FORESCOUT

Drinking the ICS Jolt Cola:

Jumpstart Your NIST CSF Maturity

Brian Proctor & Sandeep Lota

January 23, 2020

S4x20

About the Presenters

Brian Proctor

Director of Strategic OT Accounts

Operational Technology

- 13 years experience as asset owner securing and operationalizing security technologies in OT environments
- Forescout OT customer from 2014-2017
- Original member of SecurityMatters Team (now Forescout OTBU)
- IEEE author "Passive Real-time Asset Inventory Tracking and Security Monitoring of Grid-edge Devices”
- GICSP, CRISC, CISSP
- Oversee the largest and most strategic OT deployments in the US

Sandeep Lota

Sr. Systems Engineer

Operational Technology

- Almost 25 years experience designing and architecting infrastructure system breakthroughs
- Senior network security expert, supporting national and international projects for the world’s largest companies.
- As Sr. Systems Engineer at Forescout, he designs and architects transformative network and security infrastructure solutions.
- Instructor for several advanced networking and security courses
- Holds many active & advanced certifications from well-known hardware and software vendors, including Cisco, Palo Alto Networks and VMware.

Agenda

Jumpstart Your OT Cybersecurity Maturity (with NIST CSF)

Trends in the Field

Future-Proofing Your OT Security Investments

Trends in the Field

Asset owners now desire both active and passive capabilities

Field and plant operations teams want tools that improve reliability, shorten root cause analysis, and help with real-time monitoring

Asset owners' requirements focus is shifting to scaling and automation

Bi-directional integration with enterprise technologies

Leaders are maturing their OT capabilities beyond just detection and response and focusing on building a comprehensive set of capabilities across all NIST CSF domains like Identify, Protect, and Recover.

NIST CSF Focus Shift

Identify (ID)

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities

INDUSTRY LEADER USE CASES

- Triangulate physical device locations at any point in time
- Crowdsource asset classification for improved accuracy and diversity
- Expedite and automate risk assessment process, tailored to asset owner's risk methodology
- Maintain up-to-date asset inventory and baseline for serially connected assets

How to Jumpstart with Forescout

- Ability to leverage integrations with your existing network infrastructure devices and ingest telemetry in real time
- Device Cloud – An opt-in service allowing access to our device classification database with 11M+ device classifications and counting
- Automated security and operational risk score calculations and notification workflows
- Configurable and customizable risk scoring engines
- Ability to passively or actively obtain inventory and baselines for serially connected devices

NIST Cybersecurity Framework, https://www.nist.gov/cyberframework

INDUSTRY LEADER USE CASES

- Continuously assess device security posture and control what's allowed on OT network segments in real time
- Automate response actions if a device fails any policy condition. For example, transient device policy and rogue device detection.
- Ability to simulate and validate device segmentation
- Automate and audit OT segmentation enforcement when ready

NIST Cybersecurity Framework, https://www.nist.gov/cyberframework

Protect (PR)

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services

How to Jumpstart with Forescout

- Agentless capabilities allow only approved and secure devices to connect to OT network segments based upon combinations of device characteristics and security posture as defined by policy
- Based upon asset owners' policies, continuously check each device's posture
- Integration with other security technologies to automate response actions
- Graphical representation of network flow matrix by device classification and networks
- Ability to simulate and/or automate segmentation

INDUSTRY LEADER USE CASES

- Focused on TTPs and mapping to MITRE/kill chain
- Automated ingestion of threat indicators/feeds into OT detection solutions
- Analyze previously collected OT analytics data for newly discovered TTPs and indicators
- Find unknown threats via detection of malformed messages or protocols

NIST Cybersecurity Framework, https://www.nist.gov/cyberframework

Detect (DE)

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event

How to Jumpstart with Forescout

- Largest Industrial Threat Library dating back to 2008
- Feed STIX indicator messages into detection engines directly
- Leverage our threat analyst rewind capability to review previously collected OT analytics
- Malformed packet engine can detect previously unknown threats and protocol exploit attempts
- Ability to customize threat hunting capabilities by leveraging our extensible framework

Respond (RE)

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event

INDUSTRY LEADER USE CASES

- Bi-directional integrations with other security technologies to enable quick threat response
- Ability to enrich OT alert data with IT data sets
- Automate responses to threat or alert conditions, trigger workflows upon policy violations
- Reduce response time for the investigation of suspicious alerts and alarms

How to Jumpstart with Forescout

- Platform supports bi-directional integrations with 70+ security vendors
- Real-time IT and OT visibility, device status, and device health telemetry allow for the fastest anomaly correlations possible
- Seamless dynamic segmentation across all zones upon policy violation that can be automatic or manually enforced
- Ability to share real-time data with other blocking, enforcing, or alerting technologies

NIST Cybersecurity Framework, https://www.nist.gov/cyberframework

INDUSTRY LEADER USE CASES

- Automate deployments and upgrades for OT security products
- Create asset baselines and profiles for each device and understand both inbound and outbound communications
- Ability to historically examine and analyze device versions and vulnerabilities

NIST Cybersecurity Framework, https://www.nist.gov/cyberframework

Recover (RC)

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

How to Jumpstart with Forescout

- Leveraging container virtualization technology to expedite deployments and upgrades
- Understand and visualize traffic flows and trends out-of-the-box
- Validate consistency and accuracy of device inventories and states in real time
- Have an audit log of device firmware and software changes, understand and identify potential roll back points

Recommendations for Future-Proofing Your OT Security

Identify solutions that increase maturity scores across all NIST CSF Functions

Start strategizing on how to better segment flat OT networks

Implement impact-based, automated security and operational risk scoring

Choose cross-functional platforms that provide a common operating picture across all business lines

THANK YOU

Brian Proctor | brian.proctor@forescout.com | @brianproctor67

Sandeep Lota | sandeep.lota@forescout.com | @jedi443