Threat Intelligence Standard

Introduction
A Threat Intelligence Platform (TIP) is essential to ensure consistency, interoperability, and effectiveness in cybersecurity.

Purpose
Organizations use Threat Intelligence Platforms (TIPs) to enhance their cybersecurity posture by providing valuable insights into potential threats and enabling proactive responses to mitigate them.

Overall, a threat intelligence platform plays a crucial role in enhancing an organization's cybersecurity strategy by providing actionable insights, facilitating threat detection and response, and helping to stay ahead of emerging threats and vulnerabilities.

Definitions
- Threat intelligence – Threat intelligence is information that organizations use to understand potential cybersecurity threats and vulnerabilities to protect their digital assets, systems, and networks. It involves collecting, analyzing, and disseminating data and insights related to cybersecurity threats, including information about malicious actors, tactics, techniques, and procedures (TTPs), and emerging vulnerabilities.
- Threat Intelligence Platform (TIP) – A comprehensive solution designed to collect, analyze, manage, and disseminate cybersecurity threats and vulnerabilities information.
- Tactics, Techniques, and procedures (TTP) – The behavior of an actor.
- Indicators of compromise (IOC) – Are described as digital breadcrumbs that are forensic evidence of potential intrusions on a host system or network.
- Information sharing and analysis centers (ISAC) – Non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure), allowing two-way sharing of information between the private and the public sector about root causes, incidents and threats, as well as sharing experience, knowledge and analysis.

Standard
OMES Cyber Command uses a threat intelligence platform to proactively collect, aggregate, analyze, and disseminate threat intelligence data to defend against cyber and physical threats. TTPs, IOCs, and any actionable data must be correlated and prioritized. TIP must be integrated with SIEM systems, firewalls, intrusion detection systems, end-point detection response systems, web filtering systems, and email threat gateway.

- Data collection – Threat intelligence data will be collected from various sources, such as open-source information ISACs, proprietary feeds, internal logs, and information sharing with other organizations, government agencies, and cybersecurity communities.
- Analysis – Threat intelligence analysts examine the collected data to identify patterns, trends, and potential threats. They assess the credibility and relevance of the information to determine its significance.

- Contextualization – Threat intelligence is often contextualized to help organizations understand how specific threats might impact their systems and operations. This contextualization can include information on the potential impact and recommended actions.
- Classification – Threat intelligence is categorized into different types, such as strategic, operational, and tactical intelligence. These categories help organizations prioritize and respond to threats effectively.
- Dissemination – Once analyzed and classified, threat intelligence is shared with relevant stakeholders within the organization. It can also be shared with external partners and government agencies to enhance collective cybersecurity efforts.
- Actionable insights – The primary goal of threat intelligence is to provide actionable insights that help organizations improve their cybersecurity posture. This may involve updating security policies, implementing new security controls, or patching vulnerabilities.
- Threat indicators – Threat intelligence often includes specific indicators of compromise (IOCs), which are pieces of information that may indicate a security incident, such as malicious IP addresses, file hashes, or attack patterns.

Compliance
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale
To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References
- Confidential Technology Standard

Revision history
This standard is subject to periodic review to ensure relevancy.

Effective date: 12/19/2023	**Review cycle:** Annual
Last revised: 12/19/2023	**Last reviewed:** 09/06/2024
Approved by: Joe McIntosh, Chief Information Officer	