GE

Incident Response

Sean Mason
Director, Incident Response
Investing in new talent & capabilities

- Incident response
- Cyber intelligence
- Digital forensics
- Security architecture
- Identity management
- Compliance, controllership, IT management
Fundamentals
Evolution
# Threats

<table>
<thead>
<tr>
<th>Threat type</th>
<th>What</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacktivism</td>
<td>Highly visible attacks targeting large corporations and government agencies</td>
<td>• Anonymous</td>
</tr>
<tr>
<td>Advanced Persistent Threat</td>
<td>Organized and state funded groups methodically infiltrating the enterprise</td>
<td>• APT1</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>Organized crime rings targeting individuals and corporations for financial gain</td>
<td>• RBN</td>
</tr>
</tbody>
</table>
Kill Chain (KC)

**KC1 - Reconnaissance:** Collecting information and learning about the internal structure of the host organization

**KC2 - Weaponization:** How the attacker packages the threat for delivery

**KC3 - Delivery:** The actual delivery of the threat (via email, web, USB, etc.)

**KC4 - Exploitation:** Once the host is compromised, the attacker can take advantage and conduct further attacks

**KC5 - Installation:** Installing the actual malware, for example

**KC6 - Command & Control:** Setting up controls so the attacker can have future access to the host's network

**KC7 - Actions on Intent:** The attacker meets his/her goal (e.g. stealing information, gaining elevated privileges or damaging the host completely)
Incident Response process (DCAR+I)

- Detect
  - NSM
  - SIEM
  - AV/HIPS
- Contain & Collect
  - Contain Host
  - Acquire Forensic Evidence
- RemEDIATE
  - Rebuild host
  - Reset passwords
  - Task Force countermeasures
- Analyze
  - Actors
  - Methods
  - Movement
  - Accounts

- Identify Scope
  - Ticket management
- Prioritize Risks
  - Live Response status
  - Network log data
- Impact (data movement)
  - Indicators for new signatures

- Tool Alerts
- Reporting
IR measured cycle times

- **Dwell Time (DWT)**
- **Contain Time (CNT)**
  - **Business Impact Time (BIT)**
  - **Strategic Remediate Time (SRT)**

**Event**
- Event (Event Time)

**Event Analysis**
- Triage (Detect Time)

**Report**
- Report (Report Time)

**Contain**
- IR Actions (Contain Time)

**Remediate**
- Remediation/Task Force (Remediation Time)

**DWT + CNT** = Time of unauthorized access to asset

**Questions**
- How fast did we **find** it?
- How fast did we **respond** to it?
- How fast did we **fix** it?
Workflow & knowledge management
Communication

- Tailored audience based on KC
- Standard communications rhythm
  - (~1hr after declaration; COB daily)
- More detailed PowerPoint
  - End of week
- Inclusive & transparent!

RESTRICTED INFORMATION – LIMITED DISTRIBUTION; ENCRYPTED TRANSMISSION ONLY
Note: Updated information is shaded in Green and completed actions are struck through.

Kill Chain Phase:

Businesses & Locations Impacted:

Summary:

Impact:

Incident Status: MM-DD-YYYY HHMM

Host Status:

Intelligence Summary:
  - Attribution

Action Items:

Next Update:
<table>
<thead>
<tr>
<th>Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chemical</td>
</tr>
<tr>
<td>Commercial Facilities</td>
</tr>
<tr>
<td>Communications</td>
</tr>
<tr>
<td>Critical Manufacturing</td>
</tr>
<tr>
<td>Dams</td>
</tr>
<tr>
<td>Defense Industrial Base</td>
</tr>
<tr>
<td>Emergency Services</td>
</tr>
<tr>
<td>Energy</td>
</tr>
<tr>
<td>Financial Services</td>
</tr>
<tr>
<td>Food &amp; Agriculture</td>
</tr>
<tr>
<td>Government Facilities</td>
</tr>
<tr>
<td>Healthcare &amp; Public Health</td>
</tr>
<tr>
<td>Information Technology</td>
</tr>
<tr>
<td>Nuclear Reactors, Materials &amp; Waste</td>
</tr>
<tr>
<td>Transportation Systems</td>
</tr>
<tr>
<td>Water &amp; Wastewater Systems</td>
</tr>
</tbody>
</table>

Strong relationship with key stakeholders across all sectors
CRITs is a MITRE application provided to industry peers (120+ members) for:

- Indicator management
- Malware triage
- Advanced Intel analysis
- Managing the “Sharing Problem”
- Implementing threat sharing standards

OSINT
Sharing partners
Antivirus vendors
Structured indicator storage

Summary details provide the default required values about an indicator.
Structured indicator storage

Actions can be used to show tracking of an indicator to a detection deployment. Tickets can be used to relate indicators back to our tickets.
Structured indicator storage

Campaigns show the threat actor attribution from the Cyber Intelligence teams.
Structured indicator storage

Relationships build out the larger picture of how various pieces of intelligence are linked.
Structured indicator storage

Objects allow us to tag intelligence with context such as the Kill Chain or what role the intelligence plays.
Detect
Intel driven, threat centric detection

Intelligence
- Collect
- Analyze
- Disseminate

Detect
- Transform
- Develop
- Deploy

Respond
- Triage
- Respond
- Remediate

Establish Requirements
- Gather Intelligence
- Manage Collection
- Store Raw Intel

Intelligence
- Extraction
- Enrichment / Analysis
  - Prioritization
  - Validation
  - Categorization
    - god/bad/informational
  - Quality Check
    - Frequency Analysis
- Store Product
- Distribute

Detect
- Consume
- Quality Check
- Detection Alignment
  - Platform
  - Location
  - Capacity
- Development
- Build
- Pre-deployment Test
- Document
- Production Deployment
- Signature Monitoring
- Collect / Aggregate
- Notify / Present
- Alert Monitoring
- Event Analysis
- Investigation
- Feedback
- Reporting

Respond
- Formal IR
- Host Isolation
- Containment
- Live Collection
- Forensics
- Communications
- Reporting
- Remediation
- Service Restoration
- Root Cause Analysis
- Architecture Reviews
- Process Improvement

SIEM
- WAF
- HTTPRY
- IDS
- Proxy
- IPS
- NSM
- DLP
- AV

imagination at work
Detection scenarios

Recon
- File - Name
- File - Path
- URI - URL
- HTTP - GET
- HTTP - User Agent String
- URI - Domain Name
- Address - e-mail
- Address - ipv4-addr

Weaponization
- File - Name
- File - Path
- URI - URL
- HTTP - GET
- HTTP - POST
- Email Header - Subject
- Email Header - X-Mailer
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - e-mail
- Address - ipv4-addr

Delivery
- Behavior
- Win Registry Key File - Name
- File - Path
- URI - URL
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - cidr
- Address - ipv4-addr

Exploitation
- Code - Binary_Code
- Win Process
- Win Registry Key File - Name
- File - Full Path
- URI - URL
- HTTP - GET
- HTTP - POST
- Email Header - Subject
- Email Header - X-Mailer
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - cidr
- Address - ipv4-addr

Installation
- Behavior
- Win Registry Key File - Name
- File - Full Path
- URI - URL
- HTTP - GET
- HTTP - POST
- User Agent String
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - e-mail
- Address - ipv4-addr

C2
- Behavior
- Win Registry Key File - Name
- File - Full Path
- URI - URL
- HTTP - GET
- HTTP - POST
- User Agent String
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - e-mail
- Address - ipv4-addr

Act on Objectives
- Behavior
- Win Registry Key File - Name
- File - Full Path
- URI - URL
- HTTP - GET
- HTTP - POST
- User Agent String
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - e-mail
- Address - ipv4-addr
# Platform strengths (IPS+)

<table>
<thead>
<tr>
<th>Recon</th>
<th>Weapon-ization</th>
<th>Delivery</th>
<th>Exploitation</th>
<th>Installation</th>
<th>C2</th>
<th>Act on Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>File - Name</td>
<td>File</td>
<td>File - Path</td>
<td>Behavior</td>
<td>Code - Binary_Code</td>
<td>Behavior</td>
<td>Behavior</td>
</tr>
<tr>
<td>File</td>
<td>URI - URL</td>
<td>File - Full Path</td>
<td>Win-Registry-Key</td>
<td>Win Process</td>
<td>Signature</td>
<td>Win-Registry-Key</td>
</tr>
<tr>
<td>HTTP - GET</td>
<td>File</td>
<td>URI - URL</td>
<td>File - Name</td>
<td>Win-Registry-Key</td>
<td>File</td>
<td>File</td>
</tr>
<tr>
<td>URI - URL</td>
<td>URI - URL</td>
<td>URI - Domain Name</td>
<td>File</td>
<td>File</td>
<td>File</td>
<td>URI - URL</td>
</tr>
<tr>
<td>HTTP - POST</td>
<td>URI - URL</td>
<td>URI - Domain Name</td>
<td>URI - URL</td>
<td>URI - Path</td>
<td>HTTP - GET</td>
<td>HTTP - GET</td>
</tr>
<tr>
<td>URI</td>
<td>URI - Domain Name</td>
<td>URI</td>
<td>URI - URL</td>
<td>HTTP - GET</td>
<td>HTTP</td>
<td>URI - Domain Name</td>
</tr>
<tr>
<td>Hash - MD5</td>
<td>Hash - SHA1</td>
<td>Address - cidr</td>
<td>HTTP</td>
<td>Address - e-mail</td>
<td>Address - cidr</td>
<td>Address - e-mail</td>
</tr>
<tr>
<td>Address - ipv4-addr</td>
<td>Address - e-mail</td>
<td>Address - ipv4-addr</td>
<td>HTTP</td>
<td>Address - ipv4-addr</td>
<td>Address - ipv4-addr</td>
<td>Address - ipv4-addr</td>
</tr>
</tbody>
</table>

---

[Imagination at Work]
Detection visibility gaps

HTTP - User Agent String
File - Path
URI - URL

Email Header - Subject
Email Header - X-Mailer

HTTP - User Agent String
Address - ipv4-addr
Address - ipv4-addr

Example data
Detection gaps per actor

1. Recon
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. C2
7. Act on Objectives

Example data
- File
  - Email Header - Subject
  - Hash - MD5
  - Address - e-mail
- File
  - Hash - MD5
- File
  - URI - Domain Name
  - Hash - MD5
  - Address - ipv4-addr
Contain & Collect
Outpost locations

Example locations

Outpost server
Centralized Storage/Analysis
Automated & centralized C&C

1. Interactive Session
2. Suspect
3. Auto-Upload
4. Manual Upload

Outpost(s)
- Internal SSH
- External SSH

Centralized Storage & Analysis
- Python
- Ruby

Automated & Manual
Containment selection

- Find host and system type
- Identify operating system
- Determine if the host is online or offline
- Identify if the system is on VPN

<table>
<thead>
<tr>
<th>Method</th>
<th>Time</th>
<th>Desktop</th>
<th>Laptop</th>
<th>Server</th>
<th>Windows OS</th>
<th>Other OS</th>
<th>VPN</th>
<th>Offline</th>
<th>Evidence Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ACL</td>
<td>2hrs</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>1</td>
</tr>
<tr>
<td>solator</td>
<td>30m</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>2</td>
</tr>
<tr>
<td>Active Directory</td>
<td>15m</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>2</td>
</tr>
</tbody>
</table>
Virtual Isolation

- ICMP – Network Identification
- DNS (UDP/53) – Host Resolution
- SMB (TCP/445) – Authentication
- DHCP (TCP/67) – Persistence

Specified Domain Controllers

GE (3.0.0.0/8)

Outposts

C:\isolator.bat
Netsh ipsec add policy "virtual isolation" SecPermit Outpost IP ANY ANY
Netsh ipsec add policy "virtual isolation" SecPermit DC_IP TCP TCP
Netsh ipsec add policy "virtual isolation" SecPermit 67 TCP TCP
Netsh ipsec add policy "virtual isolation" SecPermit 53 ANY ANY
Netsh ipsec add policy "virtual isolation" SecPermit 445 TCP TCP
Netsh ipsec add policy "virtual isolation" Block ANY ANY ANY
more %cd%\usernotification.txt | msg %username%
Quarantine

- Internet Routable GE IPs
- GE IP Space

Suspect

- GE (3.0.0.0/8)
- VPN IPs
- Necessary Protocols*

*- ICMP – Network Identification
*- DNS (UDP/53) – Host Resolution
Isolation GPO

DC pushes GPO to suspect, GPO isolates suspect

Domain Controller

Responder adds Suspect to Isolation GPO machine group

Responder

Outpost(s)

DC informs responder that Suspect is now online

Host comes online, checks in with DC

Responder starts LR collection from outpost

The Isolation GPO

1. Isolates Suspect Host

2. Changes desktop background

3. Changes login banner

4. Suspect is now online

5. Responder adds Suspect to Isolation GPO machine group
Analysis
Analysis infrastructure

- 4 x Intel Xeon 2.4GHz (8 cores/ea)
- 48 x 32GB RAM (1.5TB)
- 16 x 900GB (13.5TB)

"$MFT that used to take 6hrs to parse took only 30 minutes"
Automated analysis processing

- Execute tasks in parallel as sub process
- Each module can be run “standalone”

1. Extract compressed LR
2. $MFT$ processing
3. HPAK & memory processing
4. Yara scanning
5. Greps/master timeline/wiki

Forensic Incident Response Extractor
Remediation
Prevention

- Leverage Intel, Detect, & Response to support prevention
- Root Cause Analysis
- Failure Mode Analysis

“Go 5 What’s & Why’s Deep!”
## Task Force template

<table>
<thead>
<tr>
<th>Kill Chain</th>
<th>Actor Action</th>
<th>Failure Mode</th>
<th>Mitigation Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance</td>
<td>Used web commercial scanner</td>
<td>Potential gaps in threat tool &amp; scanning capability</td>
<td>Establish detection capability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weaponization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivery</td>
<td>SQL injection on vulnerable ASP page to gain admin user access</td>
<td>Could not detect SSL traffic; vulnerable to SQL injection</td>
<td>Explore Secure Development and Application Security Assessments</td>
</tr>
<tr>
<td>Exploitation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installation</td>
<td>IIS web service used to upload web shell</td>
<td>Failure to restrict file upload types or configure web server to not execute uploaded files</td>
<td>Explore Secure Development and Application Security Assessments</td>
</tr>
<tr>
<td>Comm &amp; Control</td>
<td>Used web shell on initially compromised host</td>
<td>Could not detect SSL traffic</td>
<td></td>
</tr>
<tr>
<td>Actions on</td>
<td>Accessed “id.txt” which held account information</td>
<td>Management scripts failed to delete “id.txt” after running</td>
<td>Scripts retired and environment scanned.</td>
</tr>
<tr>
<td>intent</td>
<td>with admin access</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Task Force initialization

- IR Knowledge Transfer
- Task Force kick-off
- Failure Mode Analysis
- Mitigation Action Plan
- Transition to long-cycle tracking

**Example data**
Putting it all together...
In conclusion...

1. Intel & IR work is a process that can be measured, evolved and simplified.
2. Partnerships & open source intel collection are critical to success.
3. Detection should be based on a foundation of prioritized intel; understand your capabilities and gaps.
4. Risk based approach to containment. No one size fits all model.
5. Invest in your analysis infrastructure- it will reduce response time.
6. Communicate findings and learning back into other functions.

Build a thrivingIntel & IR ecosystem for your company.
QUESTIONS