SOLUTION BRIEF

DRAGOS
SAFEGUARDING CIVILIZATION

Intellectual Property Theft in Manufacturing

Protecting Your Industrial Environment Against the Growing Threat of IP Theft

Intellectual property (IP) theft is a well-known risk primarily associated with enterprise IT environments rather than operational technology (OT) networks. However, IP information is often embedded in the processes managed by OT networks, and network defenders need to consider the risk of IP theft in OT environments in the broader context of industrial espionage.

IP theft has long-term impacts with potential consequences manifesting over months and years. The loss of IP could lead to forfeiting first-to-market advantage, loss of profitability, or even losing entire lines of business to competitors or counterfeiters.

Dragos threat intelligence researchers have found:

- Adversaries are most likely to pursue IP theft in OT environments as part of a broad campaign, and the sensitive information an adversary can acquire from an OT network may not be available in other parts of a company's network
- Within enterprise IT network segments, sensitive IP is increasingly stored offline or within closely guarded network enclaves; on the OT side of the network, this IP is likely to be embedded into the processes the OT network manages and may be impossible to separate from the OT network's operation
- This information includes details on the amounts of inputs or ingredients, and the specifics of the processes applied that transform raw materials into a finished product or substance
- Network devices which aggregate and store data over longer periods, such as data historians, will remain a logical first target for adversaries targeting IP within OT network environments; this is especially true for networks overseeing continuous and batch manufacturing processes

Dragos has observed a steady growth in both threat activity and the diversity of industrially focused adversaries since 2017. While defending OT networks and their valuable intellectual property from adversary threats is challenging, there are tools, community resources, and partners positioned to assist your company along this journey.

The Dragos Platform: Protecting Your Enterprise

Dragos technology protects manufacturing facilities around the world in dozens of different sub-sectors, including chemical, petrochemical, pharmaceutical, food and beverage, machinery, automotive, and more. The Dragos Platform and professional services can strengthen the readiness and resiliency of your teams, enable secure modernization and innovation, and facilitate compliance while minimizing risk.

The Dragos Platform can help manufacturers protect against IP theft through several key features and capabilities:

Network Visibility: The Platform provides comprehensive visibility into both IT and OT networks, allowing manufacturers to monitor and analyze network traffic, system behavior, and user activities. This visibility enables early detection of any suspicious or unauthorized activities that may indicate potential IP theft attempts.

Threat Detection and Intelligence: The Dragos Platform leverages advanced threat detection capabilities and threat intelligence to identify known and emerging threats targeting manufacturing environments. It utilizes machine learning and behavioral analytics to detect anomalies and indicators of compromise associated with IP theft activities.

Asset Inventory and Management: The Platform offers robust asset inventory and management features, allowing manufacturers to maintain an accurate inventory of their OT devices and systems. This helps in identifying critical assets that may contain valuable IP and implementing appropriate security measures to protect them.

Anomaly Detection: The Dragos Platform uses anomaly detection techniques to identify abnormal behavior or deviations from baseline patterns within the manufacturing environment. This helps in detecting potential unauthorized access attempts or data exfiltration related to IP theft.

Cross-Functional Operations Insights: Monitoring assets, including those within FRCS, and properly dissecting and inspecting network traffic requires in-depth protocol coverage; otherwise, threats and asset details remain hidden. Dragos customers use the platform to detect operational process errors quickly and efficiently, monitor OT/ICS network and device health, support ATO/RMF artifacts, and integrate active defense via SIEMENS Siber Protect.

Incident Response and Investigation: In the event of a security incident or suspicious activity, the Platform provides incident response and investigation capabilities. It offers real-time alerts, workflow management, and forensic analysis tools to aid in swift incident response and mitigation of IP theft risks.

Security Orchestration: The platform integrates with existing security infrastructure and tools within the manufacturing environment, enabling streamlined security orchestration and automation. This helps in responding to security events faster and more efficiently, reducing the potential impact of IP theft.

Continuous Monitoring and Compliance: The Dragos platform facilitates continuous monitoring of the manufacturing environment, ensuring ongoing security and compliance. It helps manufacturers adhere to industry standards and regulatory requirements, reducing the risk of IP theft and associated legal consequences.

The Dragos Platform provides manufacturers with the necessary tools, visibility, and intelligence to detect, prevent, and respond to IP theft attempts. By leveraging these capabilities, manufacturers can strengthen their security posture and protect their valuable intellectual property from adversaries.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.