CREDC

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Seminar Series

Southern Company Gas

IT and OT, Information Security Architectural and Operational Divides in the Energy Sector

Cyber Resilient Energy Delivery Consortium (CREDC)

Mark Guth
Manager Corporate Security Critical Infrastructure Compliance
March 13, 2018

Agenda / Table of Contents

1. IT and OT Definitions
2. IT and OT Security Tool Options
3. Cloud Computing Impacts
4. IT and OT System Project Management Methodologies
5. Maintenance and Support
6. Training and Certification Opportunities
7. Other OT Factors Impacting Cyber Security
8. Research Opportunities
9. Questions???

1. IT and OT Definition

1. **Information Technology** (**IT**) “is the application of computers to store, retrieve, transmit and manipulate data,[1] or information, often in the context of a business or other enterprise.”[1]

2. **Operational Technology** (OT) “is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.”[2]

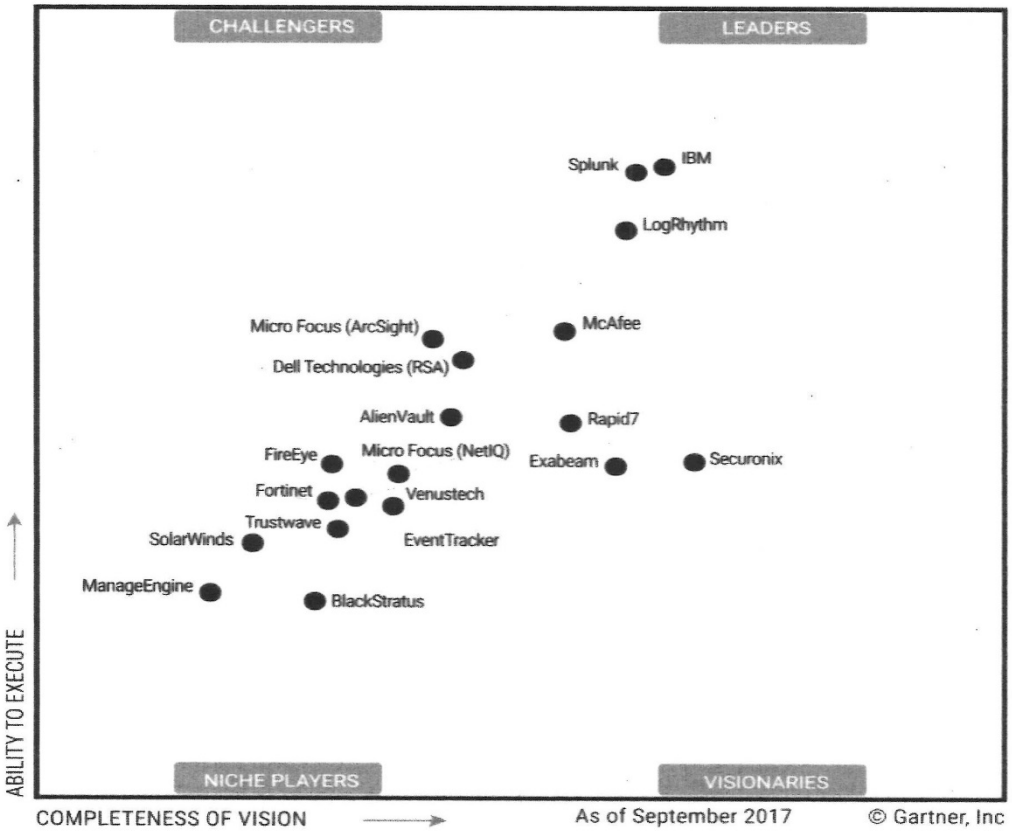
3. **SCADA - Supervisory Control and Data Acquisition** is “a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controllers and discrete PID controllers to interface to the process plant or machinery.”[3]

4. **Internet of things** (**IoT**) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure. [4]

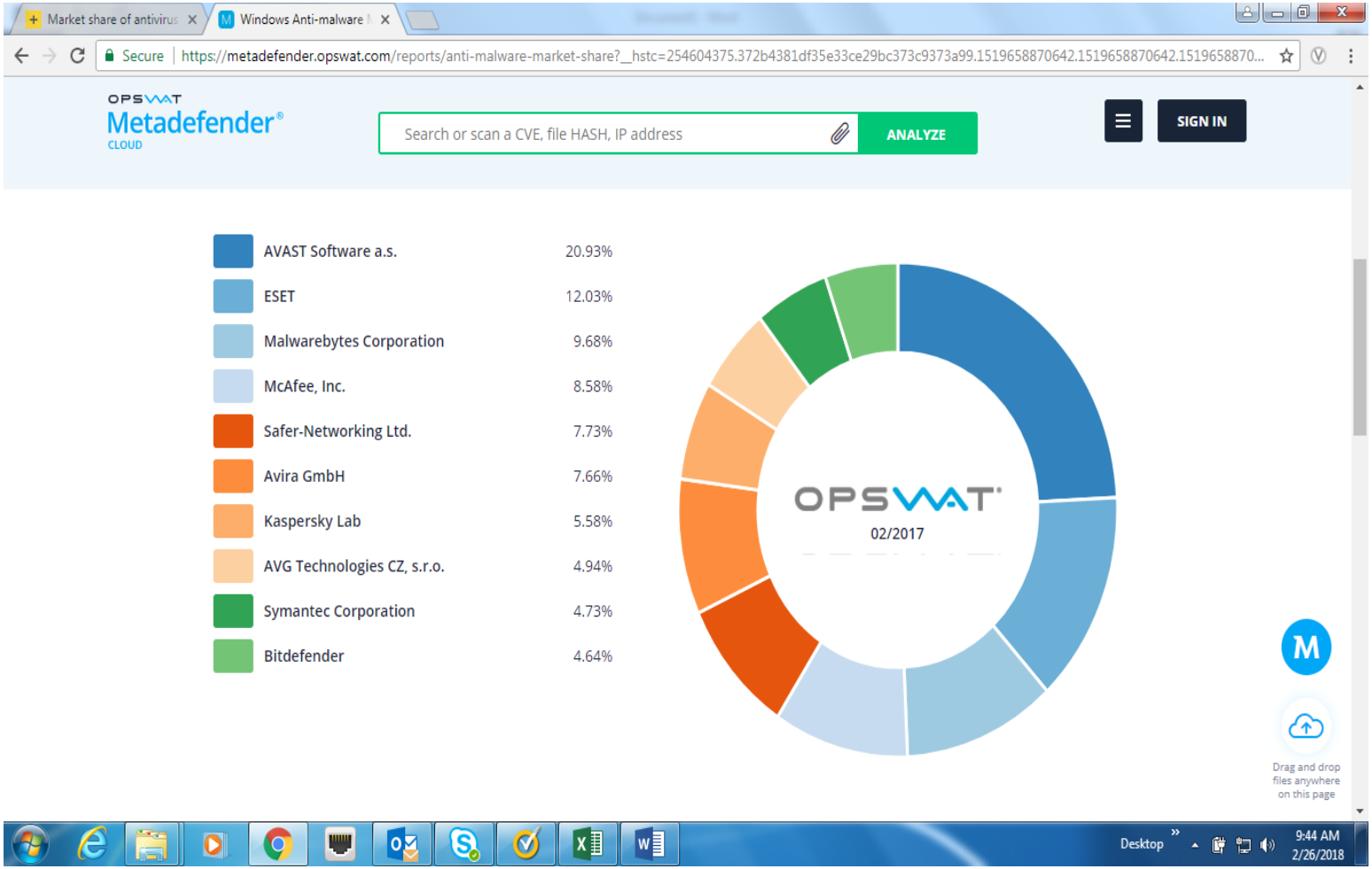
2. IT and OT Security Tool Options
Antivirus Vendors in Information Technology Market

Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management



2. IT and OT Security Tool Options
Antivirus Vendors in Information Technology Market



OPSWAT Antivirus Market Share Report 2017 [5]

2. IT and OT Security Tool Options
Antivirus Vendors in Operational Technology Market

SCADA Vendor	Primary AV Partner	Secondary AV Partner[6]
ABB	McAfee	Symantec
Emerson	McAfee	
GE	No Vendor Preference	
Honeywell	McAfee	Symantec
Mitsubishi	McAfee	
Rockwell	Symantec	
Schneider	McAfee	Cylance (New Announcement)
Siemens	McAfee	Symantec
Yokogawa	McAfee	

Does “No Vendor Preference” mean “No Vendor Support”?

Security Technologies in the SCADA Environment

- **AV Vendors** – Listed on Previous Page.
- **Network Switching Infrastructure** - Cisco Dominates as a Compatible Switching Infrastructure with one vendor providing their own hardened Switching product line.
- **Intrusion Detection Systems** – All vendors mention IDS (non-IPS mode) but only two vendors declare their support for a known product.
- **Log Management** – All vendors are agnostic about log management products as long as they use syslog forwarding.

Does “No Vendor Preference” mean “No Vendor Support”?

Implementation Differences in Security Technologies and Processes in the IT/OT Environments

- OT – AV Passive Implementation - AV Cannot Scan SCADA System Hard Drives.
- OT – IDS, not IPS – Choose not to Prevent any SCADA System Connections.
- OT – Signatures for AV and IDS must come through Intermediary.
- OT – Internet of Things – IOT in OT?.
- OT – OS and Application Patches go through very Rigorous Testing Process and Delivered via Intermediary.
- OT – Older ICS Protocols Inherently Insecure.

Does the Implementation Differences in Security Technologies and Processes in the IT/OT Environments Impact Cyber Resiliency?

Premise #1: The Smaller Supply of OT Security Technologies Contribute to the Difference in IT and OT Operations.

Conclusion – Logic Says that “Less is More”.

Premise #2: The More “Passive” Implementation of OT Security Technologies Contribute to the Difference in IT and OT Operations.

Conclusion – identical Security Posture Concepts, Substitute Security Risk for Performance Risk on the OT Side.

Premise #3: The Architectural Differences Between IT and OT Systems Contribute to the Difference in IT and OT Operations.

Conclusion – identical Security Posture Concepts, Substitute Security Risk for Performance Risk on the OT Side.

What are the Security Challenges in Cloud Deployments?

- What is Considered Cloud?
- Complexity of Cloud Implementations Including Data Accessibility, Access Controls, and Security Practices.
- Cloud Services may already be in use by Third Party Support Organizations – Software Development, Software Delivery, Patching, etc. All SCADA Vendors shown on slide 6 are already offering cloud services. (all shown on slide 6).
- Regulatory Agencies are Embracing Cloud to Help Lower Ratepayer Costs.
- What are the Pros and Cons of those Cloud offerings?

Do Cloud Implementations in IT/OT Environments Impact Cyber Resiliency?

Premise #1: Cloud Computing presents significant security challenges.

Conclusion – True, Utilities must have a clear understanding of cloud vendor security controls and to be able to extend their own control structure and governance to cloud vendors.

Premise #2: SCADA is not meant to reside in the Cloud.

Conclusion – SCADA is already in the Cloud, maybe not as a mainstream offering, but for some components. Water World states that Cloud services can save as much as 90% for a small entities. [7]

Premise #3: Cloud will become even more complex in the future.

Conclusion – Technical innovations will continue to drive cloud services. Regulatory changes will make governance even more important.

Project Management Methodology Differences in IT and OT Environments

- Project Management Methodologies for Large IT and OT Systems Projects are perceived to be different – IT more structured and OT more technical.
- Procurement Processes Include Cybersecurity Considerations
- SCADA Vendors are often Long Term Incumbents with an Established Relationship with the OT Staff.
- IT Application Testing Focuses on Documented Test Case Management Premise, OT Application Testing Focuses on Delivering Identical Results.
- In OT Environments, it is Common Practice to Operate in Parallel Production Environments for Months [6]

Do the Project Management Methodology in the IT/OT Environments Impact Cyber Resiliency?

Premise #1: New IT and OT Systems within the same Company follow different project management processes from scoping, designing, and acquisition.

Conclusion – Documentation from SCADA vendors confirm Industry accepted Project Management Methodologies are Employed [6]

Premise #2: OT SCADA Systems are Tested Longer than IT Systems Counterparts of same Criticality

Conclusion – IT and OT Applications have the same Application Test Period Lengths [7]

Premise: OT SCADA Systems are Paralleled Longer than IT Systems Counterparts of same Criticality

Conclusion – OT Applications have Significantly Longer Production Paralleling Period Lengths [7]

What are the Differences in IT versus OT Maintenance?

- Complexity of Endpoint Maintenance – Generator, Compressor, Solar, Nuclear, and Turbine.
- Lifecycle of OT Endpoint Devices Could Be Decades.
- Remoteness of Devices – Individual Devices Located in Remote Areas
- OT End Point Devices May Be Subject to Weather Extremes
- OT – Remote Access to SCADA Application is Very Controlled. In the IT Environment, Remote Access is Common.
- IT and OT – Primary Technical Support for Endpoint Devices often Involves a Third Party Organization Needing Remote Access.

Do the Maintenance and Support Differences in IT/OT Environments Impact Cyber Resiliency?

Premise #1: Complexity and age of OT Endpoint Devices Impacts Exacerbates the differences in IT and OT Systems Support.

Conclusion – SCADA Endpoint Devices may be Mechanical in Nature and Require Different Technical Skill Sets to Support. Older SCADA Endpoints may Still Use Deprecated Communication Protocols.

Premise #2: Location of OT Endpoint Devices Demand the need for Authorized Remote Access to SCADA End Points for Support Purposes.

Conclusion – Secure Remote Access is a Necessary Cyber Risk to Ensure the Safe Operations of Energy Delivery Systems.

Premise #3: Engaging Third Party Support Organizations to Monitor and Maintain SCADA Endpoints Dictates Secure Remote Access.

Conclusion – Third Party Support Organizations must Protect Their Networks to the Same Degree as SCADA Networks.

Security Training in Computing Environments

- Security Training of SCADA Technicians - SANS “The State of Security in Control Systems Today” (2015)[7]

  CISSP, CISA, or CompTIA 52%
  GICSP – 43%
  ISA99/IEC – 13%
  IACRB – 12%

  “IT security education is valuable, particularly with the converging technology trends, but it does not translate directly to ICS environments.” [7]

- ISACA Predicts a Global Shortage of 2,000,000 Cyber Security Professionals by 2019.[8]

Security Training in Computing Environments

Premise #1: More Cyber Security Training is Needed in SCADA Environments.

Conclusion – More Cyber Security Training is Needed, especially Related to Industrial Control Systems. Technicians need to take a Security First Focus.

Premise #2: Companies will face Increasing Challenges of Filling Cyber Security Positions.

Conclusion – Companies need to Devise Strategies to Attract and Retain Qualified Cyber Security Candidates, especially females.

Premise #3: The Industry will face Increasing Challenges of Filling Cyber Security Positions.

Conclusion – The Industry needs to Devise Strategies to Attract Qualified Cyber Security Candidates, especially females.

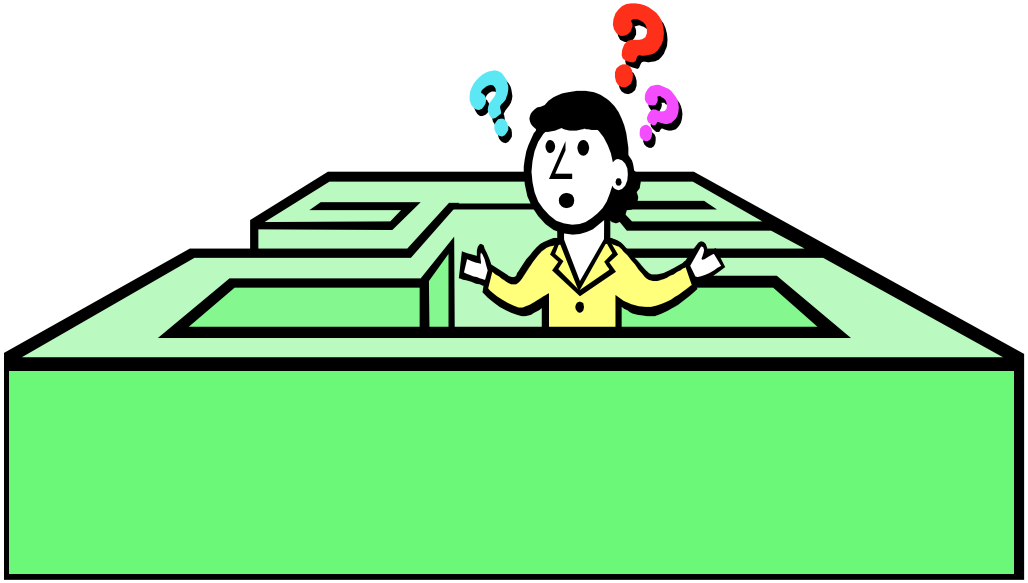
Other Differences in IT/OT Environments

- Regulatory – NERC CIP is extremely detailed relative to cyber security but only governs the Bulk Electric System and therefore only a small percentage of utility sites.
- Disaster Recovery – OT Devices can be expensive and location specific.
- Job Security – Is this divide “Self Induced”
- Budgets – Most Local Distribution Companies (LDC’s) are allowed a fixed rate of return and their budgets are determined during Rate filings. New Rate Cases may not be filed for years.
- Market – Utilities face Market Challenges as the Industry Transforms to Reduced Consumption/Lower Prices, Renewables, Lower Emissions, and the Digital and Transportation Revolution. [11]

Look to Institutional, Industry and Vendor Support

- Cloud Security Alliance – Press for an OT Domain focus. There are 34 CSA Domain Working Groups – none for OT.
- AGA/EEI – Press for an Cloud focus for OT.
- Cloud Offerings – Pros and Cons in an OT environment.
- OT Vendors - Encourage/Require SCADA Software, RTU, and PLC devices for testing for OT “certification”. Check on ICS Village.[13]
- New Technology – Programmable Automation Controller (PACS) and Cloud-sourced data – Raise new Cyber Security Challenges.
- Cloud Providers – How to obtain OT certified status such as exists for PCI Certified Vendors.
- How to attract female and minority candidates to fill cyber security job openings?

Questions?



Email me at: mguth@southernco.com

References

[1] https://www.gartner.com/it-glossary/operational-technology-ot

[2] https://en.wikipedia.org/wiki/Information_technology

[3] https://en.wikipedia.org/wiki/SCADA

[4] https://en.wikipedia.org/wiki/Internet_of_things

[5] https://www.crowdstrike.com/resources/reports/2018-gartner-magic-quadrant-endpoint-protection-platforms/

[6] https://metadefender.opswat.com/reports/anti-malware-market-share?_date=2017-02-27

[7] Individual SCADA Vendor Confirmations Available Upon Request – Mark Guth

[8] http://www.waterworld.com/articles/print/volume-28/issue-10/editorial-features/cloud-based-scada-alternatives-traditional-systems.html

[9] https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#6ba050595163

[10] SANS – State of Security in Control Systems Today. Derek Harp and Bengt Gregory Brown, June 2015

[11] https://www.velaw.com/uploadedFiles/VEsite/Resources/SummaryCIPVersion5Standards2014.pdf

[12] http://deloitte.wsj.com/cio/2018/01/19/2018-power-and-utilities-industry-outlook/

[13] https://www.automation.com/portals/factory-discrete-automation/programmable-logic-controller-plc/cybersecurity-industry-leaders-announce-launch-of-industrial-control-system-ics-village