USE CASE

Government Agency Implements Secure Splunk Data Aggregation

SOLUTION REQUIREMENTS:

1. Secure the Splunk data store from external cyber threats
2. Transfer multiple data types simultaneously
3. Enable data inspection and filtering from untrusted to trusted environment
4. Provide failover, high-availability, and load-balancing capabilities
5. Include scalable architecture for additional volume or data types as needed

Company Overview

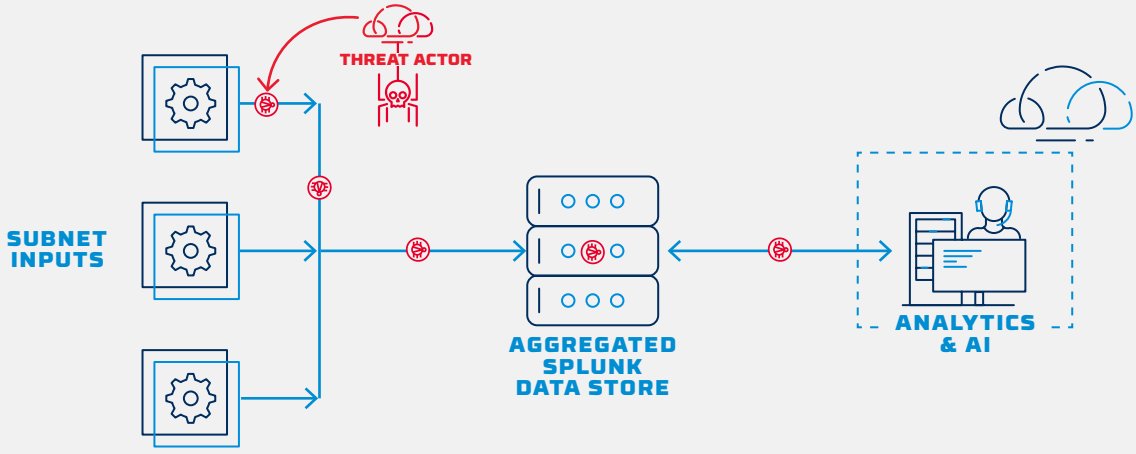
A major government agency with large, sensitive data stores.

Cybersecurity Challenge

A major government agency needed to efficiently analyze their security alerts to fully observe possible threats, their extent, and to rapidly prioritize them. In order to do this, they planned to aggregate their many subnet inputs into one master Splunk data store where they can apply analytics, machine learning, heuristics, and artificial intelligence.

However, the agency also recognized that the more they aggregated, the higher the sensitivity of the data store, thus they needed to upgrade the Splunk data store to a very secure posture. This meant both isolating the data store from possible threats, and implementing a highly-controlled mechanism for data aggregation.

USE CASE (BEFORE)

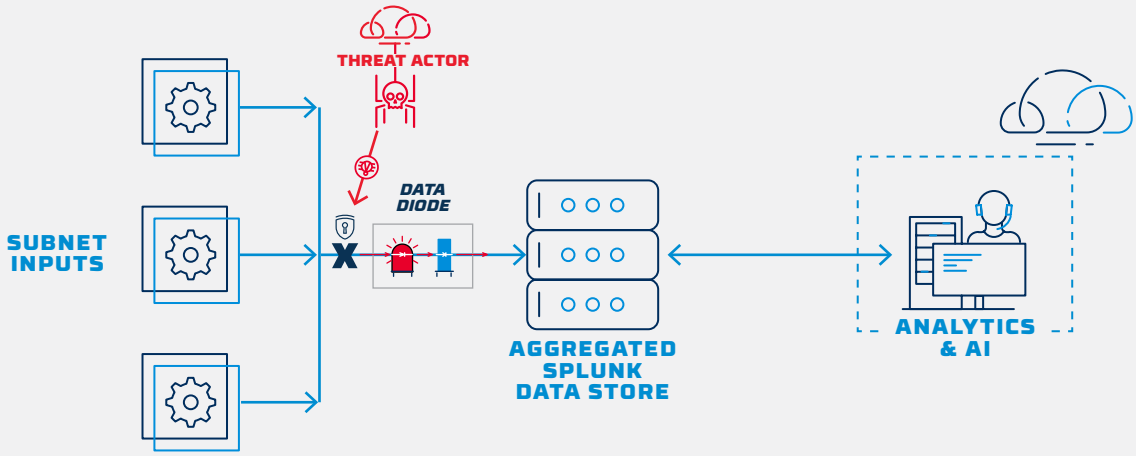


Implementation

Due to their highly reliable and secure hardware-enforced nature, Owl cross domain solutions (OCDS) were identified as an ideal protection and data transfer mechanism for the Splunk data store. Designed to transfer data only one-way and with built-in filtering and data verification, OCDS products integrate seamlessly with the Splunk data store, enabling many-to-one data ingestion capability, with optional high availability configurations.

The OCDS optical separation provides an unhackable means to prevent any network-based probing or unauthorized entry into the data store. With industry-leading bandwidth and the capability to operate with multiple devices in tandem, the agency can support a multitude of data streams into storage.

USE CASE (AFTER)



Results

1. Provided effective and network segmentation between subnet inputs and the Splunk data store
2. Enabled high-availability, one-way, deterministic data flows into the Splunk data store
3. Mitigated external threats to the data store through the ingestion data paths
4. Facilitated analytical insights into security events and alerts

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com