

# DRAGOS AND MICRO FOCUS

## Improving Detection & Visibility of OT and IT Threats

### HIGHLIGHTS

- Dragos and Micro Focus bring years of combined enterprise and industrial security experience for those pursuing greater convergence of networks.
- Technology integration between ArcSight ESM and Dragos Platform provides enhanced visibility of industrial threat activity.
- Security teams can maximize the value of their technology investments through integration that enables comprehensive coverage of both IT and OT

### THE CHALLENGE

Security executives at industrial organizations, including Chief Information Security Officers (CISO's), are often challenged to provide resources (both technology and personnel) across the entire Information Technology (IT) and Operational Technology (OT) environment. Enterprise security tools that provide analysts with visibility into the IT networks are relatively commonplace but offer limited capabilities for asset and threat identification for Industrial Control Systems (ICS). Since security teams are now required to have a broader converged view of the entire IT, OT, and IIoT (Industrial Internet of Things) networks, there is a need for technology that works together to help bridge the gap. The risk to the business is evident as the industrial threat landscape is prevalent and significant, and the need to provide security professionals with complete situational awareness and decision-making support is critical to ensure swift detection and response.

Often owners and operators of ICS across various industries lack visibility into the OT environment for effective threat detection. Additionally, it is beneficial for security teams to

have a thorough understanding of the sophisticated adversaries that are actively targeting both the IT and OT networks, which could lead to the disruption of systems leading to physical damage and loss of life. This puts increased pressure on the various stakeholders such as leadership, engineering, security specialists, vendors, etc., to ensure readiness with sufficient hardening, detection, and response mechanisms to neutralize the threat and reduce overall business risk.

Furthermore, a diverse ecosystem of different and complex technologies can add to inefficient business processes. Selecting the right partners and tools can have significant benefits down the road because technology deployments in OT environments have long lifecycles.

### THE SOLUTION

ArcSight ESM is a popular SIEM technology deployed amongst many SOC teams to aggregate and analyze threat activity across enterprise IT networks. Dragos Platform is a passive, network-based monitoring technology designed for industrial networks to enable better visibility of assets, threat detection and facilitate guided incident response. By leveraging the combined ArcSight ESM and Dragos Platform technology, customers benefit from integrated monitoring capability for both IT and OT environments within their security operations.

While the ArcSight ESM infrastructure provides analysts with better visibility of enterprise IT events, the combined visibility with Dragos OT threat detection capabilities delivers strong awareness capabilities into OT networks.

Protecting industrial operations requires a comprehensive approach that a single vendor technology cannot provide. To provide a complete solution, multiple technologies must operate together without introducing complexity, adversely impacting safety or availability, while helping security teams achieve their goals. Obtaining visibility of events across the enterprise (IT) and ICS (OT) network is essential to operational security, safety, and sometimes compliance. Understanding and enabling defenders with the ability to react quickly to adversaries that often pivot from enterprise networks to OT is essential.

Industrial environments are typically heterogeneous and consist of a wide variety of technologies and protocols across the ICS (OT) networks. Native support for these systems and their associated communications is critical to enabling effective situational awareness and multi-zone protection. The Dragos Platform passively monitors ICS protocols and decodes the information relayed across the network as well as consuming logs and events collected from ICS assets. The Platform integration with ArcSight ESM gives defenders the ability to harness the power of comprehensive OT visibility and centralized management through a single platform. The Dragos and Micro Focus combination will focus on supporting some of the primary needs of industrial environments; cybersecurity protection without impacting operational safety or availability, situational awareness for improved decision-making abilities, and multi-zone protection support in pursuit of improved cybersecurity.

## BENEFITS AND IMPACTS

BENEFITS	IMPACTS
Enhanced Visibility of IT and OT Networks	Combining ArcSight ESM and the Dragos Platform ensures more effective asset visibility, threat detection, and response for both the IT and OT domains.
Intelligence-Driven Threat Detections	Utilizing comprehensive IT and OT threat intelligence as the primary method of detecting threats, which improves detection confidence and reduces alert fatigue.
More Efficient Security Operations	Integrating the technologies enables defenders with a more comprehensive workflow from initial threat detection through response, improving Mean Time To Recovery (MTTR).

For more information, please visit [www.dragos.com](http://www.dragos.com) or contact us at [info@dragos.com](mailto:info@dragos.com)