REPORT REPRINT

# Dragos takes a threat intelligence-driven approach to improving ICS and SCADA security

**PATRICK DALY, SCOTT CRAWFORD**

**3 APRIL 2018**

With a range of critical infrastructure security offerings and an experienced threat intelligence and incident response team, Dragos is well positioned to take advantage of increasing activity in the ICS security space, both from attackers and defenders.



Although it is a growing field, the market for industrial control system (ICS) security has one factor in common with IT security: a shortage of skills and experience. In the case of ICS security, there is high need for expertise in dealing with ICS-specific threats. The significance of this shortage is magnified by the increasing number and sophistication of threats to critical infrastructure. The recently discovered TRITON/TRISIS malware, for example, represents a paradigm shift in attacker behavior because it is the first ICS-specific malware to target safety instrumented systems within ICS designed to detect unsafe conditions. Interfering with this functionality paves the way for damaging attacks to be carried out with an increased likelihood of success.

Dragos provides a portfolio designed to not only improve the security posture of ICS networks through better visibility into device activity and threat detection, but also to bring the company's expertise directly to customer security teams. This is achieved through the use of playbooks that walk analysts through a step-by-step process for incident response, training courses for existing customers to become more familiar with ICS security, and directly aiding in response and remediation with professional services.

## THE 451 TAKE

Dragos' focus on addressing the gap between its customers and their adversaries in skills, processes and tools specific to ICS security is an approach that we expect will pay dividends for the company throughout its development. Its team can call on the specific industry expertise required to provide customers with highly relevant and actionable insight and threat-driven alerts that are accompanied by guidance on proper next steps to improve the efficacy of its customers' ICS security operations. Coupling this with the enhanced visibility gained through the Dragos Platform, professional services and training courses creates a compelling value proposition. However, the fact that Dragos' platform is fueled by human-gathered threat intelligence is a double-edged sword. Gathering useful threat intel that pertains to attacker tactics, techniques and procedures is labor-intensive and requires a large, highly skilled team to perform at scale. We would therefore expect the company to continue to prioritize building out its intelligence and threat-hunting operations to keep up with the accelerating pace of ICS security threats.

## CONTEXT

Dragos officially launched in August 2016 when the company began to take in venture funding, and announced a $1.2m seed round. However, the company traces its roots back four years prior when CEO and cofounder Robert M. Lee and his two cofounders developed a passive discovery and identification assessment tool for ICS assets known as CyberLens. Lee served as a Cyber Warfare Operations Officer with the US Air Force.

Since then, Dragos' offerings have evolved beyond the initial scope of CyberLens to take a threat-intelligence-based approach to ICS security. Lee's two cofounders, CTO Jon Lavender and chief data scientist Justin Cavinee, both worked in the US intelligence community prior to starting Dragos. Lavender led both red and blue team operations, while Cavinee developed technologies to identify threats to ICS and SCADA systems.

Since its inception, Dragos has grown to 32 employees; four in sales and 15 in product development and support, with the remaining 13 devoted to threat intelligence and incident response. The company also raised a $10m series A round from Allegis Capital, Energy Impact Partners, DataTribe and BYU Cougar Capital, bringing total investment in Dragos to $11.2 m. The primary verticals that Dragos is targeting include manufacturing, petrochemical and energy.

## PRODUCTS

The Dragos portfolio currently incorporates Dragos Worldview, a set of ICS-specific threat intelligence services; the Dragos Platform for ICS security monitoring and situational awareness; and professional services to better equip organizations to handle and respond to ICS security threats. The Dragos Platform is the company's flagship technology product; its overarching goal is to bring the expertise of the Dragos team to each of its customers. This not only provides enhanced visibility and detection capabilities, but assists in incident response and threat hunting as well.

The platform is deployed as a series of hardware sensors on the ICS network with a central aggregation point called Sitestore that can be deployed as a VM on-premises or in the cloud. These sensors passively identify all ICS network assets and inter-asset communications, granting greater visibility into network activities, and establishing behavioral baselines used in risk assessment. While network traffic is a primary source for Dragos, it is not the only one. The platform also has the ability to ingest host logs as well as logs from specific ICS technologies, such as controllers and data historians, to gain deeper insights into their activity and facilitate investigations.

Where Dragos differs from some offerings currently on the market is its emphasis on using ICS-specific threat intelligence to guide detection and aid in the incident response process. Rather than alerting to just behavioral anomalies, Dragos codifies threat data gathered by its intelligence analysts in a way that can be used to flag the tactics, techniques and procedures of known adversary groups and attack campaigns, with previously unrecognized activity prompting further investigation by its threat intelligence team.

Alerts are then accompanied with a playbook outlining a step-by-step process for how the organization should respond. Playbooks are developed by the Dragos incident response team, and represent a method of bringing the company's expertise to customers in need of experienced response to ICS-related threats – a definite need when these specific skills are in short supply.

In addition to leveraging threat intel for detection on the Dragos Platform, the company also offers Worldview as a separate threat intelligence product that provides customers with malware identification and analysis, disclosure of known vulnerabilities, indicators of compromise and analysis of adversary behavior. The company delivers weekly reports and monthly webinars on relevant events and threats to continue educating its customers on the evolution of the ICS threat landscape. Dragos' 13-person team focuses exclusively on threat intelligence, and incident response continuously investigates new and known threats to populate the platform with actionable data.

The final piece of the Dragos portfolio is its services segment. The company provides security assessments, incident response, table top exercises and training courses for existing clients, all of which aim to improve the effectiveness of security tools, procedures and personnel in defending against attacks on critical infrastructure.

## STRATEGY

Although similar to other approaches in how its platform is deployed in customer environments, Dragos is seeking to differentiate on why customers should come to the company, with a model emphasizing threat intelligence for detection and providing guidance or hands-on assistance in driving response. This approach is betting that customers value the playbooks and contextual alerts for their usefulness in resolving threats, due to an industry-wide ICS security skills shortage that makes staffing teams that have relevant experience rather difficult.

The strategy reflects a larger trend not just in IT security, but in broader technology markets as well, where the application of structured 'playbook' approaches to action have become a hallmark of the automation tools and processes that increasingly define the nature of security operations, as well as of evolving approaches to enterprise IT aligned with DevOps concepts.

Dragos has also begun developing a partner ecosystem that includes Deloitte for systems integration and customers that want a managed security offering, Schweitzer Engineering Labs as an OEM and research partner, OSIsoft to pull real-time operational data from the vendors' data historians, and CrowdStrike to further advance the incident response offering through response in enterprise IT environments.

## COMPETITION

The increased demand for more robust ICS security over the past few years has contributed to a growing ecosystem of vendors, primarily startups, focusing on solving this issue. The overwhelming majority of vendors in this market have a similar deployment model to Dragos, with sensors deployed throughout the ICS network that passively pick up traffic and device information for analysis by an on-premises or cloud-based back end.

Many of these are based on the ability to recognize anomalies from observed activity. Nozomi Networks, for instance, recently announced a hybrid threat detection model that leverages YARA rules for signature-based threat detection while conducting anomaly detection for unknown threats. Claroty is another competitor that offers vulnerability management and secure remote access control on top of its network behavior-based detection.

Other competitors include CyberX, PAS, Radiflow and Sentryo, all of which incorporate some level of network behavior-based anomaly detection in their offerings. Where Dragos differentiates from many of these plays is in the ICS-focused expertise of its team, reflected in its intelligence-centric approach, where its deep and detailed knowledge of the specifics of the ICS threat landscape are born out of experience.

## SWOT ANALYSIS

### STRENGTHS

The Dragos teams' experience with ICS security informs its approach to guiding customers in responding to ICS threats, which helps make the company a valuable asset for talent-constrained customers.

### WEAKNESSES

Professional services such as incident response and threat data gathering are labor-intensive, and may not scale as well as a technology offering. While overcoming such limitations is clearly in view, particularly with the Dragos Platform, this labor bottleneck could become a more significant factor as the company continues to gain traction and add customers.

### OPPORTUNITIES

By developing newer integrations with security automation and orchestration platforms, Dragos could further reduce the manual burden of threat hunting and incident response for its customers, as well as its own team.

### THREATS

With the influx of new vendors in the space, it could become more difficult for Dragos to overcome increasing noise in the space. Its recognized expertise should, however, help it maintain its credibility edge, so long as human availability does not become a limiting factor for growth.