SEL & DRAGOS, INC.

Protecting Energy Systems from Cyber Threats

HIGHLIGHTS

- Dragos Platform's integration with SEL devices provides ease of visualization and threat detection allowing for improved situational awareness.
- Innovative joint solution which combines SEL's Software Defined Networking (SDN) technology & Dragos Platform to offer greater visibility and allows for more efficient response to detected threats.
- Joint research into emerging threats and the impact to operations will be shared with the community to empower defenders.
- SEL's 3355 hardened industrial computer is selected as Dragos' midpoint sensor for challenging environments.

THE CHALLENGE

Threats targeting energy systems have been on the rise, resulting in the first power outage due to a cyber attack in 2015.

The advances in adversary capabilities were illuminated between 2015 to 2016 with the development of the first grid targeted malware to impact operations known as CRASHOVERRIDE. In 2017 there were numerous nation-state teams targeting energy systems including teams identified by Dragos as having orchestrated hundreds of compromises across North America, Europe, the Middle East, and Asia. Often asset owners have limited awareness of new and emerging threats to industrial control systems (ICS) until its too late. Combined with the limited visibility of ICS networks, defenders face difficulties to quickly detect and respond to emerging threats that pose a risk to operations and safety.

SOLUTION OVERVIEW

The partnership between Schweitzer Engineering Laboratories (SEL) and Dragos enables asset owners to have an increased awareness of the ICS threat landscape allowing for faster detection of threats and more efficient response. As suspicious activity is detected, the Dragos Incident Response Team develops detailed investigation playbooks to guide asset owners through a response process.

Dragos Platform supports increased system resilience through:

BROADER COVERAGE

Passive network monitoring beyond just network traffic including event logs from assets and infrastructure

THREAT BASED DETECTION

Unlike environmental anomaly detection tools, Dragos' Threat Behavior Analytics are derived from real world threat intelligence to detect known adversary behavior and reduce the mean time to detection (MTTD)

INVESTIGATION PLAYBOOKS

Detection of the threat is just the beginning; Dragos' playbooks guide the analyst on the appropriate response to the threat.

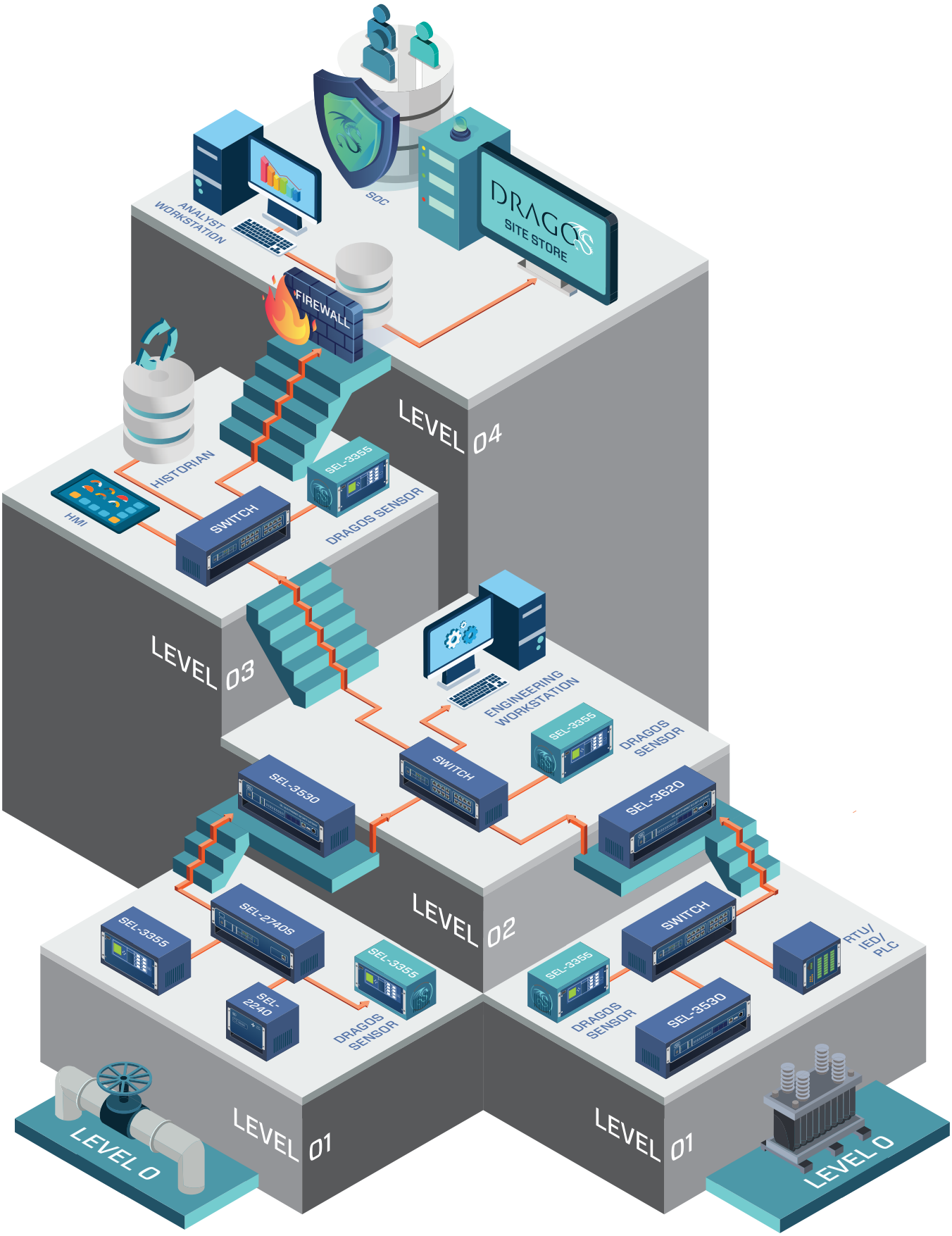
TECHNOLOGY

The Dragos Platform is the industry's only technology to take an intelligence-driven approach to threat detection and response. Expert analysts on the Dragos Intelligence team, industry cybersecurity practitioners, and incident responders in the Dragos Threat Operations Center create threat behavior analytics and investigation playbooks to power the Dragos technology. Threat analytics ensure that when a detection occurs, analysts understand the context of the alert and descriptions of the adversary behavior detected. Each threat analytic is paired with an investigation playbook that provides step-by-step guidance to investigate the adversary behavior and adjacent events. This allows the Dragos Platform to be deployed quickly and immediately usable by defenders to perform effective and efficient threat detection and response.

Additionally, the Dragos Platform provides the most coverage of data sources in the ICS security technology market. The technology passively monitors network traffic to perform deep packet inspection of ICS protocols but also collects, aggregates, analyzes, and correlates data from other sources including data historians, host logs, and logic controller events. Now, with the SEL and Dragos partnership the Dragos Platform also integrates with SEL equipment and communications including logs from SEL ICON and SEL Real-Time Automation Controllers (RTACs).

As asset owners build new industrial networks or update existing infrastructure, they are routinely turning to the SEL-2740S Software-Defined Network Switch and SEL-5056 Software-Defined Network Flow Controller for deterministic Ethernet communications in mission critical applications. The SEL-2740S and SEL-5056 is now available for integration with the Dragos Platform so that complete and accurate visibility can be maintained, and unauthorized network flows can be analyzed and investigated by the Dragos Platform. Finally, the SEL 3355 hardened industrial computer is the recommended hardware solution for Dragos Platform's midpoint sensor appliance.

THE ARCHITECTURE



FEATURES & BENEFITS

DRAGOS PLATFORM INTEGRATION WITH SEL DEVICES AND PROTOCOLS

Improved visibility of asset identification, communication flows, and threat behaviors for increased situational awareness. SEL devices include SEL ICON and SEL Real-Time Automation Controllers (RTACs). Coverage supports standard protocols such as IEC 61850, DNP3 etc. and SEL protocols.

DRAGOS PLATFORM INTEGRATION WITH SOFTWARE DEFINED NETWORKING (SDN) TECHNOLOGY

Dragos Platform integration with the SEL-5056 SDN Flow Controller and SEL-2740s SDN Switches enable analysis of packets sent in nonauthorized network flows. This allows a quick response to detected threats by modifying network flows from within Platform.

HARDENED MIDPOINT SENSOR USING THE SEL 3355 INDUSTRIAL COMPUTER

Deploy Dragos's platform in challenging environments such as substations to provide complete ICS network coverage. The SEL 3355 hardened computer meets IEEE 61850-3, 1613, C37.90, IEC 60255 & UL standards & and offers a 10 year, standard no-questions asked warranty.

THREAT RESEARCH AND IMPACT ANALYSIS

Increased exposure of emerging ICS targeted threats combined with accompanying best practices empower defenders to know what to look for and how to respond.

THREAT ANALYTICS AND PLAYBOOKS UNIQUE TO SEL SYSTEMS

Threat based recommendations on how to respond after detection.

DRAGOS

1745 Dorsey Rd
Hanover, Maryland 21076
info@dragos.com