

# 2019 PROSPECTUS



**AUSCERT**



**AusCERT  
Information Sharing  
& Analysis Centre  
(AusISAC)**

## THE STORY SO FAR ...

# AUSISAC

## OVERVIEW

Over the past couple of years, AusCERT has coordinated and run a highly-successful information sharing group for the tertiary education sector, and we are pleased to announce the establishment of an AusCERT Information Sharing and Analysis Center (AusISAC); now available to general members. Members who join will be given access to our MISP platform, where we share a curated feed of threat intelligence gathered from multiple sources, and our own malware and threat analysis.

---

# PREVENT

## The first step in defense is prevention.

Our MISP platform delivers vetted threat indicators sourced from members, AusCERT's internal analysis of captured malware and spam samples and trusted third parties.

These indicators can help minimise the risk of malicious traffic successfully penetrating your network.

You can achieve this by feeding the indicators to different layers of defensive security controls within your environment, such as SIEMs, firewalls, IDS/IPS, network and server ACLs, Web proxies and mail filters.

Threat indicator ingestion can be a manual process or automated.

## Simply choose your path.

MISP exports threat indicators in a variety of formats, with continuous integration work being undertaken by CIRCL, the developers of MISP. Some supported export formats: STIX, CSV, Snort/Suricata rules, BRO.

# DETECT

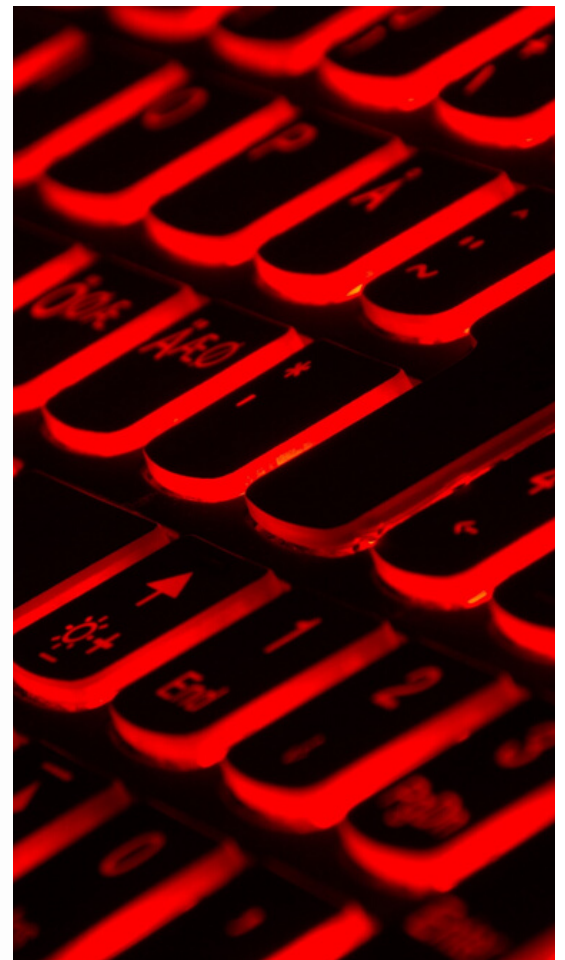
## When preventive controls fail, a primary infection or intrusion will occur.

Often times, this is followed by an attempt to propagate within the environment by targeting vulnerable systems. Malware such as Trojan downloaders also attempt to perform secondary infections on systems by fetching malware such as ransomware and backdoors from remote servers.

**Threat indicators** like domains, destination IPs, URLs of malware serving sites, when applied to your network security controls can help Identify infected hosts within your network (beaconing to C&C)

**Prevent secondary malware** from being installed, thereby reducing impact

**Detect and block malicious traffic** such as vulnerability scanner, exploits from traversing the local network by detecting patterns in traffic and host-based IDS.



---

# IDENTIFY

If a system has been compromised and you want to establish the methodology through which the compromise occurred, a forensic investigation would be initiated.



While it's possible to postulate potential infection vectors, sometimes it helps to have indicators of compromise around suspected vectors to correlate against your logs and artefacts.

**Host-based indicators such as:**

Hashes, YARA signatures and file paths to identify artefacts dropped by a malware  
Registry keys to identify Persistence mechanisms employed by a malware.

**Network based indicators such as:**

URLs, IPs, domains could help identify Command and Control servers, drop zones for exfiltrated data, malware serving hosts.

MISP's built-in correlation feature also enables human operators to sight similarities to past campaigns, such as known threat actors, exploited vulnerabilities.

PRICING: \$10,000 EXT GST PER ANNUM  
CONTACT US TO BE A PART OF THIS INITIATIVE  
[MEMBERSHIP@AUSCERT.ORG.AU](mailto:MEMBERSHIP@AUSCERT.ORG.AU)