The Dragos Platform is the most technologically complete solution in the industrial cyber threat detection and response market today. It provides security teams with unprecedented knowledge of their industrial control system (ICS) assets and activity, the threats and adversaries they face, and the tools and knowledge to defend against them. It is the industry's first and only solution to codify and integrate the knowledge of the industry's most trusted ICS security experts and an intelligence-driven approach with software technology. When you deploy the Dragos Platform, you get not only the features and benefits of advanced software, you get the transfer of knowledge from Dragos Threat Intelligence, Threat Hunting, and Incident Response teams that is integrated right into the Platform.

**Dragos Platform Overview**

The Dragos Platform was designed and built by recognized ICS security practitioners who have lived the challenges that security teams face securing industrial control systems and their surrounding infrastructure. Our deep understanding of those challenges and the ICS threat landscape is reflected in our differentiated approach to providing a solution to them, as shown below:

<table>
<thead>
<tr>
<th>Dragos Platform</th>
<th>Typical Industry Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principal threat detection method</td>
<td>Threat Behavior Analytics</td>
</tr>
<tr>
<td>Ongoing system/training adjustment</td>
<td>Minimal</td>
</tr>
<tr>
<td>Alert/threat response capabilities</td>
<td>Automated/Integrated into Platform</td>
</tr>
<tr>
<td>False positives</td>
<td>Few</td>
</tr>
<tr>
<td>Threat intelligence</td>
<td>Integrated into Platform</td>
</tr>
<tr>
<td>Detailed threat context with alerts</td>
<td>Yes</td>
</tr>
<tr>
<td>Potential for alert fatigue</td>
<td>Low</td>
</tr>
<tr>
<td>Ongoing cost of ownership</td>
<td>Low</td>
</tr>
</tbody>
</table>

“The passive, cybersecurity defenses used in most industrial cybersecurity programs may be adequate for low-risk facilities. But operators in critical industries need to recognize that, increasingly, they are on “the radar” of sophisticated attackers and must be able to ensure that their programs can defend against non-traditional, targeted attacks. Active monitoring and management of anomalies by qualified people is essential.

Adopting a context-aware, intelligence-driven approach, like that offered by Dragos, can help ensure that these resources have the information and tools they need to be both effective and efficient.”

Arc Advisory Group, December, 2017
Dragos Platform Modules

The Dragos Platform provides all of the necessary capabilities to gain visibility into industrial networks across the entire industrial cybersecurity framework. It operates as a security incident and event management (SIEM) solution, purpose built for industrial environments, and can be deployed in a security operations center (SOC) model. It is modularly designed so that it can be deployed in whole or in parts to address both immediate and longer-term needs.

### Asset Discovery
- Passively identify all assets and communications on the network
- Visualize and map network security zones and identify attack paths
- Set one or more network baselines against which to monitor changes
- Scalable to hundreds of thousands of assets across multiple sites

### Threat Detection
- Dragos threat behavior analytics provide rich context as to what is occurring and what to do next
- Indicator of Compromise and Query-Focused Datasets support threat hunting
- Collects, stores and analyzes logs and data from host systems, logic controllers and data historians, not just data traffic

### Investigation Playbooks & Workbench
- Use case management tools to manage incident response case notes, forensics and collaboration
- Playbooks from Dragos experts drive standardized, best practice response
- Automation and orchestration between different security tools reduces workload
- Reporting and Dashboards monitor analyst and system activity
“The Dragos Platform provides us with a level of real-time, situational awareness and monitoring capabilities unparalleled in the industry today, which was never before possible within our Windfarm networks. It has become an integral part of our day-to-day cybersecurity, OT network monitoring, and asset management program and has eliminated a number of manual processes while increasing our speed of incident response. A high-value system for any organization whose operations are dependent upon ICS technology, processes, and protocols.”

Marc DeNarie, Chief Information Officer NaturEner USA
Dragos Solutions Span the Entire Industrial Cybersecurity Best-Practice Framework

Given the developing nature of industrial cybersecurity tools and practices, many organizations find it useful to apply best practice methodologies to better understand, manage and reduce their cybersecurity-related risk. While there are various solid frameworks, Dragos’ view is that “know thyself, know thy enemy, and know what to do” covers the core tenets of them all.

Dragos provides the only industrial cybersecurity portfolio that spans the entire ICS cybersecurity best-practices continuum. It combines human intelligence analysts, ICS operations experts and advanced technologies to enable asset owners to build and maintain the most effective cyber-defenses possible.

Contact Information
1745 Dorsey Road
Hanover, MD, 21076 USA
dragos.com | info@dragos.com