The Future of Threat Intelligence

The Current State of Threat Intelligence

The global threat landscape is continuously changing, especially during the global coronavirus pandemic, which has caused a significant shift both in how cybercriminals operate and how they hone their skills. During the pandemic, cybercriminals have been seen advancing their capabilities, adapting quickly, and targeting relevant victim groups more effectively. While cyberattacks continue to get more complex, organizations will need threat intelligence capabilities that are powerful enough to get ahead of their adversaries.

Before we get deep into the topic, let's understand the difference between threat intelligence, threat intelligence management, and threat intelligence platform. While threat intelligence is the data and information about threats, a threat intelligence platform collects, aggregates, and organizes threat intel data from multiple sources and formats, whereas threat intelligence management is the collection, normalization, enrichment, and actioning of data about potential attackers and their intentions, motivations, and capabilities. This information can help organizations make faster, more informed security decisions and thus be better prepared for cyberthreats.

Dealing with millions of indicators daily, security teams are too exhausted to extract real value from their threat intelligence. Without any advanced enrichment capabilities, this data might look like a lot of background noise. There is a lot of manual work, collaboration, and communication required by security teams to make sense of this noise, which is very time-consuming and exhausting. Threat intel teams need to be able to act fast and have a solid, actionable threat intelligence program as they work through their alerts and daily tasks.

Threat intelligence platforms typically promise to reduce the noise from threat feeds, but there is still a ton of manual work that analysts need to do in order to map what is critical to their environment, allow/block the IPs or domains, or even create reports and share the details with their stakeholders. Security teams need to scale the enforcement policies and push the right intelligence across their entire enterprise and dozens of different security tools in a scalable fashion.

Three Topics Driving the Future of Threat Intelligence Platform

During the pandemic, hackers and threat actors have exploited the tens of millions of home-based workers who have provided new access points to malware, cyber viruses, and phishing attacks. The attack surface has never been wider. COVID-19 has created even more opportunities as emergency digital investments broaden the corporate attack surface. The implications of security breaches during the pandemic will continue to remain important for a long time to come.

As more and more businesses reopen, people go back to the office (at least part-time), and organizations launch new products and business models, they extend digital penetration to new applications, devices and business processes—all to better support the flexible working of employees—cyber risks become ever greater, and threat intelligence is even more essential.

The cyberthreat landscape is constantly evolving, and for that reason, an effective threat intelligence system with enormous scope, yet enough modularity to focus on threats relevant to the unique organization, is essential to staying abreast of unknown and unpredictable changes in threat types and characteristics. Threat intelligence can also be used as a key security strategy that allows organizations to be as flexible and dynamic as possible while keeping risks to acceptable levels.

The sections that follow describe the three key topics that we strongly believe will drive the future of threat intelligence.

1. Threat Intelligence Lifecycle

The threat intelligence lifecycle is a continuous process of effectively developing intelligence from raw data that supports organizations to develop defensive mechanisms to prevent emerging risks and threats. While data is gathered from many internal and external source feeds, building an efficient threat intelligence program consists of tools to process and analyze the raw data through automation to validate the information before dissemination.

The future of threat intelligence management lies in taking a holistic approach to the native threat intelligence lifecycle with the ability to collect, unify, process, analyze, enrich, score, validate, and share the most relevant data to stakeholders. The goal is to enable security and IR teams with ac-

tionable intel by providing deeper context around attackers and their motivations. Full security case management is key to documenting their findings in detail, enables them to collaborate in real time with other stakeholders, and provides preventive and quarantine measures across the enterprise.

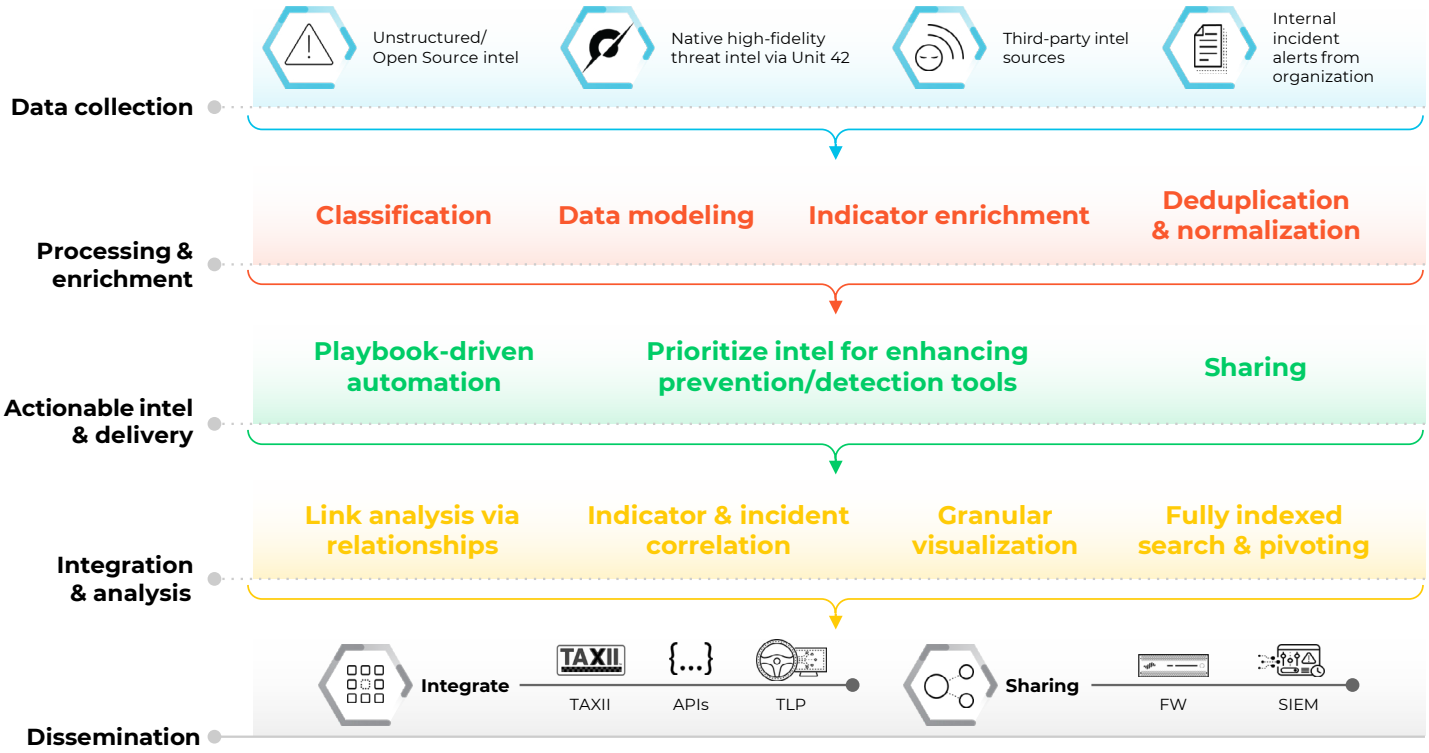

Figure 1: The lifecycle of threat intelligence platform

2. Strategic Threat Intelligence

Strategic threat intelligence is a bird's-eye view of an organization's threat landscape and has tremendous value for business decision-making. While typical security and analysis skills are still essential, producing strategic threat intelligence also requires a great deal of expertise in other areas and a strong understanding of business concepts.

When you analyze the SolarWinds attack that happened in December 2020, you will realize that this is not the first incident of this type to occur—multiple types of centralized administrative software have been compromised in the past.

The increase of managed service providers into critical businesses has boosted the severity of the situation and will continue to be compromised in the future. Administrators should consider their critical data dependencies, business functions, and business relationships with these third-party firms, as their past history of central failure and data compromise will likely continue in the future and might directly impact an organization if an incident were to occur. To ensure organizational security and protection from a similar SolarWinds-type event, organizations need the application of vulnerability awareness and the deployment of a reputable threat intelligence platform. Organizations should be able to utilize actionable and strategic threat intelligence to face potential vulnerabilities that will effectively help prevent, or at least minimize, the impacts from future SolarWinds-type events.

With strong strategic intelligence in place, organizations can easily explain and summarize an incident to senior leadership teams, share the implications of the breach, and what needs to be done in the future to mitigate compromise. For example, a series of reports detailing threat actors and their

associated attack techniques known to target an industry could be created and shared easily.

This type of intelligence provides high-level information about cybersecurity posture, threats, and attack trends. This information mostly deals with the big picture in the threat landscape and helps executives and management, such as IT managers and CISO teams, understand the financial impact of various cyber activities and the overall impact of high-level business decisions.

3. Automation

Why is security automation the future of cybersecurity? Let's accept it—automation saves time and money and improves productivity.

We've already discussed how the cyberthreat landscape is constantly evolving and getting dangerous. We saw last year how ransomware adversaries had been rapidly adopting data extortion methods. While security teams are caught up in processing, analyzing, and distributing the threat data that requires a substantial number of repetitive tasks, hackers are changing their tactics far faster and more easily than we can update our defenses. Such repetitive tasks are ideal for automation.

Automate actions to immediately shut down threats across your enterprise. You can expand the scope of your investigations by easily sharing threat intelligence across internal teams and trusted organizations.

The Value of Threat Intelligence Programs

Robust and actionable threat intelligence enables security analysts, threat researchers, and others to gain the upper hand in dealing with cybercriminals. Figure 2 below depicts three key-value statements for SOCs and threat analysts with threat intelligence management.

Figure 2: Business value from threat intelligence platform

Get Ahead of Your Adversaries with Cortex XSOAR Threat Intelligence Management

Cortex XSOAR Threat Intelligence Management (TIM) is the next level threat intelligence platform that provides unmatched visibility into the global threat landscape and native access to the massive Palo Alto Networks threat intelligence repository (more than 55 million malware samples collected, 72 million firewall sessions analyzed daily, plus strategic intelligence from Unit 42) and integrations with hundreds of other threat intelligence sources, Cortex® XSOAR Threat Intelligence Management promises a powerful threat intelligence tool to empower your security teams.

Cortex XSOAR TIM is the first threat intel platform on the market to address the full threat intel management lifecycle. Built on the extensible Cortex XSOAR platform, TIM defines a new approach to threat intelligence management by collecting, normalizing, and deduping threat intelligence from various sources, with a centralized threat intelligence library from our own Unit 42. Unlock the power of threat intelligence to enrich, prioritize, operationalize, and easily take action.

Centralized Threat Intel Library

A central threat intelligence library for your enterprise with unmatched visibility into the global threat landscape is yours, with native access to the massive Palo Alto Networks threat intelligence

repository (more than 55 million malware samples collected, 72 million firewall sessions analyzed daily, plus strategic intelligence from Unit 42) and integrations with hundreds of other threat intelligence sources.

Manage the Full Intelligence Lifecycle

A full set of features sporting both tactical and strategic threat intelligence, XSOAR TIM can prioritize the right intelligence and score it transparently, all the automation capabilities to operationalize threat intelligence and share those use cases. It's an end-to-end platform that covers all your threat intelligence needs.

Automate and operationalize

Automatically map threat information to incidents. Your incident data is the most relevant source of threat intelligence available to your organization. We automatically map and enrich incidents with external threat data to help you identify relevant threats as well as surface connections between threat actors and attack techniques previously unknown in your environment.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com