INTRODUCING A “VITAL” NEW CONCEPT FOR ICS CYBERSECURITY PROGRAMS

SANS ICS Summit

Brian Proctor & Chris Triolo
3/18/2019
About the Presenters

**Brian Proctor – GICSP, CISSP, CRISC**
Director, OT Strategic Accounts

- 13 yrs. experience as asset owner in cybersecurity
- Electric utility and gas pipelines background
- Engineer, architect, research and development
- Employee #4 in US for SecurityMatters
- SilentDefense customer from 2014-2017
- Work with strategic OT accounts for Forescout

**Chris Triolo**
VP, Customer Success

- More than 20 years in information security industry
- CISSP
- Background includes Federal and DoD, and commercial customer environments
- Deep experience with security operations center build-outs, security analyst training, and monitoring and incident response processes
- Led SOC Build Service Offering for HP ArcSight, established 65+ SOCs from ground-up, assessed and consulted on 100+ others
Why Are We Here Today?

To talk about how our Virtual ICS Threat Analyst Logic (VITAL) solution helped solve ICS cybersecurity challenges for a large energy provider that:

1. Needed situational awareness to detect cyber and operational threats to ensure the availability and safety in their ICS networks

2. Needed 24x7, continuous, automated security monitoring in un-manned environments.
CHALLENGE #1

OT Network Visibility
Challenge #1: OT Network Visibility

**Cybersecurity**
- No (to limited) visibility in OT networks
- Inability to discern if systems are vulnerable
- Lack of ICS analytics and contextual information in enterprise security platforms
- Slow and expensive threat detection and response time in ICS/OT

**Networking**
- No network maps
- No segmentation
- Inability to monitor and understand packet/traffic flows
- Lack of device compliance (Is my switch configured correctly?)

**Operations**
- No real-time asset inventory
- Inaccurate tracking device firmware and model information
- Incomplete vendor and contractor activities
- Costly and time-consuming site visits to field
Our Solution: **SILENTDEFENSE™**

**Achieve Complete ICS Visibility**
- Gain Control over OT Network
- Specific Passive Technology
- Risk Mgmt. & Compliance

**Proactively Manage Cyber Threats**
- Detect Cyber & Operational Threats
- Detailed Alerts for Effective Incident Response
- Automated Processing

**Integrate Across the Enterprise**
- Real-Time Asset Inventory
- Complete Situational Awareness
- Vulnerability Management
- Change Management
SilentDefense: What It Achieves

- Provide deeper visibility into OT and ICS environments
- Deliver unified OT risk management and compliance support
- Enable dynamic ICS network segmentation
- Automate rapid detection and incident response for OT

Expanded capabilities and advanced features to secure industrial environments.
CHALLENGE #2
Automated Security Monitoring
Challenge #2: Automated Security Monitoring

Security operations is challenged with its “people-first” design.
COMPLEX THREATS
LACK OF BUSINESS CONTEXT
HUMAN FACTORS
VOLUME AND SCOPE
LIMITED USE CASES
ANALYST SCARCITY AND RETENTION
Challenge #2: Automated Security Monitoring
120+ SOC Analysts Surveyed

Activity rankings across perceptual dimensions

- **Enjoyment**
  - Hunting
  - Forensic
  - Intel
  - Intrusion
  - Response
  - Training
  - Proactive
  - Collaboration
  - Monitoring
  - Tools
  - Shift Ops
  - Reporting

- **Expertise**
  - Hunting
  - Forensic
  - Intrusion
  - Intel
  - Response
  - Training
  - Proactive
  - Collaboration
  - Monitoring
  - Tools

- **Value**
  - Response
  - Forensic
  - Intrusion
  - Intel
  - Hunting
  - Proactive
  - Collaboration
  - Monitoring
  - Tools
  - Reporting

- **Dynamic**
  - Hunting
  - Forensic
  - Intrusion
  - Intel
  - Response
  - Proactive
  - Collaboration
  - Tools
  - Shift Ops
  - Reporting

- **Resources**
  - Hunting
  - Forensic
  - Intrusion
  - Intel
  - Response
  - Proactive
  - Collaboration
  - Tools
  - Reporting
  - Hunting

- **Time**
  - Monitoring
  - Intrusion
  - Shift Ops
  - Response
  - Collaboration
  - Tools
  - Intel
  - Reporting
  - Training
  - Proactive

Voice of the Analyst Survey, 2018, Cyentia Institute
Our Solution:

AUTOMATES SECURITY MONITORING AND TRIAGE

ANALYZES SECURITY ALERTS FROM INDUSTRY’S TOP DETECTION TOOLS

ESCALATES MALICIOUS AND ACTIONABLE SECURITY INCIDENTS

1st Security Operations Virtual Analyst

Delivers vetted incidents to speed response and resolution
Respond Analyst Reasoning: How It Works

Respond Analyst considers all factors in parallel to make a decision, and getting smarter.

**PRIORITIZE**
- Business impact? Escalate to Incident response?

**THE ATTACK**
- How does it work? Relevant?
- New? Exploit the system?

**SCOPE**
- Related to other attacks? Attack duration?

**INTERNAL**
- Asset type? Function?
- Criticality? Vulnerable?

**PATTERNS**
- Legitimate? False positive?
- Automated? Historical?

**EXTERNAL**
- Whois? Known bad?
- Business here? Partner?
Respond Analyst Reasoning: How It Works

Respond Analyst considers all factors in parallel to make a decision, and getting smarter.

Bayesian probability **predicts**
Conditional probability **contextualizes**
Graphical modeling **relates causality**
Machine learning **learns**

Example: Graphical Modeling
RESPOND SOFTWARE + SILENTDEFENSE

The VITAL Solution
Use Case

Mutual customer seeking automated monitoring for ICS environment.

- Respond Analyst for ICS developed with SilentDefense as the core event feed.
- SilentDefense’s rich capability to identify OT-specific security issues helps ensure suspicious activity is detected and reported to the Respond Analyst.
- Respond Analyst’s decision engine analyzes each alert to prioritize and notify on malicious incidents.
SilentDefense Deployment

- **Control Center**
  - Servers and HMIS
  - SilentDefense™ Command Center
  - Workstations
  - Network Switch

- **Other Networks**
  - Other networks (e.g., corporate, secondary control centers, …)
  - Gateway / Firewall

- **Other Stations**
  - Measurement Station
  - Sensors
  - Actuators

- **Sensors**
  - e.g. OPC, proprietary protocols

- **Actuators**
  - e.g. IEC104

- **Field protocols**
  - Gateway / Firewall

- **SILENDEFENSE™ Monitoring Sensor**
  - Pipeline
Respond Analyst Deployment

PGO – Intelligent Decision Engine

Case Builder (Gather Facts)  Knowledge base (Retain tribal knowledge)  Models (Determine outcomes)

Analyst Server

Selective Data Extraction  Tokenization  Sensitive Reference Checks

External Context

Threat Intel Lists  VPN Lists  TOR Exit Nodes  Geolocation Data  STIX/TAXII integration  Known Bad Hashes  WHOIS

User interface

Incidents  Feedback

Event Data  Company Context  Integrations

SilentDefense  Active Directory  Incident Response Management
IP/IDS  IP address ranges/zones  IT Ticket Management
EPP/AV  Critical Assets & Accounts  SIEM’s
Vuln. Scans  Asset classification  Notification
Web Proxy/Filter  Whitelists  EDR
EDR

Knowledge base (Retain tribal knowledge)

Models (Determine outcomes)
Respond Analyst + SilentDefense Functional Architecture
The Results

Visibility and threat detection in ICS network

Contextual asset information and alerts

Automated, 24x7 deep analysis of events, without the need to staff humans

Accurate escalation of security incidents in ICS environment

Context of the OT environment is applied to intrusion analysis models
THANK YOU