IPS Industrial Signatures: Protecting Industrial Control System

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

**IPS Industrial Signatures: Protecting Industrial Control System**

Summary the design goals, technology & engineering, and explains how IPS Industrial Signatures are deployed in industrial control systems networks

1. **Goal:**

There are multiple principles of network IPS (intrusion prevention system), but the main goal is to ensure that level of security is maintained after the sensor is integrated into the network (2).

1. **Technology and Engineering:**

The Cisco IPS signatures are a set of rules used by the Cisco IPS sensors to detect know attacks (for example denial of service (DoS) attacks…). The sensors analyze packets and, if malicious, a signature is triggered based on the way the IPS sensor has been configured to react against the attacks.

According to (2), Cisco IPS sensor signatures are generally classified into three types:

* Default Signatures are signatures created for known attacks.
* Tuned Signatures are signatures created by modifying built-in signatures to suit particular needs
* Custom Signatures are created based on certain criteria, which the administrator decides on.

Each of these types has the same properties: Signature Name, Signature ID, Signature Status, Severity Engine, Severity Ratings, Fidelity Rating, Triggering Conditions, Summarization Strategy, and Response Actions.

Each of these properties can be modified and set up based on the policy of each organization. Each property will handle a different security setting to make sure security is enforced based on a predefined policy. For example, a signature engine is a component of the analysis engine of the sensor that inspects a particular aspect of network traffic and supports a category of signatures. Each Cisco IPS signature is created and controlled by a signature engine that is specifically designed for the type of traffic being monitored. For example, the STRING.TCP engine examines TCP connections searching for string patterns.

IPS Industrial Signatures are deployed or operated in industrial control systems networks by determining the criteria that trigger an action by matching network traffic. The sensor will operate primarily as an IDS, IPS, or a mixture of both. The Cisco IPS Sensor allows network admins to have various detective or preventive actions based on the signature. While some of these actions will work only in inline mode, others will work only with specific network protocols (2)

References

Chapple, M., & Seidl, D. (2023). Chapter 11: Defending Endpoints In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 103–124). essay, Jones & Bartlett Learning. (1)

Davidbu (2019) Cisco IPS Signatures 101. Retrieved from [Chalk Talk - Cisco IPS Signatures 101 - Properties, Engines, Alerts, & Actions - Cisco Community](https://community.cisco.com/t5/security-knowledge-base/chalk-talk-cisco-ips-signatures-101-properties-engines-alerts/ta-p/3124168#:~:text=IPS%20Signatures%20are%20a%20set%20of%20rules%20used,sensor%20has%20been%20configured%20to%20react%20to%20such.) (2)