Operationalizing Threat Intelligence

Technical Operations & Program Integration
Cyber Defense Centre Consulting – who we are

**Practice Background**
- Established in 2012
- Designed 25+ CIRT Teams
- Assessed 50+ Cyber Defense Centers
- Served all industries, most notably: Finance, Oil & Gas, Technology, Energy, and Telco’s

**Consultant Backgrounds**
- Fortune 100 SOC Managers
- Incident Response Leads for Fortune 100
- Forensics Investigators for US Govt.
- Global Presence

**Expertise**
- Mandiant’s consultants have successfully designed and developed some of the world’s largest Cyber Defense Centers. Our consultants apply in-depth knowledge and experience gained through hundreds of investigations, intelligence and best-practice implementations.
- Our consultants bring the Mandiant IR framework and real world knowledge to develop and transform CIRT teams into Cyber Defense Centers, from reactive capabilities to proactive capabilities in order to detect, respond and contain today’s targeted threats.
Agenda

- Mtrends Report Findings
- Program Components
- Intelligence Collection
  - Open Source Intelligence
  - Third Party Intelligence
- Program Integration
- Information Sharing
- Intel Frameworks
- Program Development
- Samples
31% victims discovered the breach internally

69% victims notified by an external entity
Median number of days that threat actors were present on a victim’s network before detection
Quadrant Model - Functional Alignment
Data > Information > (Actionable) Intelligence

Relationship of Data, Information, and Intelligence

- Operational Environment
- Data
- Information
- Intelligence

Collection, Processing and Exploitation, Analysis and Production

Credit: SANS.org
Program Integration – Collection & Processing

**Develop and integrate** threat intelligence capabilities to enable and enhance cyber defense operations, including:

- Threat / data feeds
- Threat Intelligence processes / procedures
- Technology Integration (e.g., SIEM, Intel Correlation)
- Leverage Security Intelligence Frameworks
Intelligence Collection Considerations

- Dedicated IOC creation function
- Trend/Historical analysis
- Actionable intelligence only
  - Regular securing tool tuning
    - White/Blacklists
    - IOCs
    - Alerts
  - Updates to security policies
- Quality assurance
Threat Intelligence / Information Sharing Frameworks - Examples

- **SIEM Communities**
  - Qradar Threat Exchange, Splunk feeds, etc.

- **Technical Platforms / Frameworks**
  - OpenIOC
  - OpenTPX – Open Threat Partner Exchange
  - STIX / TAXII
  - Collective Intelligence Framework (CIF)
  - Avalanche/Soltra (FS-ISAC)

- **Relevant Legal Frameworks**
  - E.g., CISA

- **Sector-specific Communities**
  - E.g., HITRUST Cyber Threat Xchange

- **Public/Private Programs**
  - DHS / NCCIC / US-CERT
  - CISCP / ECS
  - Country CERTs
  - ISACs
    - Financial Services, Information Technology, Multi-State, Water, Power, etc.
  - ENISA
    - E.g., European Financial Institute – Information Sharing & Analysis Centre

- **Common Vernacular**
  - Cyber Atlas
Program Integration – Analysis & Dissemination

Key questions to consider:

- What data / information is selected for processing?
- What analytical process is employed?
- What systems / technologies are leveraged?
- How is the information shared with stakeholders?
Intelligence Sharing – Portals & Partners

- Use a portal (preferably an existing one) to collectively share intelligence and indicators of compromise across staff. The portal should provide the following minimum capabilities:
  - granular access control
  - quick and easy access by all authorized staff
  - history of changes made to content
  - login history
  - the option for two-factor authentication
  - secure storage of content

- Developing relationships with law enforcement will assist in receiving information they collect from investigations

- Joining information sharing organizations can assist in understanding threats facing others in your industry

- Information sharing should be bi-directional
Understanding & Articulating

- Is this targeted?
- Is this part of a larger campaign? What’s the scale?
- Who else is seeing this? What are others saying?
- Or is this an insider threat?
- What are the TTPs? How do you find them?
- How do you remediate?
- How do you share?
Strategic vs. Tactical

- Understand the threat
- Weigh counter actions
  - Monitoring
  - Intelligence Collection
  - Tactical countermeasures
Proactive Capabilities – Hunting & Post-Incident Actions

- Hunting the network provides the capability to conduct proactive analysis to develop new IOCs
  - Data mining historical data
  - IOC Sweeps

- A mature IOC capability includes:
  - Dedicated individuals to design and build IOCs
  - Develop and update IOCs regularly (IOC Editor)
  - Processes and tools in place to actively check systems for IOCs

- Post-incident, hunting assists in ensuring remediation and eradication activities were successful
THREAT INTELLIGENCE PROGRAM DEVELOPMENT: TOOLS & TECHNIQUES
### Standardize Definitions

- **Event:**
  - Any observable occurrence in a system or network

- **Event of Interest:**
  - Any event with potential of security risk / threat

- **Incident:**
  - Violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

- **Vulnerability:**
  - An unintended flaw in a software code or a system that leaves it open to the potential for exploitation

- **Threat:**
  - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information and/or denial of service.

- **Threat Intelligence:**
  - Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard. - *Gartner*
Criticality Example – Commodity vs. Targeted Malware

• **Targeted, Advanced Persistent Threat**: High - Critical
  - Well Resourced attacker
  - Methodical, pre-meditated tactics
  - Advanced technical abilities

Vs.

• **Commoditized threat**: Low - Medium
  - Target of opportunity
  - Elementary tools & tactics employed
  - Script kiddie
# Categorizing Threats

<table>
<thead>
<tr>
<th>Objective</th>
<th>Nuisance</th>
<th>Data Theft</th>
<th>Cyber Crime</th>
<th>Hacktivism</th>
<th>Network Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>Botnets &amp; Spam</td>
<td>Advanced Persistent Threat</td>
<td>Credit Card Theft</td>
<td>Website Defacements</td>
<td>Destroy Critical Infrastructure</td>
</tr>
<tr>
<td>Targeted</td>
<td>☒</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Character</td>
<td>Automated</td>
<td>Persistent</td>
<td>Opportunistic</td>
<td>Conspicuous</td>
<td>Conflict Driven</td>
</tr>
</tbody>
</table>

© Mandiant, a FireEye Company. All rights reserved. CONFIDENTIAL
Formalize & Institutionalize Threat Intelligence Program

- Mission & Strategy
- Service Catalog
- Use Case
- Threat Intel Playbook
- Enterprise Process Workflow
Use Case Documentation

• Use Case Overview – Threat Intelligence
  • Additional Intelligence Related Use Cases
    Detection / Triage (Alerting)
    Data Loss
    Malware
    Unauthorized Access
    DoS / DDoS
    Web Attack
    Pen Testing
    Cyber Hunting
Playbook Overview

- **Functional Roles**
  - Event Analyst
  - Incident Analyst
  - Incident Responder
  - Security Team Manager
  - Relevant Stakeholders
    - Executives
    - Network Operations
    - System Owners
    - Security Team Members/Stakeholders
    - Relevant stakeholders / Business Reps

Credit: Athlonsports.com
Use Cases

Mandiant implements use cases at each stage within the kill chain. This ensures complete visibility and allows the CDC to detect and respond to cyber threats earlier, in order to reduce exposure and loss.
Source as many IOCs as you can

- APT Reports & White Papers - 2015
  - Behind the Syrian Conflict’s Digital Frontlines
  - APT30
  - Hiding in Plain Sight (with Microsoft)
  - HAMMERTOSS (APT29)
  - WITCHCOVEN

- Intel Sharing Frameworks
- Intelligence Sources
- Service Providers
- Email Distros
- Blogs
- Etc.
Source as many IOCs as you can (cont.)

- Sample APT Report
Q & A

Discussion

Nucleus, patented
32 million node
graph-based engine, mines data with 200
volumes of storage, and 500M+ captured
network streams

Helix malware triage
system uses proprietary
sandboxing, machine
learning, and genotyping
tech to identify new
samples of interest

Team of 25 PhDs,
linguists, analysts, and
foreign policy experts
from NSA, CIA, DIA, and
military put intelligence
into context

51 GB of command and
control monitored

40 Current industry-
specific threat profiles

150,000 Indicators of
compromise

20 million compromised
computers check in
with Mandiant every
hour

2,700 Advanced malware
samples from client
engagements analyzed
last year

200 Attacker groups
tracked

17 Million unique compromised
devices observed every day

400,000 Unique malware samples
gathered every day

1 Landmark report which shifted the
industry dialog:

Exposing APT1