Question(s) to consider:

1. What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?

Cybersecurity Trend 1 - Adoption of Cyber Threat Intelligence(CTI)

Why Use It?

One trend/aspect that Government should be exploring as part of Horizon 2 is the use of cyber threat intelligence to prevent, detect and respond to potential cyber security incidents and assist the decision-making process.

Using an intelligence-led approach, organisations will be able to better understand threat before they can protect against it. If organisations have a good understanding of the threats they face, then they are able to combine this understanding with an assessment of the maturity of their defences to understand the likelihood of an incident occurring. This likelihood can be combined with an assessment of the impact of such an incident to understand the risk. This allows organisations to deploy their usually limited security resources against the highest priority risks.

How To Use It?

Threat intelligence is generally categorized into three types: tactical, operational, and strategic.

Intended audience, and their sphere of influence determine the threat intelligence category. Threat intelligence is most readily understood and properly applied when targeted and delivered in packages designed for a specific audience, below are some examples:

- **Tactical** - Technical indicators and to inform network level action and remediation. Audience: Security Operations, Cyber Defenders and Incident Response.
- **Operational** - Intelligence on adversary behaviour informing: holistic remediation, threat hunting, behavioural detection, purchasing decisions, and data collection. Audience: Threat Hunters, Incident Response and Security Leadership.
- **Strategic** - Places threat into a business context and describes strategic impact informing risk management and organizational direction. Audience: Security Leadership and Organisational Leadership.

Cyber Threat Intelligence lifecycle enhances an organization's ability to defend against cyber threats and contributes to a more strategic, efficient, and comprehensive approach to managing cybersecurity risks. The lifecycle is a continuous process that assists organisations in improving their comprehension of the threat landscape and adjusting their defences accordingly. By concentrating on pertinent threats, the lifecycle reduces the impact of attacks, enabling organisations to respond more effectively and maintain a robust cybersecurity posture.

The cycle typically consists of these stages:

1. **Direction/Discovery:** Aims to identify or discover customer's intelligence requirements.
2. **Collection:** Data and information are collected from various sources to meet the identified requirements.
3. **Processing:** Data is processed to remove duplicates, inconsistencies, and irrelevant information, transformed into a format suitable for analysis, and enhanced with additional context and metadata.
4. **Analysis:** Raw data and information are collated with other sources and turned into intelligence with various machine-based and human techniques.
5. **Dissemination/Action:** The timely distribution of completed and relevant intelligence products to the intended customers.
6. **Feedback**: Ongoing assessment of the effectiveness of each step of the intelligence cycle.

In addition to threat intelligence levels and intelligence cycle, threat intelligence frameworks can arm organizations with the structured approach and knowledge needed to anticipate and counter cybersecurity threats. This information helps cybersecurity experts make decisions, act more swiftly, and safeguard digital assets from the damaging impacts of cybersecurity attacks. Common threat intelligence frameworks include:

Kill Chain

Provides a step-by-step approach to identify and counteract malicious activity. It breaks down cybersecurity attacks into stages, intending to disrupt one stage at a time. Use Case: Cyber Defenders can identify potential security measures and map their cyber defences to each stage of an attack.

Diamond Model

Focuses on understanding adversary infrastructure, capabilities, and victimology. Use Case: Security Operations teams can correlate threat actor behaviours to proactively block malicious infrastructure.

MITRE ATT&CK

Provides a knowledge base of adversary Tactics, Techniques and Procedures and helps develop detection rules aligned with adversary behaviours. Use Case: Cyber analysts can enrich alerts by mapping events to MITRE ATT&CK techniques, improving detection accuracy.

Cybersecurity Trend 2 - Adoption of Intelligence-Driven Cyber Threat Modelling capability

Why Use It?

Intelligence-driven Cyber Threat Modelling capability can assist with tracking everchanging cyber threat landscape and its relevance to an organisation or a government. The following principle can be used as a foundation to build the capability:

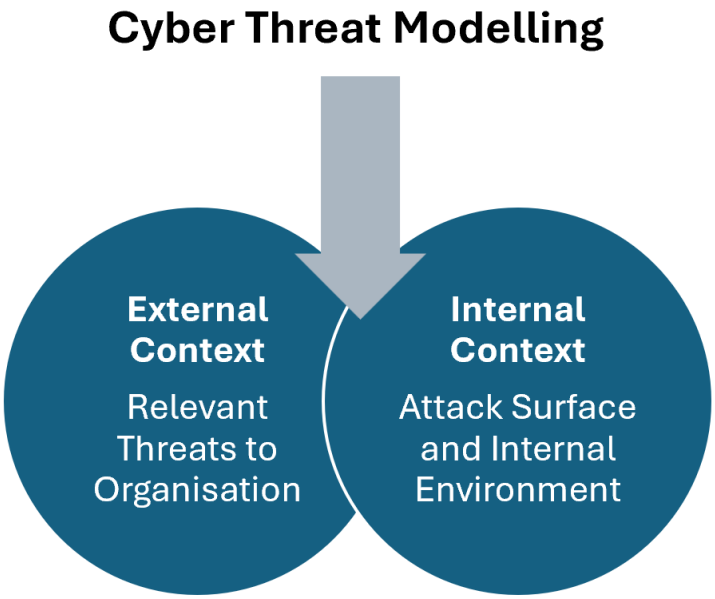
"Intelligence-driven Cyber Threat Modelling allows an entity to keep up with new developments in cyber adversarial tradecraft, and how it relates to entity's environment, for the purposes of guiding cyber activities towards risk reduction and improvement in entity's security posture."

How to Use It?

One implementation example could be used and could be advised to private and public sector organisations as an approach to adopt this capability:

1. Adopt Mitre ATT&CK Framework as a framework of choice for intelligence-driven threat modelling exercise due to its ability to track updated and detailed tactics, techniques and procedures(TTPs) of adversaries.
2. Adopt Mitre ATT&CK's Attack Navigator tool(https://mitre-attack.github.io/attack-navigator/) as an environment to perform threat modelling exercise as it offers flexible way to track adversarial behaviour and performed combined analysis on multiple threat actors and their tradecraft.
3. Obtain External Context. Analyse cyber threat actors(Nation-State, Cybercriminals, Hacktivists etc.) that could target a given entity based on its industry of operation and geographical region. Layer TTPs of all relevant and identified actors inside Mitre ATT&CK's Attack Navigator tool(https://mitre-attack.github.io/attack-navigator/) and combine them to create a combined set(using Create Layer from Other Layers function)

4. Obtain Internal Context. Analyse entity's attack surface and internal environment and record systems, technologies and platforms that could be exploited and accessed by cyber adversaries. Take TTPs from External Context step and filter only those that are applicable to entity's attack surface and internal environment(based on Platforms option under Layer Controls).



5. Use the result of filtered and combined set of TTPs in your defensive operations. TTPs can be colour coded and prioritised based on their prevalence amongst the number of adversaries.
6. Update model regularly(e.g. every 6 months) to keep up to date with changes to cyber adversaries, their tradecraft and entity's attack surface and internal environment.

Benefits

Intelligence-driven Cyber Threat Modelling can be used to guide and facilitate defensive actions to improve security posture of an organisation. Following benefits can be realised by different cyber teams and areas:

Cyber Threat Intelligence

- Cyber Threat Modelling can assist threat intelligence team to track profile and adversarial tradecraft changes of threat actors relevant to an organisation.
- Cyber Threat Modelling can help to tune adversarial tradecraft of relevant threat actors based on organisation's attack surface and internal environment.

Incident Response

- Cyber Threat Modelling can assist incident responders with understanding stages of cyber-attacks and tactics and techniques used by relevant threat actors to prioritise response actions.
- Cyber Threat Modelling can assist with mapping of incident behaviours and indicators to tactics and techniques used by relevant threat actors.
- Cyber Threat Modelling can assist with guiding scope for tabletop exercises based on relevant threat actors and their tradecraft as it relates to an organisation.

Threat Hunting

- Cyber Threat Modelling helps to form threat hunting hypotheses based on actors relevant to an organisation and a prioritised list of tactics and techniques.
- Cyber Threat Modelling helps to prioritise list of techniques and sub-techniques of actors relevant to an organisation cluster which in turn can uncover TTPs of the adversary that can be used as a base to generate security alerts to enable proactive threat hunting.

Red Teaming

Cyber Threat Modelling can be used by red teams and penetration testers to simulate real-world attacks based on relevant adversarial tradecraft and identify vulnerabilities and weaknesses in an organisation's defences. By following relevant tactics and techniques, testers can better replicate attacker behaviour and provide more realistic and potential testing scenarios for an organisation.

Cyber Security Engineering

Cyber Threat Modelling can be used by security engineering teams to review current security tooling applicability, detection coverage, gaps in defences and map those constructs to relevant tactics and techniques in the model. This will help identify areas where organisation is well protected and any gaps that need to be addressed.

Compliance and Audit

Cyber Threat Modelling can be used by compliance and audit teams to assess organisation's security posture and to demonstrate compliance with industry and regulatory standards. By mapping security controls to relevant tactics and techniques from the model, teams can better demonstrate their ability to detect and prevent attacks that organisation could be potentially facing.

Cybersecurity Training

Cyber Threat Modelling can be used by cybersecurity trainers to educate employees and other targeted stakeholders of the organisation on tactics and techniques used by attackers targeting an organisation. This can help employees better recognise and respond to potential cyber threats.