Cyber Defense Center
To Infinity and Beyond

Nicholas Slaughter
Manager, Strategic Transformation Service
Introduction

- What is a Cyber Defense Center?
  - How is it different from a traditional SOC

- How have we assisted past clients in building or maturing their incident response organizations?

- How can Mandiant assist your SOC?
  - Maturation of existing services
  - Transformation guidance through partnerships
  - FireEye tool usage and enhancements
NICHOLAS SLAUGHTER

Cyber Defense: Center Service Line
Manager, Strategic Transformation Services
Operationalizing Security Is Difficult

- Too Many Alerts
- Detection Efficacy
- Inconsistent International Policy
- Rapid Evolution of IT
- Increasing Complexity of Threats
- Increasing Consequences
- Talent Shortage
- Security Vendor Management
Solution Overview

- Mandiant’s transformation services are designed to work with all clients, regardless of size or industry.
- Focus is on breaking through the **maturity barrier** and moving to a proactive security posture.
- Solutions are tailored based on your specific needs, not “one size fits all” solutions.
- Combination of tools, threat intelligence, process, and expertise.

- **Sectors we’ve worked in:**
  - Retail
  - Healthcare
  - Federal
  - State, Local, and Educational
  - Critical Infrastructure

- **Client Sizes range from 1,000 employees to over 350,000.**
The Maturity Barrier Challenge
Overcoming Complacency and Insurmountable Odds

- Basic or no documented IR Plan or Processes
- Tool-based approach to Security Ops
- Little or no Dedicated Security Staffing
- Compliance-driven decision making

Foundational

Evolving

- Fully Intelligence-led Risk-based decision making
- Active Threat Hunting

Resilient

- 24x7x365 fully investigation capable (Forensics and Malware)
- Self-Evolving
Mandiant will design and develop solutions based on the unique challenges of our clients to meet their needs.

Using a combination of technology, personnel and processes, Mandiant will implement the developed solutions and will provide testing methods to ensure effectiveness and identify improvements.

Understanding that there is a difference between effectiveness and maturity, Mandiant focuses in understanding the strengths and weakness of existing capabilities.
Cyber Defense Center Development

Helping our clients **build new capabilities** and
**mature their existing capabilities**

**THE MANDIANT DIFFERENCE**

- Trusted Advisor
- Experience & Expertise
- Tools
Expertise On Demand is a prepaid, annual subscription that provides flexible, pay-per-use access to FireEye’s industry-recognized security expertise and threat intelligence.

**CDC Service**

EOD units for services such as:
- Use case review
- Playbook development

**Intelligence Access**

- Daily intelligence news analysis
- Quarterly threat briefings
- Digital threat assessment
Working With Helix

Mature Helix customer programs to a proactive posture

- Develop hunt books
- Federated dashboard development
- Automation and integration
- External intelligence feed contextualization
Verodin inclusion allows for focus on transformation validation

- Provide validation of technical controls
- Continuous testing to validate transformation
- Real-time feedback on prevent/detect tech
- Detection allows for increased response drive
Cyber Defense Center Transformation a Case Study

Developing a Unified Incident Management Framework
Scenario

- Client Information:
  - Approximately 200,000+ endpoints globally
  - Financial sector with domestic and international regulatory, compliance, and data residency considerations
  - New CISO entering into the organization

- Client challenge:
  - Otherwise traditional SOC broken into multiple disparate organizations, each with their own processes and tools

Mission

Combined two separate Incident Response Organizations into a single Unified Incident Management framework
Expanding on the Challenges

- SOC broken into two functions
- First function as BAU ticketing (T1 and T2), the second was special investigations (T3)
- Lack of communication
- Investigations not performed in tandem
- Disparate technology stacks
- Disparate ticketing systems
## The End State Goal

<table>
<thead>
<tr>
<th>Objective</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Combine the two separate IR groups with a focus on their individual requirements</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Evaluate, identify, and design unified framework tools and technologies</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Develop unified processes – CDC intake process, investigations, major incident management, etc.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Test the newly developed incident management framework</td>
</tr>
</tbody>
</table>
The Unification Process

- Assessments to identify strengths & opportunities for improvement
- Develop unified incident management blueprint detailing how the two organizations will be merged
- Provides evaluation, design, and tool recommendations

- Clear roadmap on what each unit brings to the table
- Identify needed changes to technologies, personnel, and process
- Recommendations and support developing justification for new tool acquisition
Taking your SOC to Infinity and Beyond
Mandiant Cyber Defense Center Development

- Focus on Maturity & Operational effectiveness
- Partnership with embedded dedicated personnel resolve your challenges
- Focus on better understanding the underlying challenges to make better solutions
- Technology agnostics
Questions????
THANK YOU