Threat Detection & Response
Control Point Management

Developing a Visibility and Measurement Platform that Manages and Improves Operations

Nancy Thompson
Director of Operations
“After careful consideration of all 437 charts, graphs, and metrics, I’ve decided to throw up my hands, hit the liquor store, and get snockered. Who’s with me?!”
Agenda

- Approach
- Resulting Approach Complexity
- Solution Challenges
- Results
Addressing the Lockheed Martin Cyber Kill Chain®

- **Advanced Warning**
  - External intel
  - System probes
  - Phishing

- **Infiltration**
  - System exploitation
  - Malware

- **Escalation**
  - Account hijacking
  - Privilege escalation
  - Lateral movement

- **Exfiltration**
  - Data transmission &
  - theft

**Timeline**

1. Weaponization
2. Delivery
3. Exploitation
4. Command & Control
5. Actions on Objective

**Cybersecurity Phases**

- **Reconnaissance**
- **Delivery**
- **Installation**
- **Exfiltration**

**Duration**

- **DAYS**
- **WEEKS**
- **MONTHS**
Resulting Complexity

**Cyber Risk Defense Center (CRDC)**
- Executive Security Intelligence Briefings
- Security Oversight

**Threat Management & Governance**
- Service Level Management
- Operational Efficiency (Workflow)
- Analytics & Reporting
- Escalation

**Governance**
- Projects
- Security Admin
- KP-IT
- SOG Team

**Run**
- Content Engineering
- Use Case Design
- Policy Engineering
- Remediation Governance
- CERT
- Forensics
- eDiscovery

**Build**
- Security Device Data
- Aggregate Security Events
- Event Data (Int./Ext.)
- Custom Rules
- Event Patterns
- Reporting Data Warehouse
- Correlation Vendor APIs

**SOC Platform Components**
- SIEM
- Ticketing & Workflow
- Business Intelligence
- Sec-Intel Feeds
- Security Platforms
- Big Data

**SOC Data Sources**
- Logs (Transactional)
- Unstructured (Big Data)
- Network Hierarchy & Design
- Asset & Data Classifications
- Business Data from Structure & Geography
- Threat Intelligence

Legend:
- C-DC
- IT / Corp
## Solution Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process flow flexibility</td>
</tr>
<tr>
<td>Ability to add in “control points” where we needed them</td>
</tr>
<tr>
<td>Dashboards which manage work, issues &amp; offer visibility to operations</td>
</tr>
</tbody>
</table>
Control in management means setting standards, measuring actual performance and taking corrective actions.

### Control (management) Characteristics

- Control is a Continuous Process
- Control is Forward Looking
- Control Helps to Achieve the Standard

### Control (management) Process

- Setting, Measuring & Comparing Performance Standards
- Analyzing Deviations
- Take Corrective Measures
Solution Challenges

CALL

Incident

Resolve

Close

Governance

Risk

Compliance

Agile Development

Demo Release

Develop Functionality N

Integrate and Test

System Testing

Client’s Feedback

Make Changes

All Functionalities Complete?

Yes

No

Next Iteration

Develop Functionality 1

Develop Functionality 2

Integrate and Test

Integrate and Test

© 2015 Kaiser Foundation Health Plan, Inc.

Technology Risk Office
Results
Evolution of the Threat Activity Case

December 2014

March 2015

April 2015
Components of Operations

- Input
- Team Checklists
- Non-Actionable Events
- False Positives
- Actionable Events
- Critical Events
- Incident
- Child Processes
  - Remediation Request
  - Use Case Request
  - Tuning Request
  - Policy Engineering Request
Team Control Point - Checklists

Customized Forms
Help Boxes
Links to Processes (ePO process in sharepoint)

Lateral Movement Checklist
- ePO Checked? *
- FireEye Checked? *
- PCap obtained from all relevant NetScout Interfaces? *
- Tanium Checked? *
- TippingPoint Checked? *

EnCase
- EnCase Checked? *
- EnCase Cyber Checked? *

Qradar
- QRadar Events Exported? *
- Exported QRadar Events
- QRadar Related Events Exported? *
- Exported QRadar Related Events

An asterisk (*) indicates a required field.
If an escalation is rejected by Incident Handlers 2 or more times, leadership is notified.

**ACTION REQUIRED: Team Conflict Notification - TAC: 2799 - SANS Test**

*alert* to: Brian McNelly
Please respond to alert

Leaders,

The TAC listed below has been escalated to the KCERT team and rejected 2 or more times. Please follow up with the team members below to resolve this conflict.

**REQUEST SUMMARY**
Request #: 2799
Request Name: SANS Test
Requested by: Brian McNelly
Rejected by: Jon Jack
Rejected Reason: This does not meet the minimum criteria of an incident as there is no PHI or PHI accessible by or on the machine.

To view the details of this request click the following link:
https://k...
Audit Control Point - Closure and Feedback

Audit Closure

% Audit closure form here.

Analysis

Incident Closeout Description *

Closed Reason *

Is an After Action Report Required? *

Lessons Learned Review Required? *

An asterisk (*) indicates a required field.
Not All Actions Completed

There are still action items open related to this incident. Select the Submit button at the bottom of this form to return to the Actions task.
An asterisk (*) indicates a required field.

TAC: PHI Error

You selected PHI/PII is at risk on the Intake form but selected a type of case other than Incident.

You have two options to correct this issue:
1. Return to Type of Case and select Incident
2. Return to TAC Intake and modify your "PHI/PII at Risk?" answer

What do you want to change? Type of Case
An asterisk (*) indicates a required field.
**What’s Next**

<table>
<thead>
<tr>
<th>Input Work Integrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dispatch System Integration</td>
</tr>
<tr>
<td>Dynamic Visualization Tools</td>
</tr>
</tbody>
</table>
Questions?

“Thompson, great job...you’ve delivered the wedding cake!”