TSYS® People-Centered Payments

TSYS Threat Management Center

Lessons shared from the road

Jody Lee
CISO, TSYS

TSYS - What We Do and Where We Are

~ 400
Clients Around the World

>80
Countries Where TSYS Does Business

>15 Billion
Enterprise-wide Transactions

> 8,700
Team Members

TSYS Security Operations Center

- Created 7 years ago as 1st attempt at dealing with security events
  - Served primarily as a service desk function
  - Light 2nd and 3rd shift coverage primarily for International incidents
  - Responsibilities included:
    - Password resets for privileged systems
    - Firewall policy pushes (validation done by another group)
    - Remote access troubleshooting
    - SPAM and email quarantine management
    - Limited vulnerability management activities
    - Security device availability monitoring
    - Manual intrusion monitoring and report reviews
  - Projecting 3 major screens for 15+ security consoles

The Problem: *Too many screens, too many events, too few eyes, and no correlation*

TSYS®

TSYS Security Operations Center

- Firewall Log Console
- SNMP Console
- Wireless IPS Log Console
- Intrusion Prevention Console
- Service Desk Call Management Console
- Web Application Firewall Console
- Remote Access Log Console
- …and more

SOC Security Analysts
(single coverage exits across 1st, 2nd, and 3rd shifts)

Unable to detect actionable events across multiple security consoles among millions of log events

TSYS®

SIEM – The Journey

- **Our Solution**: **SIEM**
  - Single Pane – centralized, holistic view of security event data
  - Correlated security data to create **Actionable Intelligence**
- Making the Initial Investment
  - Define the Vision - create your plan and stick to it
  - Don't waste a "Good Crisis;" Timing is Everything
  - Create a Business Case that Exec Management Can't Deny
  - As with any negotiation, start with your maximums
  - Let Exec Mgmt know, you will be coming back to the well
  - Show the value, even if it scares them a little
  - Oversize the deployment - integrated systems are very chatty
  - Invest in professional services and training

(SIEM): Centralized, holistic view of correlated security event data to produce Actionable Intelligence.

TSYS®

SIEM – The Journey

- The Rollout
  - Include Operations and Network teams in the planning
  - Market Log Management as a Service
  - Don’t use PCI as the driver, but you may need it as a hammer
  - Bandwidth use can be heavy; stay close with network team

- Correlation
  - Get creative on use cases - Think like a bad guy
  - Include areas not traditionally Information Security
  - Don’t let excitement result in scope creep
  - Prioritize the Use Cases and Focus only on actionable events

TSYS®

Today: TSYS Threat Management Center

- APT Event Data
- Firewall Event Data
- Network IPS Event Data
- Wireless IPS Event Data
- DLP Event Data
- Antivirus Event Data
- Web APP Event Data
- RAS Event Data
- HR Event Data
- Proxy Event Data
- …and more

Correlated Events

Enterprise SIEM Main Channel Console

(ACTIONABLE EVENTS)

Priority 1 Severity Events
Priority 2 Severity Events
Priority 3 Severity Events

TMC Organizational Structure Changes
(Additions: Daytime Mgr, After-hour Mgr, 6 SIEM Analysts)

The Result : *Single pane, correlated and prioritized actionable events, and removal of non-threat monitoring*

TSYS®

TSYS Lessons Learned

- SIEM was the right Solution to our Problem, but…
  - The SIEM technology surpassed TMC team member ability.
    - We had to invest time and money into training after launch.
  - SIEM needs investment in process/procedure development
  - SIEM needs continued investment (storage capacity, increased licensing, training, professional services, etc.)
  - SIEM needs engineering care and feeding
  - SIEM identified Operational cleanup opportunities
  - SIEM generated enough questions to staff a Forensic Team
- SOC was rebranded as a Threat Management Center
  - Removed responsibilities from TMC that were not threat related
  - Changed organizational structure to support new processes
  - Increased staffing levels to manage volume

TSYS Information Security

- Questions?

Thank You!