

Threat Intelligence: A Guide for Senior Leadership (Blueprint)

Cyber Threat Intelligence Briefing Note for Higher Education
Provider Senior Leadership



Enhancing Cyber Security
Across Australia's Higher Education Sector

WHAT IS THREAT INTELLIGENCE?

One of the biggest challenges for higher education providers is to ensure the security and privacy of the individuals' and organisation's data. Cyber attacks have increased in frequency and sophistication, resulting in significant challenges for organisations in defending their data and systems from capable threat actors. This ever-increasing number of cyber attacks warrants higher education providers to deploy dedicated cyber security teams and resources with the expectation to detect, analyse and defend against these cyber threats in almost real-time.

In order to defend themselves, higher education providers need to know who they are up against - who are the adversaries that might attack them and how? What are their goals? And, most importantly, if there is a potential pathway for the attacker to exploit, what will be the impact on the higher education provider?

Cyber Threat Intelligence (CTI) is the security data that has been aggregated, transformed, analysed, interpreted, or enriched with the aid of artificial intelligence, machine learning and advanced mining techniques to provide the necessary context for decision making processes. It assists higher education providers to identify, assess, monitor and respond to cyber threats.

Cyber Threat Intelligence may include information such as technical artefacts to:

- suggest an attack is imminent or currently underway,
- describe the tactics and techniques of an attacker, or
- provide brief alerts, advisories, vulnerability notes and reports, etc.



CYBER THREAT INTELLIGENCE SHARING (CTIS) PLATFORM AND ITS IMPORTANCE

Cyber Threat Intelligence Sharing (CTIS) is the exchange of knowledge about cyber threats, incidents, vulnerabilities, mitigations, leading practices, or technologies concerning the technology-based/technology-leveraged risk set.

The Australian Cyber Security Centre (ACSC), led by Australian Signals Directorate (ASD), has developed and hosts a [CTIS platform](#) for Australia. The CTIS platform allows ACSC Partners, such as the higher education sector, to exchange CTI, enabling partner organisations to leverage the collective knowledge, experience and capabilities of the higher education sector.

The long-term goal of the CTIS program is to create an Australian CTIS community of practice comprised of many Australian industries including the higher education sector, and Government partners, each sharing intelligence with a central Government system for the benefit of Australia.

COMMON APPROACHES TO THREAT INTELLIGENCE

Some common approaches to Threat Intelligence include:

MITRE ATT&CK Framework

The [MITRE ATT&CK Framework](#) is a publicly available curated knowledge repository on cyber adversary tactics, techniques and procedures. It is a vast resource of cyber security information, intended to be used as a tool to strengthen an organisation's security posture. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in Government, and in the cyber security product and service community.

Threat Modelling

Threat Modelling can be defined as the structured process or the series of tasks by which the security professionals can identify different threats and vulnerabilities, assess their severity, and take immediate remediation steps to mitigate the risks associated with those threats. There are a number of threat modelling frameworks available to mitigate such risks posed by the threats, namely:

STRIDE

[STRIDE](#) is a model for identifying computer security threats. It provides a framework for evaluating security threats in six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of privilege.

OWASP

The [OWASP Top 10 Web Application Security Risks](#) identifies the most critical security risks to web applications to assist organisations to take steps toward ensuring more secure software development. The top 10 risks are:

- Broken access control
- Cryptographic failures
- Injection
- Insecure design
- Security misconfiguration
- Vulnerable and outdated components
- Identification and authentication failures
- Software and data integrity failures
- Security logging and monitoring failures
- Server-side request forgery



Sources

This blueprint has been developed using [OWASP](#), [MITRE ATT&CK](#), and [CTIS background](#) resources.