Intrusion detection and prevention data (IDS and IPS)

IDS and IPS are complementary, parallel security systems that supplement firewalls – IDS by exposing successful network and server attacks that penetrate a firewall, and IPS by providing more advanced defenses against sophisticated attacks.

IDS is typically placed at the network edge, just inside a perimeter firewall, although some organizations also put a system outside the firewall to provide greater intelligence about all attacks. Likewise, IPS is typically placed at the network perimeter, although it also may be used in layers at other points inside the network or on individual servers. IPS usually works by dropping packets, resetting network connections and blacklisting specific IP addresses or ranges.

In the Common Information Model, intrusion detection and prevention data is typically mapped to the Intrusion Detection data model.

Visibility

IDS logs provide security teams detailed records of attacks including the type, source, destination and port(s) used that provide an overall attack signature. IPS logs provide the same set of attack signature data, but also may include a threat analysis of bad network packets and detection of lateral movement. This data can also detect command and control traffic, DDoS traffic, and malicious or unknown domain traffic.

Application

When your Splunk deployment is ingesting intrusion detection and prevention data, you can use it to accomplish security and compliance use cases.

- Investigating a ransomware attack
- Detecting AWS security hub alerts
- Monitoring NIST SP 800-53 rev5 control families

Sources

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). In addition, these Splunk Add-Ons and Apps are helpful for working with intrusion detection and prevention data.

- Splunk Add-on for Juniper
- Splunk Add-on for Cisco FireSIGHT
- Splunk Add-on for OSSEC
- Splunk TA for Suricata