DRAGOS

Nexus between OT and IT threat intelligence

Selena Larson

October 2019

About me

👩🏼‍💻 SELENA LARSON

- Cyber threat intelligence analyst at Dragos
- ICS cybersecurity
- Previously: Cybersecurity & privacy journalist

A Tale of Two Hackers

Financially-motivated hacker who executes ransomware attack

- **Adversary:** Cybercriminal
- **Target:** IT-focused business ops
- **TTPs:** Spearphishing, RobinHood ransomware, network propagation via psexec

Adversary interested in disrupting electric distribution

- **Adversary:** Sufficiently resourced, sponsored by entity who wants to further political means
- **Target:** Initial IT access to facilitate OT access
- **TTPs:** Spearphishing, customized malware, use of OT-specific devices and protocols

A Tale of Two Hackers

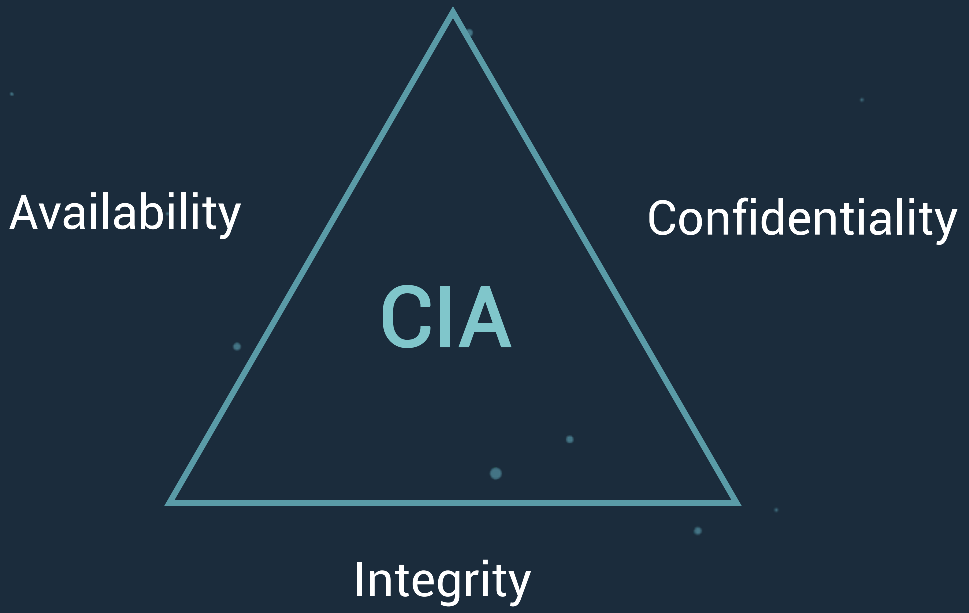
The way companies detect, respond to, and prevent attacks from each will vary based on environment, risk analysis, and business decisions.

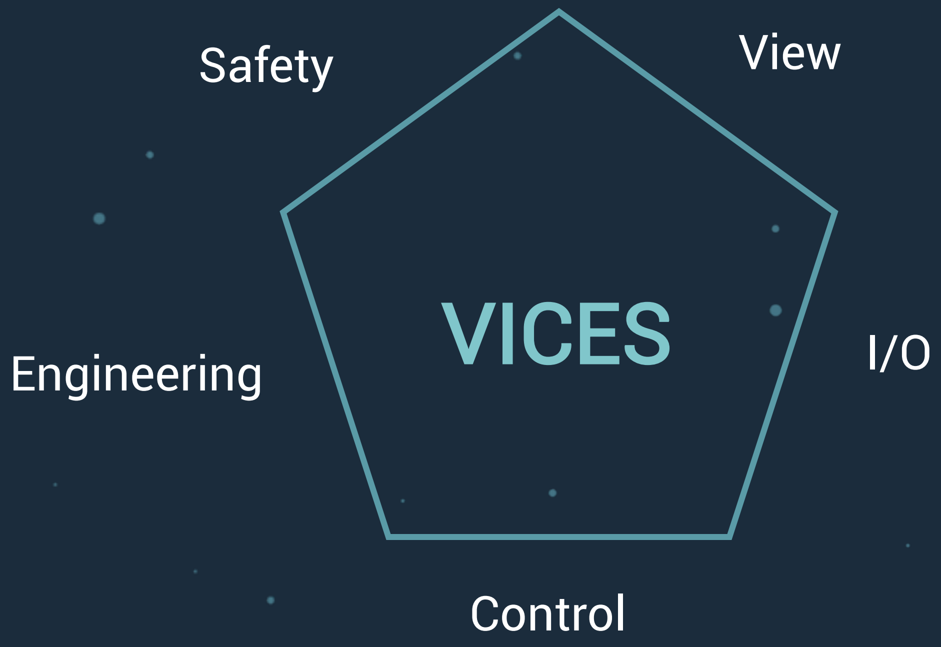
Defining OT

- OT: Operational Technology. OT should be thought of as mission critical IT in the ICS. It is the hardware and software that controls and monitors operations in an ICS environment like domain controllers and Windows PCs.

- ICS: Industrial Control Systems. An umbrella term for software and hardware that controls and automates industrial processes. ICS environments can include electric utilities, oil & gas, and manufacturing.

Cybersecurity Principles





Common myths/misconceptions

- ICS networks are airgapped
- OT staff don't care about security
- OT systems are easy to hack because we see them on Shodan
  - Seeing an HMI on Shodan doesn't indicate a vulnerability to an actual consequence

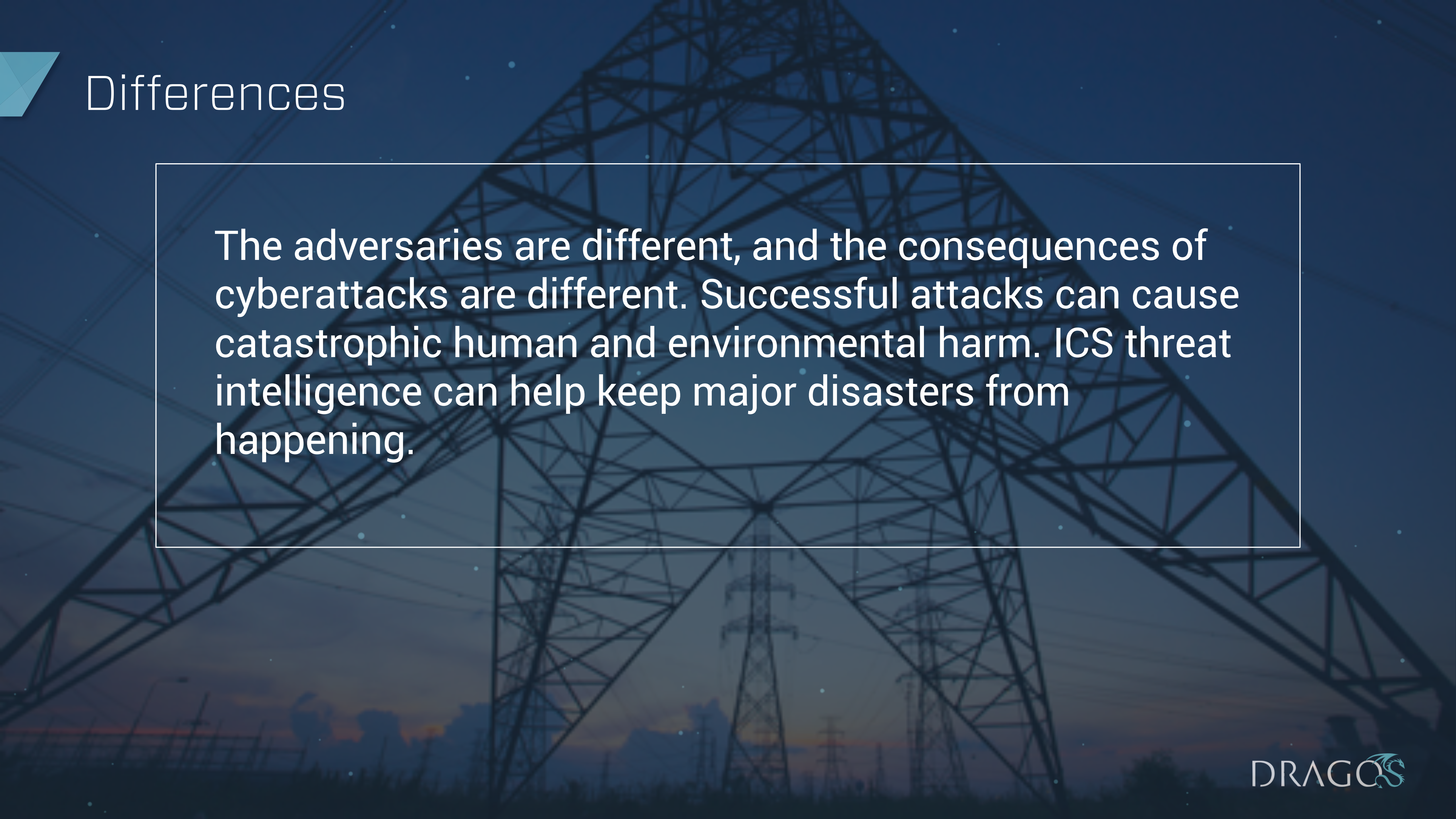
Similarities

Fundamentally, the goals of IT and OT threat intelligence are the same: obtaining actionable information on adversaries so defenders and organizations can reduce harm through better security decision making.

Similarities

- Some similar tactics, techniques, and procedures
- IT networks can be initial attack vectors
- Threats to IT networking infrastructure can impact ICS
- Engineering workstations (EWS), human machine interfaces (HMIs), data historians, OPC servers run Windows operating systems
- IT ransomware can infect and disrupt the OT

Differences



The adversaries are different, and the consequences of cyberattacks are different. Successful attacks can cause catastrophic human and environmental harm. ICS threat intelligence can help keep major disasters from happening.

Differences

ICS threat intelligence falls into three categories: Interested Adversary, Direct ICS Threat, and Indirect ICS Threat.

Interested Adversaries	Intelligence on activities of adversaries known to have an interest in control systems, operation networks, and ICS organizations Example: MAGNALLIUM targets oil and gas and energy firms. Recent activity includes uptick in password spraying following heightened tensions in the Middle East
Direct ICS Impact	Intelligence on threats directly affecting the operation of industrial control systems Example: TRISIS is a malware framework designed and deployed to disrupt oil and gas operations, targeting SIS
Indirect ICS Impact	Intelligence on threats not associated with industrial control systems but have a high likelihood of disrupting their operation Example: WannaCry and NotPetya ransomware do not target industrial control systems but their capabilities have shown to be debilitating to organizations if they access operational networks

Source: https://dragos.com/wp-content/uploads/Industrial-Control-Threat-Intelligence-Whitepaper.pdf

Differences

- Threat landscape is different
- OT has enterprise technology, but a lot of it requires specialized knowledge
- An adversary must maintain access and learn two different networks with specialized technology requiring specialized capabilities
- Components of threat intel might be the same (i.e. using IOCs and threat behaviors), however the behaviors themselves will be much different
- Decision-making calculus is different

Threat Landscape

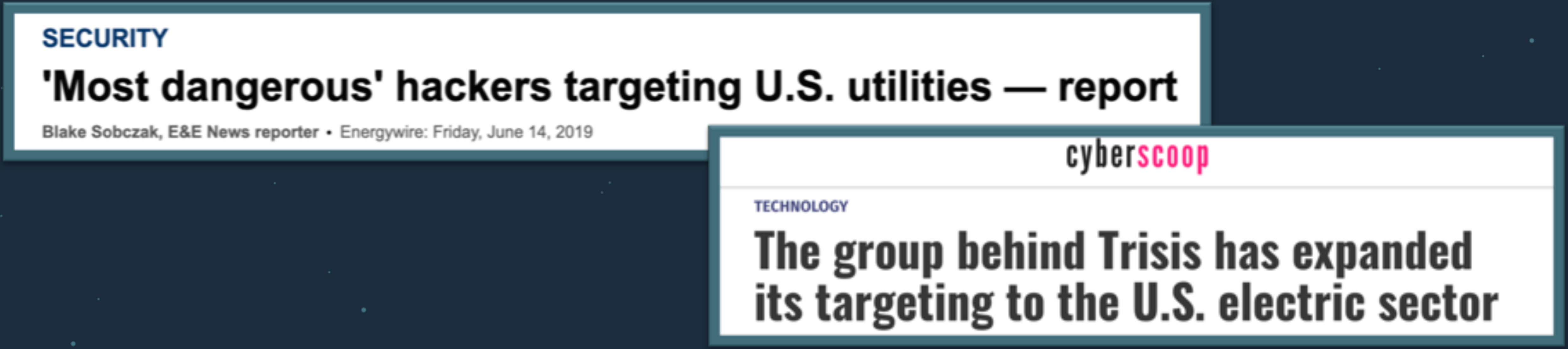
As our capabilities in threat hunting and identification of ICS-focused threats expand, we achieve greater visibility into the threat landscape and can create a more holistic picture of the threats, behaviors, and tradecraft affecting ICS environments.

Threat Landscape & Threat Surface

- 9 activity groups targeting ICS
- ICS-specific malware
- Supply chain and third-party access
  - OEMs, telecommunications
- Remote access, vendor access
- Systematic and input/output threats

Threat Landscape & Threat Surface

- Proliferation of threats
  - Similar to physical weapons proliferation, threats are spreading in the cyber realm, too.
  - Caused by increasing government investment in offensive cyber capabilities and ability to disrupt critical infrastructure.
  - Easier to obtain resources and skills necessary for a disruptive cyber-physical event.



SECURITY

'Most dangerous' hackers targeting U.S. utilities — report

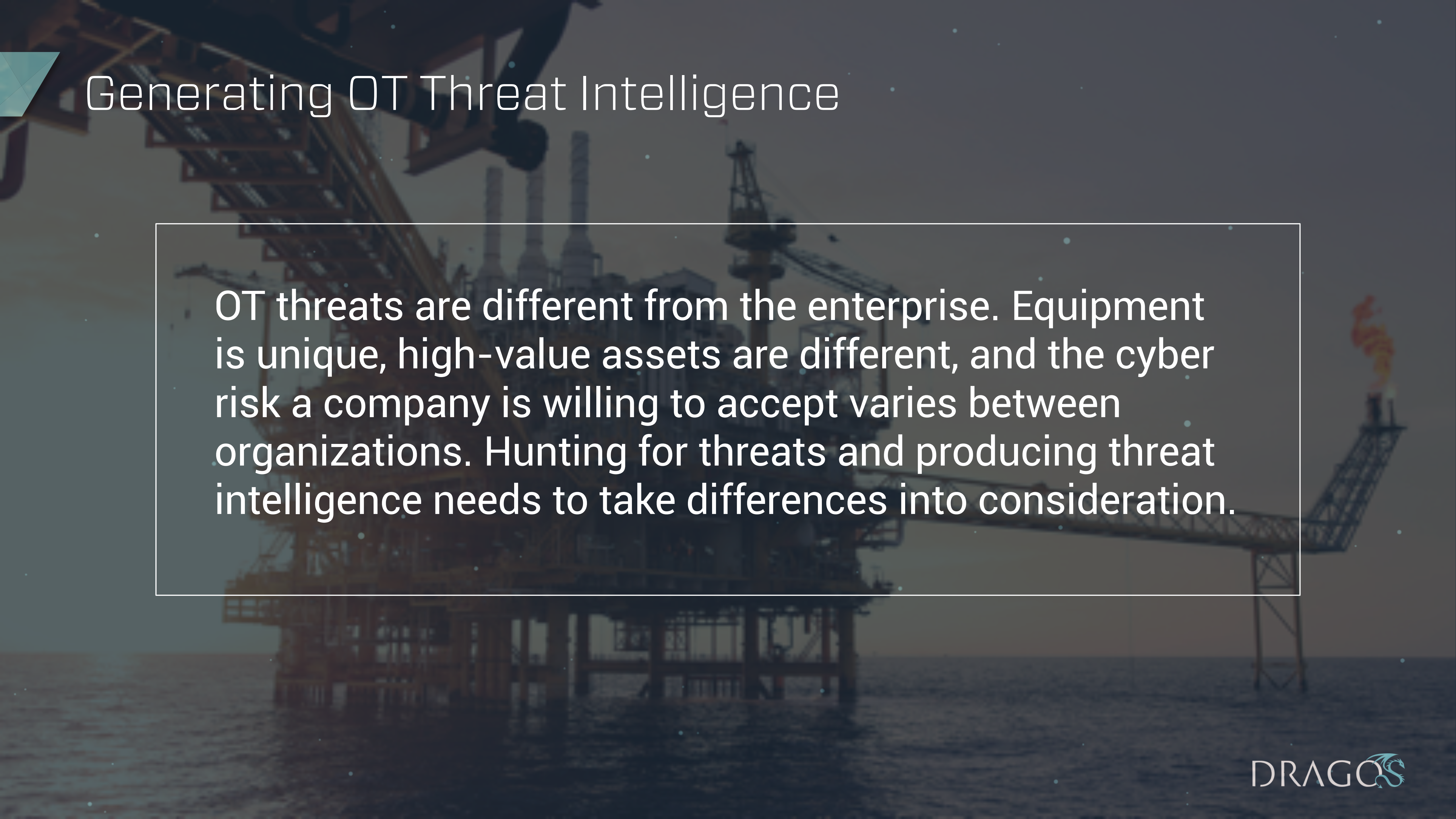
Blake Sobczak, E&E News reporter • Energywire: Friday, June 14, 2019

cyberscoop

TECHNOLOGY

The group behind Trisis has expanded its targeting to the U.S. electric sector

Generating OT Threat Intelligence



OT threats are different from the enterprise. Equipment is unique, high-value assets are different, and the cyber risk a company is willing to accept varies between organizations. Hunting for threats and producing threat intelligence needs to take differences into consideration.

Generating OT Threat Intelligence

- High-value assets (“Crown Jewels”) vary by industry and company. And so do the motivations for attacking them.
  - Data historians, chemical processing, safety controls
- Develop a hunt hypothesis based on an understanding of adversary's behavior.
  - If I increase the number of third-party service providers with access to my OT network, then this will provide adversaries additional avenues of access to my sensitive processes.
    - Identify third-party service provider and vendor relationship connections as a starting point for detecting potentially malicious activity.

Generating OT Threat Intelligence

- Develop sufficient data sources and visibility
- Understand the audience and be aware of context to make threat intelligence relevant
- Understand customer environments and operational requirements to make useful recommendations
    - e.g.: Vulnerability scanning can break the OT; endpoint detection doesn't exist or isn't supported
- OT threat intelligence should help IT understand threat impact and context
- Understand outside factors: Attacks on ICS entities like oil and gas or electric utilities can be used to further political, economic, and national security goals

Operationalizing OT Threat Intelligence

1. Goals of threat intelligence are largely similar for IT and OT threat intelligence practitioners
2. Attacker capabilities, motivations, and attack surface vary between IT and OT targeting adversaries
3. Security decisions within the IT and OT will be made differently, even if based on the same intelligence
4. It takes everyone working together to make ICS entities – and the communities they operate in and support – safer and more secure

References & Resources

- Industrial Control Threat Intelligence – Sergio Caltagirone, Dragos (https://dragos.com/wp-content/uploads/Industrial-Control-Threat-Intelligence-Whitepaper.pdf)
- Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE – Joe Slowik, Dragos (https://dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf?hsCtaTracking=25456437-61c7-415a-ab14-7ec85e60babb%7Cef8df52d-ed60-405b-929a-df2b1b05dbdc)
- Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies – US Department of Homeland Security (https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf)
- Ransomware isn't just a big city problem – Malwarebytes (https://blog.malwarebytes.com/ransomware/2019/05/ransomware-isnt-just-a-big-city-problem/)
- 'Most dangerous' hackers targeting U.S. utilities — report – E&E News (https://www.eenews.net/stories/1060575609)
- The group behind Trisis has expanded its targeting to the U.S. electric sector – Cyberscoop (https://www.cyberscoop.com/trisis-xenotime-us-electric-sector/)
- Confessions of an IT / OT Marriage Counselor – Lesley Carhart, Dragos (DerbyCon 2019 presentation)
- Risks Posed by Firewall Firmware Vulnerabilities – NERC (https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf)
- Two sides of IT vs. OT Security and ICS Security Operations – Robert M Lee, Dragos (https://dragos.com/blog/industry-news/two-sides-of-it-vs-ot-security-and-ics-security-operations/)

DRAGOS

Thank you

@selenalarson

DRAGOS