ARC VIEW

DECEMBER 7, 2017

Critical Industries Need Active Defense and Intelligence-driven Cybersecurity

By Sid Snitkin

Keywords

Industrial Cybersecurity, Risk Management, Threat Intelligence, Anomaly & Breach Detection, Active Defense, Threat Behavior Analytics

Summary

Cyberattacks are a major concern for industrial organizations around the world. Most have accepted the need for cybersecurity and invested in defensive technologies and practices recommended by automation suppliers and security consultants. This should protect operations from common hackers and malware. But, these passive defenses are often not enough to stop advanced, targeted attacks. To deal with these risks, industrial organizations need an active defense program guided by intelligence.

Defensive technologies and practices recommended by automation suppliers and security consultants are enough to stop common hackers and malware. But, critical industrial facilities need an intelligence-driven, active defense program to manage advanced, targeted attacks. This report describes the requirements for an effective intelligence-driven, active defense program. It also discusses the offerings of Dragos Inc. relative to these requirements.

The SANS Institute defines active defense as "the process of analysts monitoring for, responding to, and learning from adversaries internal to the network." Active defense requires the right mix of knowledgeable people, proven processes and fit-for-use technology. The right people have expertise spanning cybersecurity, control systems and industrial processes. The right processes reflect an understanding of attacker behavior and defender best practices. The right technology integrates detection of suspicious behavior with capabilities for effective, efficient investigation and response.

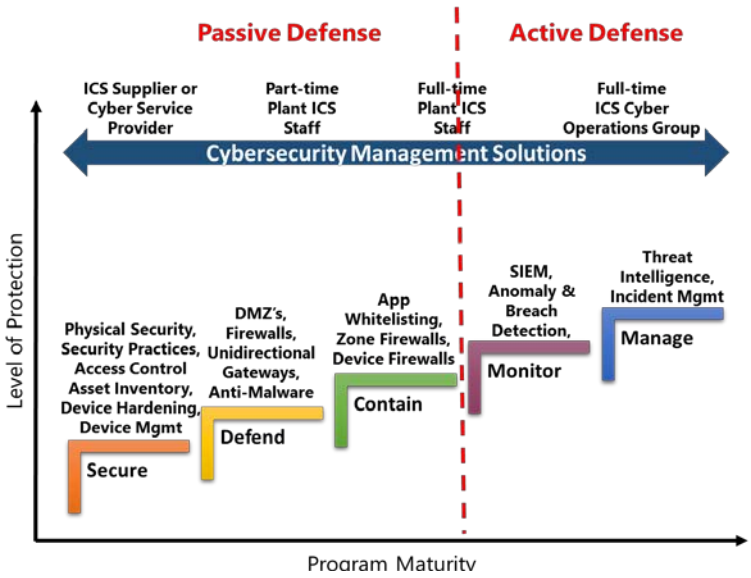
Recently, ARC Advisory Group discussed this with executives at Dragos Inc., a company that offers active defense solutions. The company's staff has extensive experience in industrial cyber defense and intelligence. They

leverage this and the Dragos Platform technology solution to deliver threat intelligence, incident response, and management support.

The Dragos Platform passively identifies and visualizes industrial assets, monitors industrial facilities for threats using threat analytics, and codifies the Dragos team's knowledge and expertise to recommend response actions and best practices to customers when issues arise.

Cybersecurity Requires Passive and Active Defenses

ARC developed the Industrial Cybersecurity Maturity Model to help industrial managers understand their cybersecurity challenges without having to become cybersecurity experts. It enables managers to balance cybersecurity investments with their willingness to accept cyber risks and the cost benefits of additional security layers. This model also provides a convenient way to explain the differences between passive and active cyber defense.



ARC Cybersecurity Model Shows Passive vs. Active Cyber Defense

ARC's model breaks cybersecurity into a set of steps that incrementally reduce cyber risks. Each step addresses a specific, easily understandable, security issue like securing individual devices, defending plants from external attacks, containing malware that may still get into a control system, monitoring systems for suspicious activity, and actively managing sophisticated threats and cyber incidents. Each step has an associated set of actions and technologies that can be used to accomplish its goals. The model also shows the human resources and tools required to sustain and utilize the technology investments effectively.

Critical Operations Need Active Defense

While cybersecurity recommendations from automation suppliers and security consultants span all the steps in this model, ARC's research indicates that most companies have only equipped their facilities with the passive,

defensive technologies shown in the first three steps. Many organizations also lack the resources to maintain and use the more sophisticated defenses above this level.

This may be adequate for companies that can tolerate process disruptions. But operators of critical infrastructure cannot accept any unnecessary risks. They need to be prudent and ensure that their programs include active defense of all facilities, driven by an intelligence-based approach. This will ensure rapid root cause analysis and appropriate response to cyber threats that minimize the mean time to recovery for any incidents.

Essential Elements of an Effective Active Defense Program

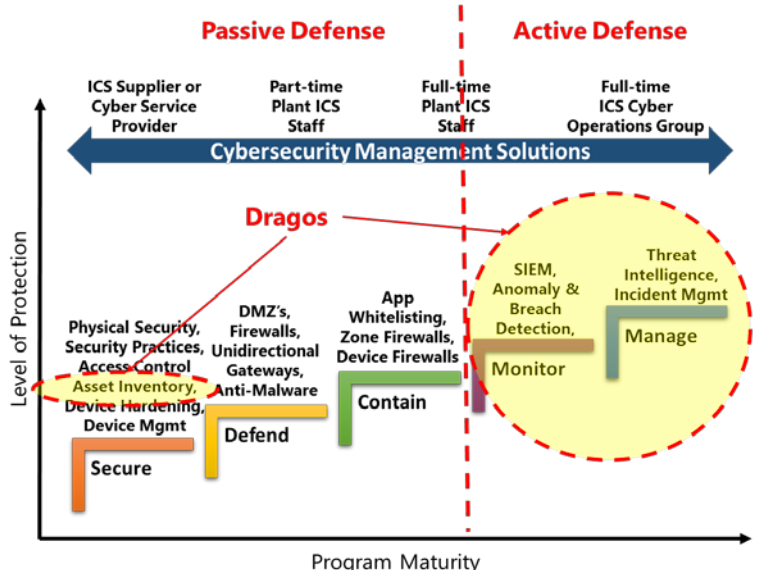
An effective active cybersecurity defense program requires continuous monitoring by people who can recognize and react to sophisticated cyberattacks. Intelligence provides them with the context and appropriate action recommendations for each threat. This often requires organizations to make additional investments in technology, people, and processes.

Industrial anomaly and breach detection is necessary for active defense, but not sufficient. A good anomaly and breach detection product will notify users of changes in endpoints or message patterns, but active defense requires additional features that support the needs of active defenders. These include:

- Detection based on intelligence-driven context, instead of context-less anomalies that put the full cost of investigation on the analyst
- Detections that account for multiple devices and types of data, instead of just network traffic
- Historical records of the kinds of events and network messages that defenders need to understand the context of suspicious behavior
- Tools and workflows that support efficient investigation and management of suspicious behavior. This includes the ability to perform data queries for patterns that attackers might utilize to disrupt system operation (e.g., the steps in the popular ICS Cyber Kill Chain model)
- Ability for defenders to implement specific, ad hoc detection and evaluation queries that incorporate information from threat intelligence sources monitoring emerging threats and changes in attacker tradecraft

As the ARC model illustrates, most organizations lack the resources for active defense. They could address this through training plant staffs,

developing shared corporate resources, and contracts with external service providers. Whichever approach is chosen, the final team requires both expertise that spans cybersecurity, control systems, and industrial processes; plus the tools to do their work efficiently. Good defenders need to appreciate industrial constraints and have the knowledge to anticipate paths attackers may take to disrupt operations.



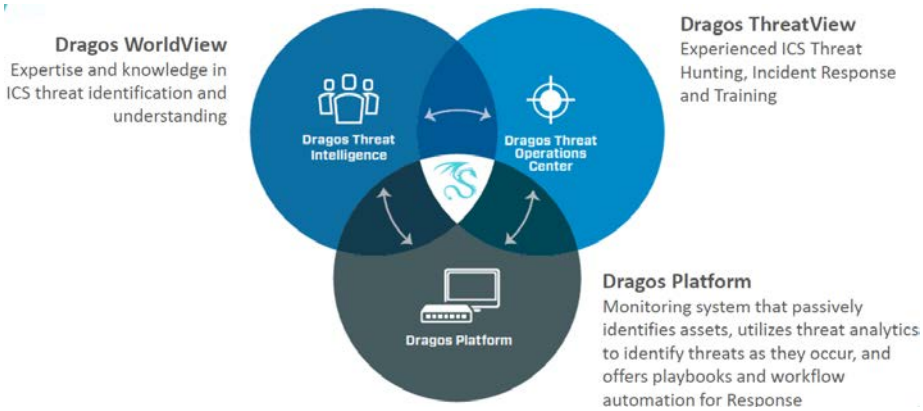
Dragos Enables Programs to Incorporate Active Defense

Addressing Key Active Defense and Intelligence Issues

As ARC learned, Dragos offers a suite of products and services that span all active defense elements in ARC's model and ICS-specific threat intelligence.

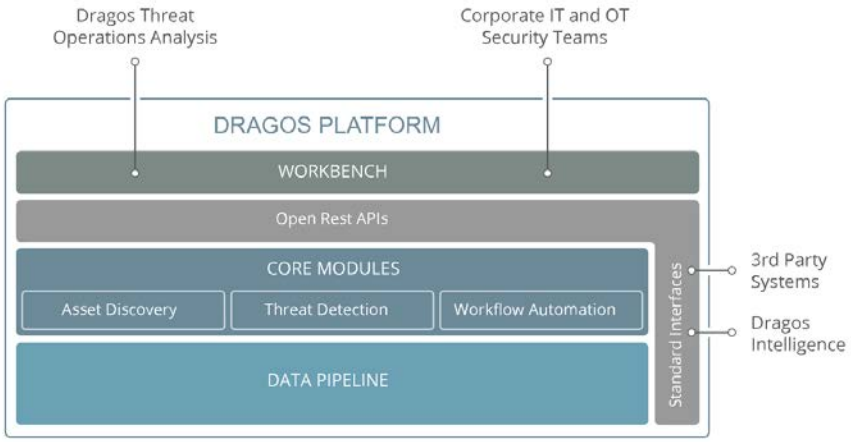
Experts in the Dragos Threat Operations Center can augment a company's internal resources to help manage sophisticated attacks, support incident management, and train staff. Cybersecurity experts in Dragos Threat Intelligence group provide ongoing insight regarding actions a company should take to recognize and manage emerging threats to industrial plants and infrastructure operations.

The company's flagship product, the Dragos Platform, is designed to support active defenders. It codifies the knowledge of the intelligence and threat operations teams. Its capabilities and features reflect the company's extensive experience in cyber defense. The company continuously updates the Dragos platform with threat behavior analytics, providing context to



Dragos Ecosystem

inform defenders about what they are looking at and recommending appropriate responses for new threats identified.



Dragos Platform

The Dragos Platform includes a data pipeline that collects network traffic information from passive network sensors and augments this with additional information from repositories like controller logs and alarms. The asset discovery module uses this information to develop asset maps and network connectivity patterns across all major industrial protocols. Information collected by the data pipeline is centralized and normalized, acting like an ICS SIEM (security information and event management) system.

Dragos' threat behavior analytics are run across the collected data. Unlike conventional anomaly detection, behavioral analytics provide an intelligence-driven approach that incorporates specific threat context. This lowers the total cost of ownership of investigation for a company's security team. The Dragos Platform also includes knowledge-based incident response playbooks and workflows that provide guidance based on the lessons learned by the company's threat intelligence and operations team. The workbench provides user-friendly access to all platform capabilities.

The company demonstrated the capabilities of the Dragos Platform to several ARC analysts. This made it clear that any defender could gain significant benefits from its capabilities. ARC notes some capabilities that illustrate how this product differs from industrial anomaly and breach detection solutions. These include:

- An asset viewer that collects, identifies, and visualizes interconnected systems and assets to help make defenders fully aware of the environ-

ment and detected changes. The asset viewer has impressive scale, allowing defenders to monitor hundreds of thousands of assets across geographically separated infrastructures.

- A fully-integrated case management capability to start a case, document observations and hypotheses and collaborate with other defenders. An included journal provides a full audit log during a case.

- An Analytic Manager that enables users to monitor and modify important threat behavior analytics that drive the system's threat hunting guidance. Monthly content packs are delivered to clients with new threat behavior analytics created by the Dragos intelligence team.

- Playbooks created by the Dragos Threat Operations Center accompany the analytics and contain work steps that guide a defender through the investigation of different kinds of threats. These steps are linked to various data sets to help them get the info they need quickly. These playbooks could make experienced defenders more efficient, but more importantly, they might enable even less-skilled people to investigate and manage incidents effectively.

Recommendations

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.

For further information or to provide feedback on this article, please contact your account manager or the author at srsnitkin@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC