS (ASSESSED, TARGET, AND ASPIRED TARGET)

- Establish assessed maturity levels from evaluations, target maturity levels from threat profile (MITRE ATT&CK detections and mitigations, and proactive defences from MITRE D3FEND and Engage.

Illustrative

Global Anchor Shipping (GAS), a maritime shipping company is engaged in transporting goods via container ships, managing a fleet that operates on trade routes connecting major ports in **Australia** and **New Zealand** (ANZ). GAS provides **shipping and logistics**, including containerization, supply chain management, freight forwarding, customs clearance, and intermodal transport solutions.

Business activities nature: Maritime and Shipbuilding, Shipping and Logistics
Territorial exposure / involvement: Australia, New Zealand
Time currency: last 18 months

Threat Modelling Parameters

Identify relevant threat actor groups that was observed to have attacked similar organisations like GAS in ANZ and is active in the past **18 months**

Identified **4** **Relevant Threat Groups**

- Volt Typhoon
- Lazarus Group
- Mummy Spider
- Tropical Scorpius

Illustrative

***Capability**: Known to have access to proprietary, highly-effective and/or use of native environment tools*

***Hostile Intent**: Known to have targeted victims in GAS's business activities and relevant geography in the last 18-months*

***Opportunity**: Known to exploit common vulnerabilities (e.g., cyber supply chain) with high success rates*

ENSIGN THREAT CLASSIFICATION MATRIX	*NIL*	Mummy Spider Tropical Scorpius	Lazarus Group	Volt Typhoon
	→→→ *Increasing levels of threat to the subject* →→→			
	INSUBSTANTIAL	POTENTIAL	IMPENDING	MATERIAL
Capability		●	●	●
Intent	●		●	●
Opportunity	●	●		●

Identified **2** **Impending & Material Threat Groups**

- Volt Typhoon
- Lazarus Group

Baseline Defense Posture

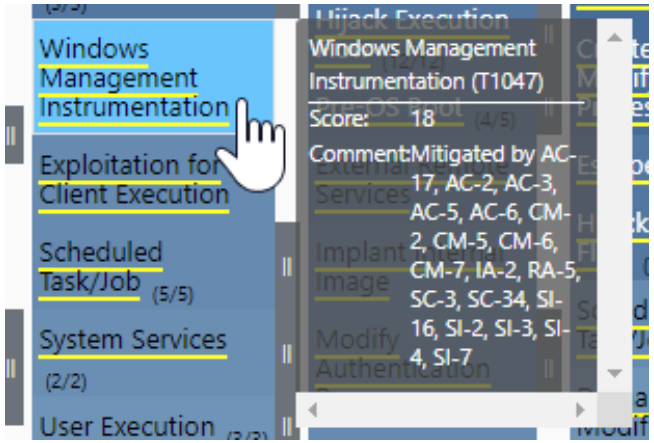
- The baseline defence posture will consider the two (2) **Impending** and **Material** Threat Groups, which will subsequently be mapped to the MITRE ATT&CK Techniques Heatmap.

TTP Heatmap

Consolidate the Techniques used by both threat actor groups across Tactic families

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1589: Gather Victim Identity Information	T1584: Compromise Infrastructure	T1189: Drive-by Compromise	T1047: Windows Management Instrumentation	T1098: Account Manipulation	T1134: Access Token Manipulation	T1036: Masquerading	T1557: Adversary-in-the-Middle	T1087: Account Discovery	T1534: Internal Spearphishing	T1005: Data from Local System	T1573: Encrypted Channel	T1048: Exfiltration Over Alternative Protocol	T1485: Data Destruction
T1591: Gather Victim Org Information	T1588: Obtain Capabilities	T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1098: Account Manipulation	T1497: Virtualization/Sandbox Evasion	T1110: Brute Force	T1057: Process Discovery	T1570: Lateral Tool Transfer	T1074: Data Staged	T1090: Proxy	T1041: Exfiltration Over C2 Channel	T1491: Defacement
T1593: Search Open Websites/Domains	T1583: Acquire Infrastructure	T1566: Phishing	T1203: Exploitation for Client Execution	T1543: Create or Modify System Process	T1547: Boot or Logon Autostart Execution	T1070: Indicator Removal	T1555: Credentials from Password Stores	T1012: Query Registry	T1021: Remote Services	T1560: Archive Collected Data	T1071: Application Layer Protocol	T1567: Exfiltration Over Web Service	T1561: Disk Wipe
	T1587: Develop Capabilities	T1078: Valid Accounts	T1106: Native API	T1574: Hijack Execution Flow	T1543: Create or Modify System Process	T1134: Access Token Manipulation	T1056: Input Capture	T1082: System Information Discovery		T1557: Adversary-in-the-Middle	T1132: Data Encoding		T1489: Service Stop
	T1585: Establish Accounts		T1053: Scheduled Task/Job	T1542: Pre-OS Boot	T1574: Hijack Execution Flow	T1622: Debugger Evasion	T1003: OS Credential Dumping	T1016: System Network Configuration Discovery		T1056: Input Capture	T1001: Data Obfuscation		T1529: System Shutdown/Reboot
	T1608: Stage Capabilities		T1204: User Execution	T1053: Scheduled Task/Job	T1055: Process Injection	T1140: Deobfuscate/Decode Files or Information		T1049: System Network Connections Discovery			T1008: Fallback Channels		
				T1505: Server Software Component	T1053: Scheduled Task/Job	T1564: Hide Artifacts		T1033: System Owner/User Discovery			T1105: Ingress Tool Transfer		
				T1078: Valid Accounts	T1078: Valid Accounts	T1574: Hijack Execution Flow		T1497: Virtualization/Sandbox Evasion			T1104: Multi-Stage Channels		
						T1562: Impair Defenses		T1010: Application Window Discovery			T1571: Non-Standard Port		
						T1656: Impersonation		T1622: Debugger Evasion			T1102: Web Service		
						T1202: Indirect Command Execution		T1083: File and Directory Discovery					
						T1027: Obfuscated Files or Information		T1654: Log Enumeration					
						T1542: Pre-OS Boot		T1046: Network Service Discovery					
						T1055: Process Injection		T1069: Permission Groups Discovery					
						T1620: Reflective Code Loading		T1018: Remote System Discovery					
						T1553: Subvert Trust Controls		T1518: Software Discovery					
						T1218: System Binary Proxy Execution		T1614: System Location Discovery					
						T1221: Template Injection		T1124: System Time Discovery					
						T1078: Valid Accounts							
						T1220: XSL Script Processing							

MITRE ATT&CK mapping of TTPs to NIST SP800-53r5



NIST CSF mapping of TTPs to NIST SP800-53r5

Subcategory	800-53
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	AC-02
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	AC-02
PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	AC-02

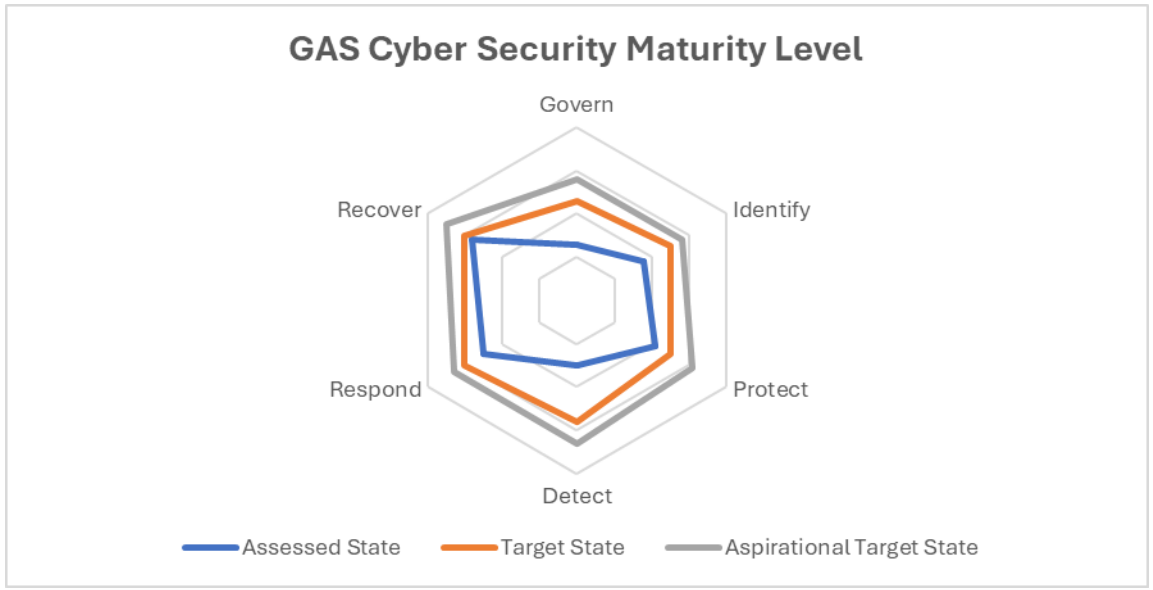
MITRE ATT&CK™

- Detections
- Mitigations

MITRE DEFEND™

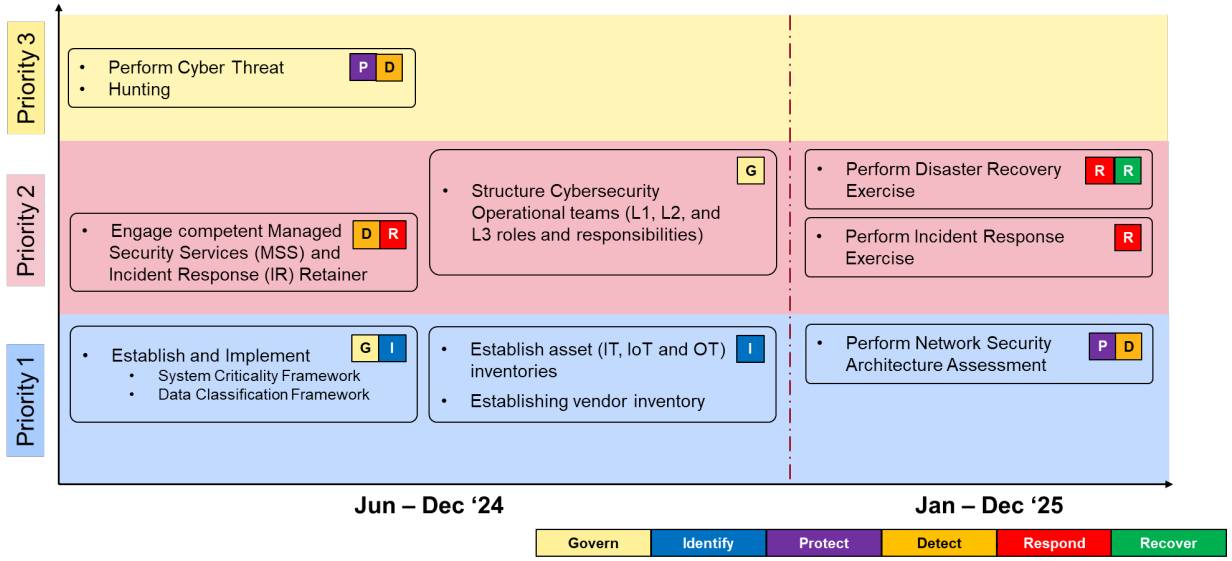
MITRE | Engage™

Translating NIST SP 800-53 controls into maturity levels using NIST CSF



	Govern	Identify	Protect	Detect	Respond	Recover
Assessed State	1.3	1.8	2.1	1.5	2.5	2.8
Target State	2.3	2.5	2.5	2.8	3	3
Aspirational Target State	2.8	2.8	3.1	3.3	3.3	3.5

Providing Executives with the next step, Roadmap of Cybersecurity initiatives



Ray Zhou

Head of Cyber Transformation

ray_zhou@ensigninfosecurity.com
https://www.linkedin.com/in/ruihong-zhou-bb584857

Next Steps:

Connect with me on

For the Ensign Cyber Threat Landscape Report

Download at:
https://www.ensigninfosecurity.com/resources/98