The Active Cyber Defense Cycle is a model to consume threat intelligence. It focuses on bridging various security teams to take a security operations focus on identifying and countering threats. It can start at any phase of the cycle, with the phases continually feeding into one another in order to create an ongoing process.

**Network Security Monitoring** focuses on hunting threats in the environment and is comprised of three phases: collect, detect, and analyze. In the collect phase analysts should gather data from the environment such as network traffic, system logs, and security device logs. In the detect phase analysts should look for abnormalities and use adversary IOCs and TTPs to hunt for adversaries. The analyze phase helps to confirm that the threats are real and not a false positive. This helps reduce incident response false positives.

**Incident Response** should focus on scoping the impact of the threat and any malicious activity while containing and eradicating the threat. IOCs should be used to understand and fix the true scope of the problem to avoid reinfections.

There are three levels of threat intelligence: strategic, operational, and tactical. The levels should be used as a reference guide to remember that different audiences have different requirements of threat intelligence.

**Strategic-level** players such as executives and policymakers should look for an understanding of the wider threat landscape to identify the risk to the organization and changes that can be made in investments or the corporate culture.

**Operational-level** personnel should look to translate strategic objectives into tactical efforts and vice versa by identifying the overarching goals or trends of an operation or campaign. They should also aim to be aware of adversary campaigns instead of single intrusions, identify organizational knowledge gaps, and share information with peer organizations to alleviate those knowledge gaps.

**Tactical-level** intelligence is often consumed in the form of indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs). This helps drive the security of an organization and enable it to hunt down threats and better respond to them. Consider using models such as the Active Cyber Defense Cycle.

**Active Cyber Defense Cycle**

The Active Cyber Defense Cycle is a model to consume threat intelligence. It focuses on bridging various security teams to take a security operations focus on identifying and countering threats. It can start at any phase of the cycle, with the phases continually feeding into one another in order to create an ongoing process.
Organizations that want to generate threat intelligence should have well-established security practices and be able to gather data from successful and attempted intrusions into their organizations. Generating threat intelligence should start with clear requirements and proceed to taking advantage of internal knowledge, such as intrusion data, and external knowledge, such as openly available reports and information. They key is empowering trained analysts to interpret information and produce knowledge about observed threats while detailing technical information that can be used to help enhance security operations and incident response.

The Kill Chain

The Kill Chain highlights steps that adversaries usually perform to complete their objective. It should be used as a reference model to understand adversary activity and observable indicators of compromise (IOCs). Categorizing and identifying indicators and patterns across large numbers of intrusions can reveal connections in intrusion activity including an adversary's campaign.

Determine the Intelligence Requirements

Does the organization need better technical knowledge such as IOCs and adversary tactics, techniques, and procedures (TTPs) to increase incident response and threat detection? Or does the organization need knowledge about adversary campaigns and guidance to executives on the organization's threat landscape? Are these goals specific to certain threats or to safeguard specific data in the organization? Requirements guide what you collect, what and how you analyze it, and the final product dissemination.

Analyze Internal Information

Have incident responders, enterprise security teams, malware analysts, and other members of your organization provided data and information on previous intrusions into the organization? Analyze the intrusions against models such as the Diamond Model or Kill Chain to extract indicators and to identify adversary patterns. Organizations should have a minimum of 60 days of logs to generate useful data. Lastly, remember that the best data is internal to your organization.

Enrich the Information

Utilize open-source information with tools such as Google, ThreatMiner.org, or professional tools to determine if others have seen the technical indicators or adversary TTPs before. Attempt to avoid duplicating efforts – use existing information.

Validate the Information

Open-source information exists in abundance and it needs validating. Not all information is correct or relevant to your organization. Simply taking a threat feed or data source and using it blindly will generate false positives and overload analysts. Have processes for refining indicators and information that is no longer useful. The analysts’ approach to indicators will always fall over time.

Store the Information

Store the information using a common format and ensure that analysts can also add notes or analyze relationships between technical indicators. Make sure internal security personnel can quickly access and utilize the information. Additionally, seek feedback from the consumers to help improve the intelligence processes while confirming that the feedback is useful.

A Sample Process from SANS FOR578*

What is a TTP?

An adversary tactic, technique, or procedure (TTP) is the means by which adversaries accomplish their goals. TTPs often consist of a pattern or sequence of adversary activity that those adversaries routinely perform. As an example, if an adversary consistently gains access to unauthorized VPNs in an environment and then leverages PowerShell within the environment to steal intellectual property documents, that pattern could be observed as one of their TTPs. In the future, if you identify that adversary is using PowerShell in your environment, you may want to quickly safeguard intellectual property documents while identifying and removing unauthorized VPNs.

The Diamond Model

The Diamond Model of Intrusion Analysis identifies the four core components of any malicious event: the victim, the capability, the infrastructure, and the adversary. It is a stand-alone model but can also be applied to each phase of the kill chain. Performing this type of analysis allows organizations to start with one component they can identify (such as the victim) and work towards uncovering the other three components. This helps understand adversary motives as well as the infrastructure and capabilities they use.

References and Suggested Reading

Kill Chain:
http://dfir.to/KillChain

Diamond Model:
http://dfir.to/DiamondModel

The Sliding Scale of Cyber Security:
http://dfir.to/SlidingScale

Analysis of Competing Hypotheses (Chapter 8):
http://dfir.to/CompetingHypotheses

Sherman Kent and the Profession of Intelligence Analysis:
http://dfir.to/ShermanKent

SANS Cyber Threat Intelligence Summit Presentations:
http://dfir.to/CTISummitArchive

A Sample Process from SANS FOR578*