USE CASE

ANOMALI

Threat Intelligence is a core component of a Zero Trust Architecture (ZTA)

Threat intelligence is a core component of a Zero Trust Architecture (ZTA). ZTA is a security concept and framework that assumes that all network traffic is to be untrusted and requires strong authentication and authorization. Threat intelligence can then be used to support the development and implementation of zero-trust policies and controls.

Threat intelligence can help an organization identify and better assess potential threats and risks to systems and networks. Threat intelligence can be used to identify previously known threat actors and the tactics, techniques, and procedures (TTPs) they use. Threat intelligence can also identify emerging threats that may not be previously identified. This valuable information can be used to further enhance security controls to better monitor for related suspicious activity within the network.

The NIST SP 800-207 guideline, focusing on the Zero Trust Architecture Framework, highlights the vital significance of threat intelligence within this architecture. In accordance with NIST SP 800-207, threat intelligence stands as an integral element of the Zero Trust framework.

A straightforward illustration would involve an organization leveraging threat intelligence to pinpoint a threat actor and the malicious malware tools they employ. This allows the existing security measures to incorporate this threat intelligence, enabling them to identify and successfully block the malware from infiltrating the network.

Additionally, threat intelligence serves as an educational resource for training employees on the identification and optimal response to potential threats. Within a Zero Trust network environment, all network traffic is viewed as untrusted, necessitating employees to remain vigilant for any signs of suspicious activity. Zero Trust aids organizations in recognizing and preempting threats at an earlier stage, thereby influencing the development and deployment of more robust security controls.

In accordance with NIST SP 800-207, titled “Zero Trust Architecture,” threat intelligence plays a crucial role in helping organizations gain insights into potential threats and informing the implementation of effective security controls. The guideline underscores that “threat intelligence can be employed to identify known malicious actors and their Tactics, Techniques, and Procedures (TTPs), as well as previously undisclosed emerging threats.”

In Figure 1 of NIST SP 800-207, you can observe that threat intelligence is prominently featured as a fundamental logical component within the Zero Trust framework.

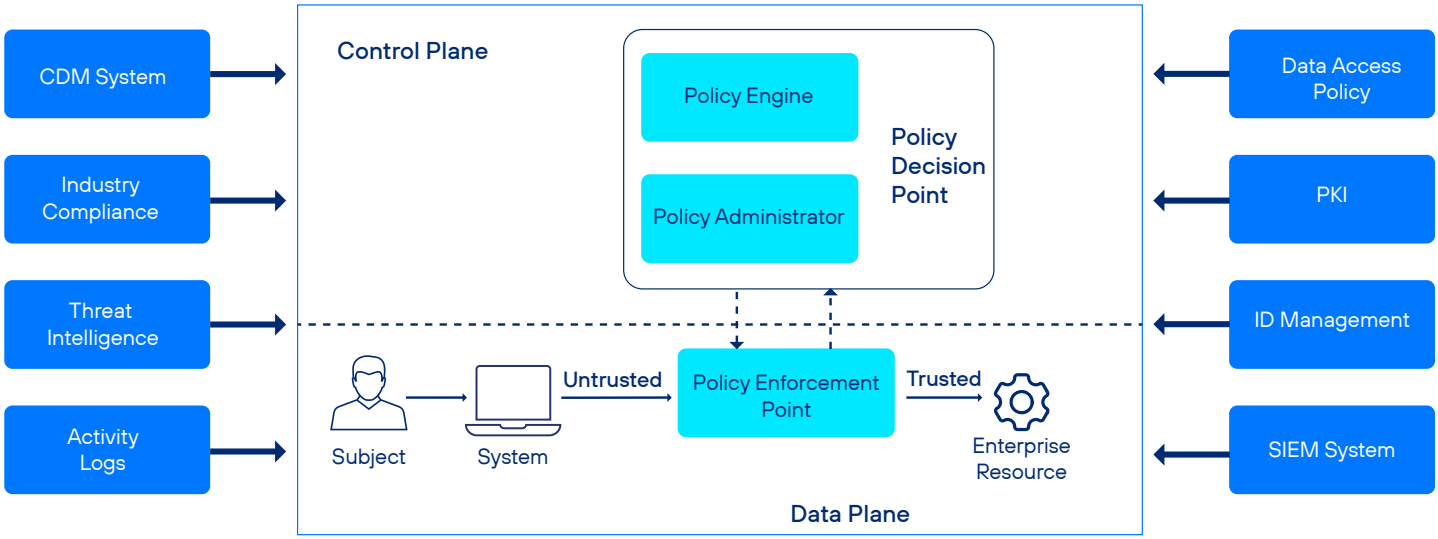

Figure 1: Core Trust Logical Components

Anomali's threat intelligence plays a pivotal role in bolstering the implementation of a zero-trust architecture within organizations. It achieves this by furnishing real-time insights into potential threats lurking in its systems and networks. This is made possible through the use of threat feeds, which constantly provide updated information on known malicious actors and their tactics, techniques, and procedures (TTPs). Armed with this wealth of threat feed data, organizations can craft and put in place security controls that effectively identify and thwart potential threats from infiltrating their network.

Anomali ThreatStream brings together external threat intelligence feeds and internal threat intelligence, data, or research, to enable analysis and investigations of threats in a single interface and to integrate the threat intelligence with the organization's security systems (SIEMs, EDR, FWs, etc.) to enable the efficient mitigation of threats.

Importantly, this then enables security operations to work with stakeholders to prioritize and remediate threats according to their impact on the business services. Similarly, it enables threat intelligence and incident response functions to prioritize their research/investigative efforts according to the same information, in a more coordinated and informed approach across all security teams and stakeholders focused on threats to the organization.

In this manner, ThreatStream provides a technical realization of one of the key objectives of establishing a CTI function: Understanding and mitigating business risk from cyber threats using an automated and integrated Threat Intelligence Platform.

The MITRE ATT&CK framework and other threat intelligence models are in-built to an advanced Investigations Workbench, for users to leverage, research, and produce finished intelligence reports for further action.

Anomali Lens is the first natural language processing (NLP) based web content parser that highlights all cyber threat information for further investigation, thereby supercharging Threat Research and Reporting.

Attackers inevitably set the agenda for cybersecurity analysts. Yet CISOs want answers and actions from those same analysts—and they want them now. Analysts are constantly racing against the clock to understand attacks and how to prevent threats from harming their networks.

Anomali Lens enables analysts to work and stay in any single web-content location for faster research and to communicate cyber risk better to the executive leadership. This is especially critical in high-pressure environments such as widespread cyber-attacks and high-profile data breaches.

Anomali Lens scans and converts unstructured data, such as news stories, social media, research papers, blogs, paste sites, coding repositories, and internal content sources like SIEM user interfaces, into actionable intelligence. Anomali Lens leverages natural language programming (NLP) that takes unstructured data and identifies threat actors, malware families, and attack techniques as they relate to threat intelligence.

To explore further details on the Anomali Threat Intelligence Platform as well as Lens+ please visit https://www.anomali.com/products/threatstream and https://www.anomali.com/products/lens.

ANOMALI