PARTNER BRIEF

DRAGOS SAFEGUARDING CIVILIZATION | Microsoft

Dragos Platform and Microsoft Sentinel Integration: Unifying IT and OT Security

Bridging the IT-OT Gap with Advanced Threat Intelligence and Cloud-Powered Analytics

Top Five Highlights

1. Seamless installation through Microsoft Sentinel's Content Hub (future feature)
2. Custom data connector for pushing data from the Dragos Platform and pulling notifications from MS Sentinel
3. Pre-built analytics rule template for generating Sentinel incidents
4. Entity mapping between Dragos notifications and Sentinel entities
5. Raw data access for custom querying and analysis

The Dragos Platform and Microsoft Sentinel integration brings together two powerhouses in the cybersecurity realm, offering a comprehensive solution for industrial environments. This partnership addresses the growing need for unified IT/OT security monitoring and management.

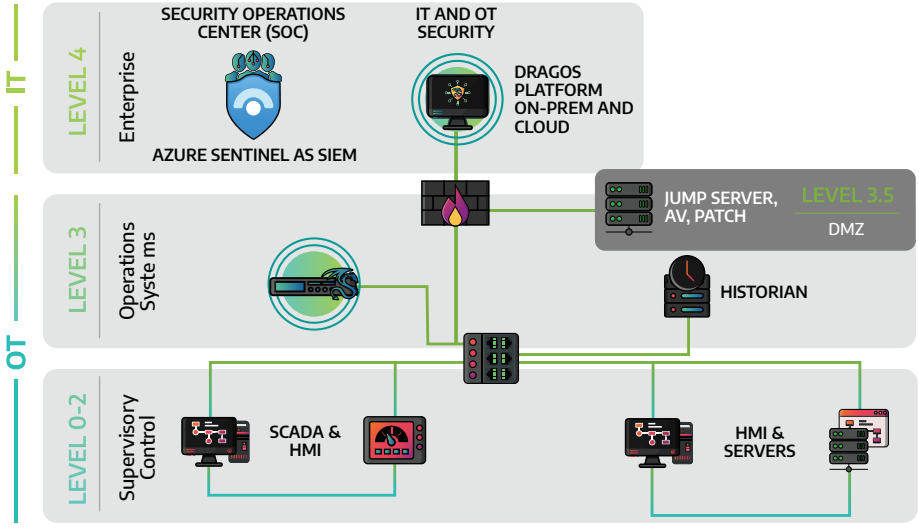
Industry Challenges and Solutions

From sophisticated threats to the complexities of managing diverse control systems, organizations struggle to maintain a strong security posture. The Dragos-Microsoft Sentinel integration directly addresses these pain points, offering innovative solutions that bridge the gap between IT and OT security.

Common Challenges Addressed by the Dragos Platform & Microsoft Sentinel Integration:

- Increasing sophistication of cyber threats in industrial environments
- Difficulty in correlating OT security data with IT security information
- Limited visibility across diverse industrial control systems
- Complexity in managing multiple security tools and platforms
- Need for rapid threat detection and response in critical infrastructure

The Dragos-Microsoft Sentinel integration offers a comprehensive suite of solutions designed to address the complex cybersecurity challenges faced by modern industrial environments. By combining Dragos's unparalleled expertise in OT security with Microsoft Sentinel's advanced cloud-based analytics, this partnership delivers a powerful set of tools that bridge the gap between IT and OT security.



From unified visibility to scalable operations, these solutions empower organizations to enhance their threat detection capabilities, streamline incident response, and maintain a robust security posture across their entire infrastructure.

Each of these innovative solutions contributes to a more secure and efficient industrial cybersecurity landscape:

1 Unified Security Visibility:

By integrating Dragos's industrial threat intelligence into Microsoft Sentinel, this solution provides a single pane of glass for both IT and OT security. This unified view enables security teams to quickly identify and respond to threats across the entire infrastructure.

2 Enhanced Threat Detection:

The integration leverages Dragos's deep OT expertise alongside Sentinel's powerful analytics capabilities. This combination results in more comprehensive and accurate threat detection, especially for industrial-specific threats that might otherwise go unnoticed.

3 Streamlined Incident Response:

With automated incident creation in Sentinel based on Dragos notifications, security teams can respond faster to potential threats. This automation reduces the mean time to detect (MTTD) and mean time to restore (MTTR), crucial metrics in maintaining a robust security posture.

4 Customizable Alerting:

The integration offers flexible severity filtering and custom query capabilities, allowing organizations to tailor their security monitoring to their specific needs and risk profile. This customization ensures that security teams focus on the most critical alerts for their environment.

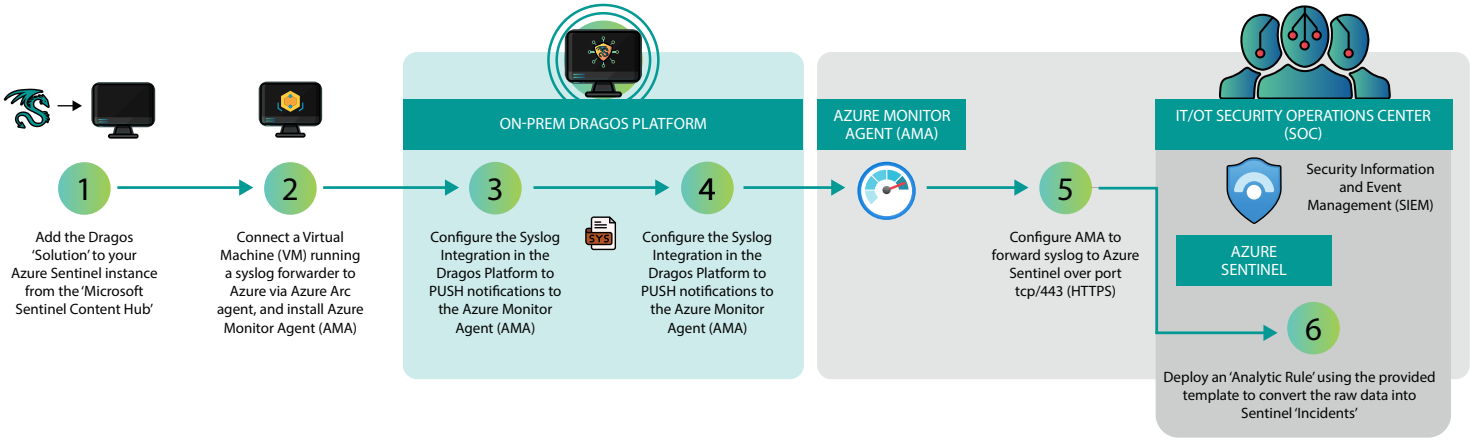
5 Scalable Security Operations:

As a cloud-based integration, this solution supports large-scale deployments and centralized management of industrial cybersecurity. This scalability is essential for organizations with multiple sites or those planning for future growth.

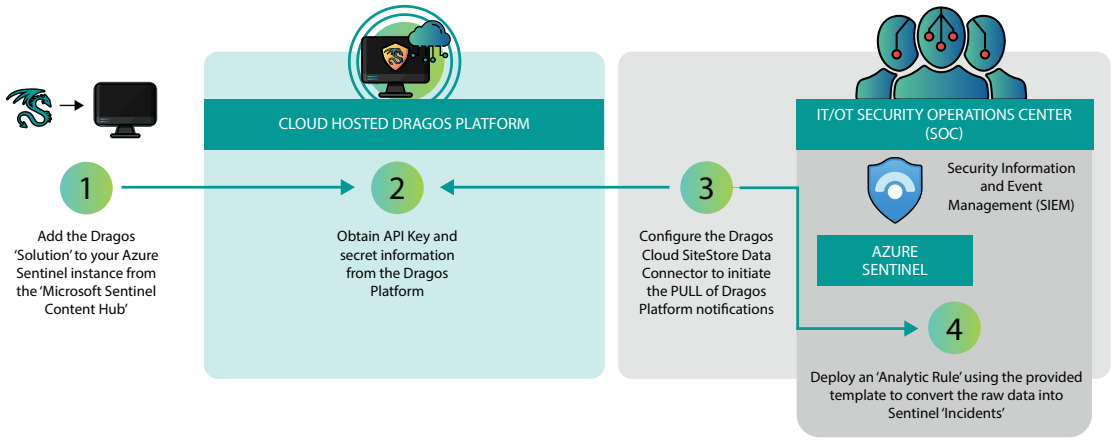
How the Integration Works

The Dragos-Microsoft Sentinel integration is designed for ease of use and efficiency, streamlining the process of connecting these two powerful platforms. From installation to data analysis, each step is optimized to provide maximum value with minimal complexity.

Dragos Platform On-Prem - Azure Sentinel (PUSH)



Dragos Platform Cloud – Azure Sentinel (PULL)



1 Installation:

- Currently deployed via custom Azure Resource Manager (ARM) template
- Future: One-click installation through Microsoft Sentinel's Content Hub

2 Data Connector Setup:

- Configure Dragos Site Store URL, API credentials, and severity filters
- Deploys a Data Collection Rule (DCR) in Azure

3 Data Ingestion:

- DCR pulls notifications from Dragos Platform every 5 minutes
- Raw JSON data stored in custom "Dragos_Alerts_CL" table in Sentinel

4 Analytics Rule:

- Pre-built rule template processes ingested data
- Maps Dragos notification fields to Sentinel entities
- Creates incidents in Sentinel based on Dragos notifications

5 Incident Management:

- Incidents appear in Sentinel with "Dragos" prefix
- Includes extracted entities, custom metadata, and severity mapping

6 Custom Analysis:

- Raw data available for custom querying and additional analytics

How the Integration Works

The Dragos-Microsoft Sentinel integration offers a range of benefits that significantly impact an organization's security posture. Its unique differentiators set it apart in the crowded field of cybersecurity solutions, making it an invaluable tool for industrial environments.

Benefits:

- Unified IT/OT security monitoring
- Automated OT threat detection and incident creation
- Leverages existing Microsoft Sentinel investments
- Scalable cloud-based solution
- Customizable to specific industrial environment needs

These benefits collectively enhance an organization's ability to detect, respond to, and mitigate threats across both IT and OT environments, all while maximizing existing investments in Microsoft Sentinel.

Impacts:

- Improved mean time to detect (MTTD) and restore (MTTR)
- Enhanced collaboration between IT and OT security teams
- Increased visibility into industrial cybersecurity posture
- Better utilization of security resources through automation
-

The impacts of this integration extend beyond just improved security metrics. By fostering collaboration between IT and OT teams and providing comprehensive visibility, it helps create a more holistic and effective security culture within organizations.

Unique Differentiators:

- Combines Dragos's OT expertise with Microsoft's cloud and SIEM capabilities
- Pre-built content specifically designed for industrial environments
- Flexible deployment options (cloud-hosted or on-premises Dragos Platform)
- Maintains raw data for advanced analytics and compliance requirements
- Potential for future expansion with custom playbooks and automated responses

These differentiators highlight how the Dragos-Microsoft Sentinel integration goes beyond typical security solutions, offering a tailored approach to industrial cybersecurity that leverages the strengths of both platforms.

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.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo | Contact Us

About Microsoft

Microsoft Sentinel is a scalable, cloud-native security information and event management (SIEM) that delivers an intelligent and comprehensive solution for SIEM and security orchestration, automation, and response (SOAR). Microsoft Sentinel provides cyberthreat detection, investigation, response, and proactive hunting, with a bird's-eye view across your enterprise.

Microsoft Sentinel also natively incorporates proven Azure services, like Log Analytics and Logic Apps, and enriches your investigation and detection with AI. It uses both Microsoft's threat intelligence stream and also enables you to bring your own threat intelligence.

Use Microsoft Sentinel to alleviate the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

Learn More