
fal.con
virtual
CrowdStrike
Cybersecurity
Conference
10.2020
falconexperience.crowdstrike.com

Cautionary Statement Regarding Forward-Looking Statements

This presentation includes express and implied "forward-looking statements", including forward-looking statement within the meaning of the Private Securities Litigation Reform Act of 1995. Forward-looking statements include all statements that are not historical facts, and in some cases, can be identified by terms such as "anticipate," "believe," "estimate," "expect," "intend," "may," "might," "plan," "project," "will," "would," "should," "could," "can," "predict," "potential," "continue," or the negative of these terms, and similar expressions that concern our expectations, strategy, plans or intentions. Forward-looking statements contained in this presentation include, but are not limited to, statements concerning the performance and benefits of our platform, products and services; our strategic plans or objectives; our growth prospects; and our future financial and operational performance. By their nature, these statements are subject to numerous risks and uncertainties, including factors beyond our control, that could cause actual results, performance or achievement to differ materially and adversely from those anticipated or implied in the statements. These and other risk factors are described in the "Risk Factors" section of our most recent Form 10-Q and/or Form 10-K filed with the Securities and Exchange Commission. You should not rely upon forward-looking statements as predictions of future events. Although our management believes that the expectations reflected in our statements are reasonable, we cannot guarantee that the future results, levels of activity, performance or events and circumstances described in the forward-looking statements will be achieved or occur. Recipients are cautioned not to place undue reliance on these forward-looking statements, which speak only as of the date such statements are made and should not be construed as statements of fact. Except to the extent required by federal securities laws, we undertake no obligation to update these forward-looking statements to reflect events or circumstances after the date hereof, or to reflect the occurrence of unanticipated events.

Securing Your Industrial Operations With the Power of Dragos and CrowdStrike

Matt Cowell – Dragos, Inc.

Agenda

- The Industrial Environment
- Threats to Industrial Operations
- Recommendations to Secure Operations

Matt Cowell

Sr. Director of Business Development

- Over 20 years of experience in ICS and OT environments.
- Led ICS cyber security training classes for industry associations such as AWWA.
- DEFCON ICS Village/RSA sandbox volunteer.

Introduction to Dragos

Industrial Control Systems (ICS)

- Sometimes referred to as Operational Technology (OT)
- Operates essential infrastructure society depends upon
- Complex, engineered systems comprising various vendor technologies
- Disruption can cause significant impact to human safety and/or revenue

Generally Speaking…

Industry Challenges

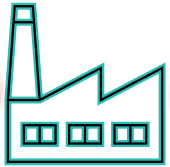
Focus on safety and uptime
Diverse systems & technology
Complex change processes & patching challenges
Long system lifecycles
Insufficient monitoring
Insecure by design
Limited threat visibility
Digital transformation

Threats to ICS

Targeted

Activity Groups
- Internet Connectivity
- Supply Chain
- Remote Services

eCriminals
Insider



Impact
- Credibility
- Financial
- Espionage/IP Theft
- Disruption
- Safety

Untargeted

eCriminals
- Ransomware
- Commodity Malware

https://www.dragos.com/year-in-review/

Differences Between IT and OT Cyber Security

	IT Security	OT Security
Endpoints	Typically PC's, Servers, Mobile Devices	Diverse. Includes Specialty embedded devices, PC's, Servers
Vulnerability Scanning	Commonplace, effective	Undesirable. Known to have caused system outages
Patching	Quickly and Frequently	Delayed. Only when approved by vendor and tested in sandbox. Scheduled outage.
Internet Connectivity	Commonplace, Cloud technology popular	Infrequent. Often restricted through DMZ and jump hosts.
Encryption	Commonplace at rest and in transit	Some usage. Rarely used at transport layer.
Main Priority	Data Protection	Safety & Availability

Best Practice: #1 Assess Your Maturity

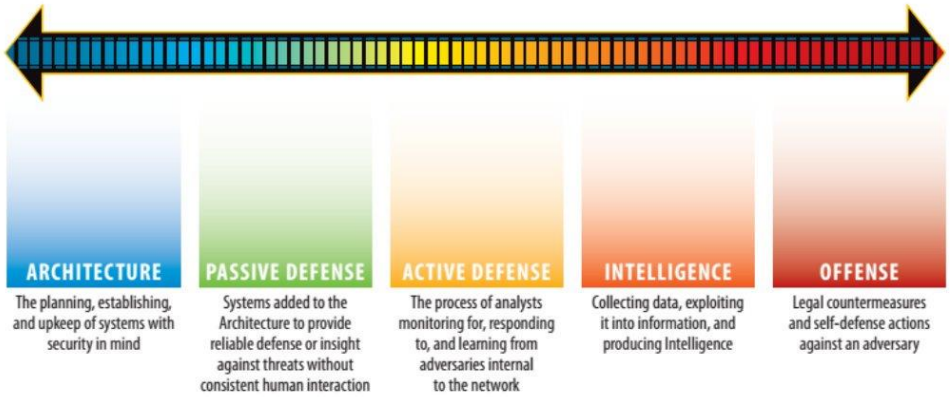
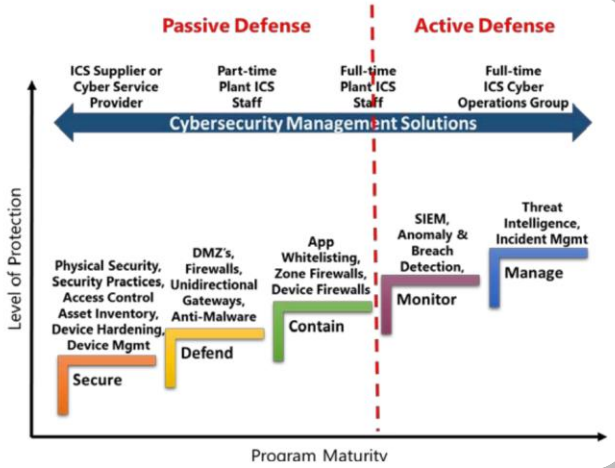


Figure 9: The Sliding Scale of Cyber Security

https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240



https://dragos.com/media/ARCView Dragos-01.pdf

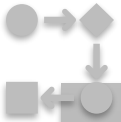
Best Practice: #2 Understand Your Gaps

People

- Domain Expertise
- Multi-skilled
- Tiered support

Technology

- Collection
- Visibility
- Detection
- Workflows



Process

- Consensus based
- Tested
- Adaptable
- Responsibilities

Best Practice: #3 Be Proactive

"An ounce of prevention is worth a pound of cure" – Benjamin Franklin

1. Better understand your environment and weaknesses
2. Develop and refine your processes
3. Be better prepared for an incident

Assessments

Threat Hunting

Threat Intelligence

Training

Proactive Support From Dragos & CrowdStrike

People

OT

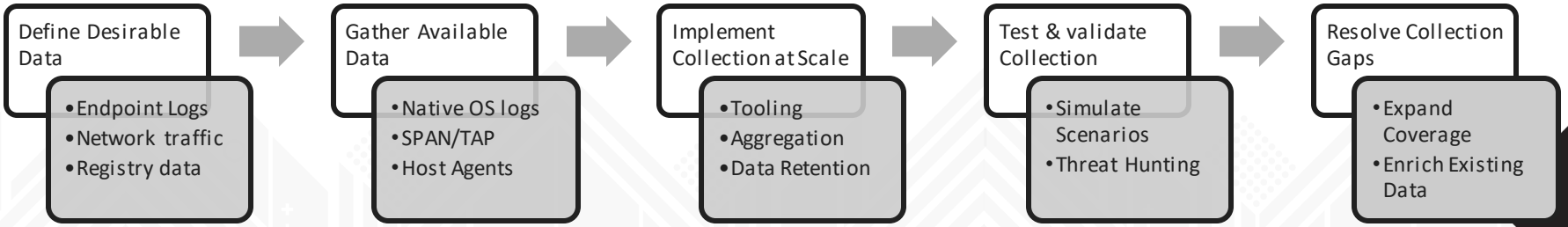
- Threat Hunting
- Neighborhood Watch
- WorldView Threat Intelligence
- Assessments:
  - Penetration Testing
  - Architecture Review
  - Network Vulnerability Assessment
- Training

IT

- Compromise Assessment
- Falcon Overwatch
- Falcon X Threat Intelligence
- Assessments
  - Penetration Testing
  - ..

Best Practice: #4 Define a Collection Management Framework (CMF)

- Effective threat detection begins with thorough data collection
- Reconcile overall goals against available information - asset types, data types, collection method, data retention etc.
- Establish a CMF:



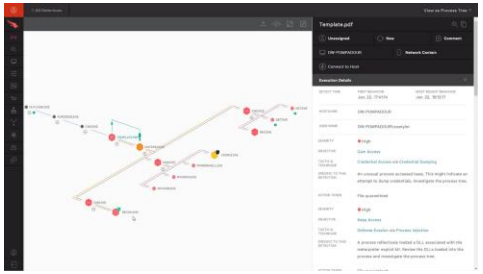
https://www.dragos.com/resource/collection-management-frameworks-beyond-asset-inventories-for-preparing-for-and-responding-to-cyber-threats/

Threat Detection With Dragos & CrowdStrike

Technology

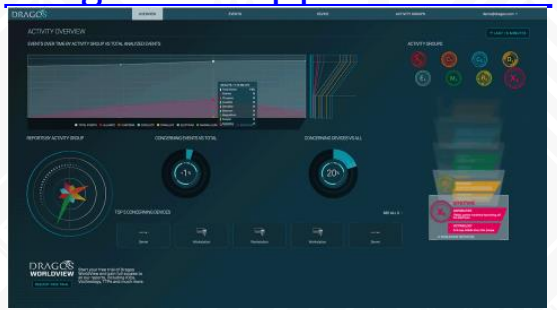
- Dragos Platform

- CrowdStrike Falcon



+

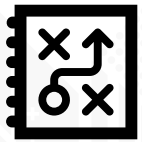
- Dragos ICS App for Falcon



Best Practice: #5 Incident Preparedness

"Be Prepared" – Lord Baden Powell

1. Develop a response plan for various applicable scenarios inclusive of all stakeholders
2. Clearly define roles and responsibilities
3. Test and validate IR plans to ensure efficacy and identify gaps



IR Planning

Tabletop Exercises

Simulation/Drills

Reactive Support From Dragos & CrowdStrike

People

- Joint IR Retainer for IT and OT

OT

- Incident Response Retainer
- Tabletop Exercise

IT

- Incident Response Retainer
- Tabletop Exercise

Conclusion

- Your approach to secure OT needs to be different from your IT strategy
- Industrial threats are increasing in frequency and sophistication
- The right solution requires a combination of people, process and technology
- The right balance depends on your current capabilities and goals
- Develop a plan that's realistic relative to available resources, time & budget
- Leverage trusted vendors and partners to fill current gaps
- Assume breach - be proactive, be prepared

Thank you.

mcowell@dragos.com

@m_p_cowell