OSISOFT, LLC. & DRAGOS, INC.

Detecting Threats Using Broad ICS Datasets

HIGHLIGHTS

- Dragos Platform's integration with OSIsoft PI System provides broader analysis of network and operational data in the pursuit of detecting threats.
- Event Frames received from PI System are analyzed and correlated against network activity using Threat Behavior Analytics
- As threats are detected within Dragos Platform, threat notifications can then be pushed back to PI System for data recording
- Investigation playbooks further guide analysts through the appropriate response referencing available data from network, host and PI events.

THE CHALLENGE

One of the biggest challenges facing Industrial Control Systems (ICS) is that ICS networks are relatively unsupervised with little ICS specific security monitoring. This lack of monitoring combined with an unknown threat landscape can make defending control systems difficult. Having greater visibility of events at the network & host level correlated with events at the operational level can enable defenders to have the coverage required for robust threat detection and response capabilities.

SOLUTION OVERVIEW

OSIsoft's PI System is a system of record for operational data allowing customers to track processes and events to ensure processes run efficiently and safely. Existing deployments of PI System could be driven by compliance, process optimizations, troubleshooting or predictive analysis. Given that OSIsoft's PI System is commonly deployed across many industrial vertical markets including Energy, Petrochemical, and Manufacturing, it's a wealth of available data.

Dragos Platform's integration with PI System further extends the application of PI System data already available in an environment to also benefit ICS defenders. Dragos Platform utilizes PI System data in addition to its broad collection of industrial network and host data to provide the most complete coverage for ICS threat detection and response in the industry today. Threat detection in the Dragos Platform is primarily performed through Threat Behavior Analytics. These threat analytics running within the platform can correlate malicious activity and operational events to identify the threat behavior and potential impact to operations.

PI System collects data from a wide variety of sources including non-Ethernet based sensors. This level of data was previously unavailable to network security monitoring platforms without adding additional layers of complexity (e.g. media converters). Analyzing data from all sources available is integral to complete threat detection across the control system architecture.

TECHNOLOGY

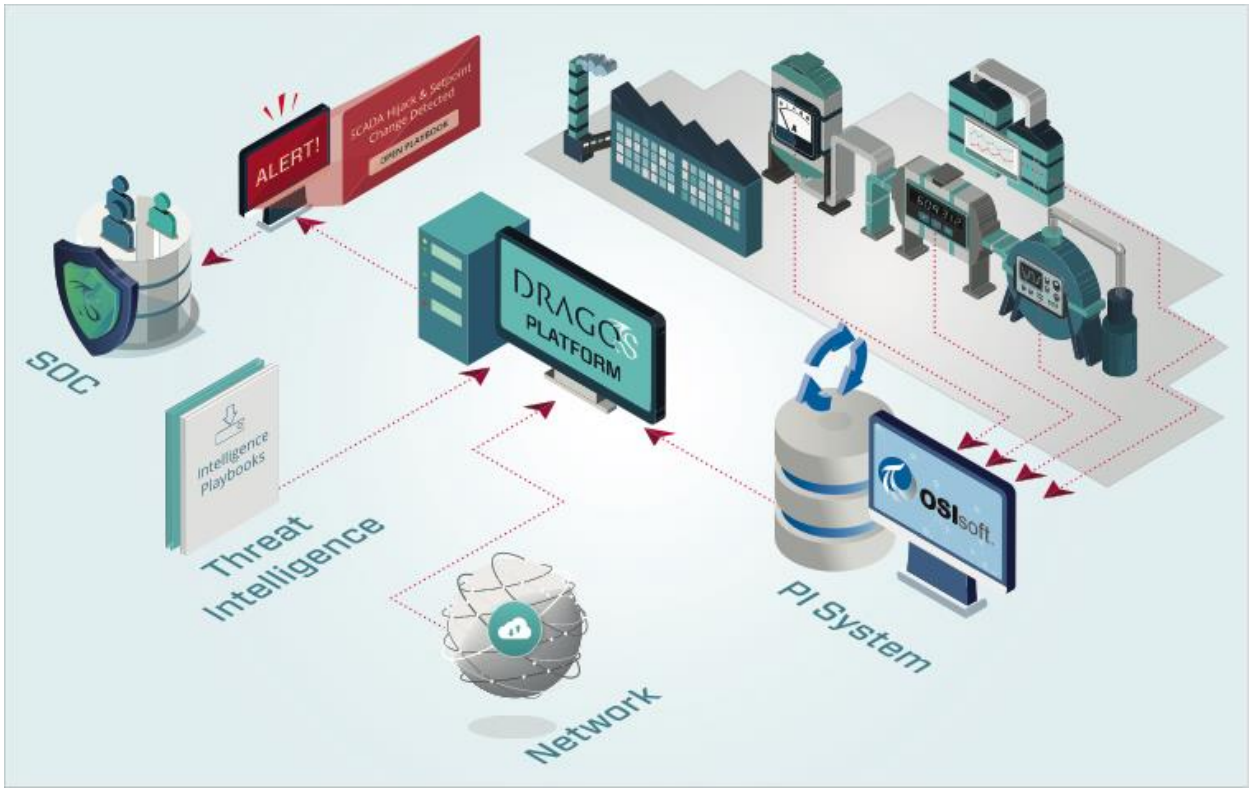
Dragos Platform consists of network appliance Midpoint Sensors and a centralized server known as the SiteStore. Dragos Platform offers deployment flexibility allowing for the PI Server to connect to either the Midpoint Sensor or SiteStore depending on environment considerations. Once integrated, Event Frames can then be exchanged in either direction between PI System and the Dragos Platform.

As Event Frames (such as setpoint or alarm limit changes) are received in the Dragos Platform, Threat Behavior Analytics correlate the event with other network and host activity to alert operators of known malicious activity. These threat analytics are created by Threat Intelligence analysts at Dragos on new and emerging industrial threats and provided on a regular basis to Dragos Platform customers as a downloadable content pack. Each threat analytic is also paired with an investigation playbook made by Dragos' incident responders and threat operations analysts so that customers have a step-by-step guide to investigating detections for highly effective and efficient investigations and responses. The PI System and Dragos Platform integration also enable the development of new specific investigation playbooks.

The Dragos Platform can be used for situational awareness and continuous monitoring, threat hunting, and incident response applications:

- Robust search functions with pre-made correlations and content provide analysts with the ability to examine various datasets such as network and process events, in the ICS in an ad-hoc fashion such as required for threat hunting.
- Threat Behavior Analytics automatically provide notifications when known malicious behavior has been detected in the ICS with appropriate context as to what the behavior means and what should be done.
- Investigation Playbooks guide analysts on the appropriate response leveraging both the network, host and PI System data available helping to scale industrial specific security knowledge across teams of diverse backgrounds.

ARCHITECTURE



FEATURES & BENEFITS

Features	Benefits
Enhanced Asset Discovery	Data from PI System provides additional asset detail to help characterize assets including non-ethernet devices.
Correlated Threat Discovery With Operational Events	Dragos Platform's Threat Behavior Analytics correlate known threat behavior with associated operational data and Event Frames from PI System to help analysts understand the full impact of the threat and reduce mean time to recovery (MTTR).
Expanded Search Capabilities Through Vast Datasets	Dragos Platform's Query Focused Datasets (QFD's) allow for retroactive searches through both network, host and operational data to assist in threat hunting and incident response activities
Investigation Playbooks Incorporate Guidance Using PI System Data When Relevant	Associated playbooks guide defenders on how to use the Platform's PI System data to appropriately respond to detected threats on the ICS