Level Up Your Incident Response

Building and Testing Response Capabilities for Today’s Reality and Tomorrow’s Threats

InnoTech Conferences – November 2018

Brian A. Engle, CISO & Managing Director of Advisory Practice
Leveling Up Your Incident Response

A Plan for Continuous Response

Essentials of the Incident Response Program

Fighting Above Your Weight Class – Going From Good to Strong
A Plan for Continuous Response

There’s never a perfect time for things to go wrong…
The Incident Response "Plan"

A Plan for Continuous Response
Developing the Incident Response Plan

Garner Stakeholder Support

- Create the Incident Response Policy to define authority levels and management’s responsibility for support
- Create a strategic plan for developing the Incident Response Program – goals, objectives and activities to enable capabilities, obtain required resources and achieve necessary effectiveness
- Define the budget requirements across the strategic plan milestones
Anticipating Failure to Ensure Success

Dependence on the Information Security Program

Identify | Protect | Detect | Respond | Recover

People | Process | Technology
Essentials of the Incident Response Program

The Incident Response Program - Putting the plan into action.
Preparation Stage

Fortune favors the prepared.
The Clock is Ticking
Preparation starts today

There’s no better time than the present
Preparing to Handle Incidents

Breaking it Down Before Things Break Down

Identify  Protect  Detect  Respond  Recover

People  Process  Technology
Identifying the Assets, Threats, Countermeasures and Defenses

Plotting the Battlefield
An Ounce of Prevention…

Is exactly one ounce of prevention. Add protections that limit impact and slow down attackers.
Protection is Imperfect

Continual Analysis of Defenses, Threat Vectors, Vision Space and Blind Spots

- Evaluate data flows and architecture
- Analyze protections, threat vectors and gaps in defense
- Enable detective capabilities beyond protection devices
- Consider the supply chain and partners
Detection and Analysis Stage

Are you about to have a bad day, or is everyone about to?
There Are Two Types of Companies

“There who’ve been hacked, and those who don’t yet know they have been hacked.” – Sun Tzu
Detection and Analysis

Let Impact and Frequency Drive Priority

Establish Incident Severity Levels (Impact)

<table>
<thead>
<tr>
<th>Severity Classification</th>
<th>Users Impacted</th>
<th>VIP / Management Impact</th>
<th>Tier 1 Business Applications</th>
<th>Tier 2 or 3 Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Establish Incident Types and Categorizations (Frequency)

- Denial of Service - Availability
- Unauthorized Access - Confidentiality and Privacy
- Improper Usage – Policy Violation, Insider Threat
- Vector Attacks - Malicious Code/Malware, Scans/probes/access attempts, Phishing, Ransomware
Threat Analysis

The Spectrum of Threats – Basic Levels of Attribution

Attacker Tactics, Techniques and Procedures (TTPs)

• At minimum, determine who will likely target your organization

Identify characteristics, create detection profiles

• Evaluate current detection capabilities, identify blind spots
Kill Chain Analysis

Threat Actors are similar in methodology, but not identical

Lockheed Martin Kill Chain Model

General Asymmetric Adversary/Target Model

Customize the Kill Chain for your business model
Detection and Analysis

Signs of an Incident – Sources of Precursors and Indicators

Standard Sources
• Intrusion Detection and Prevention System (IDS/IPS)
• Event Logs / Security Information and Event Monitoring (SIEM)
• Antivirus and Antispam systems
• Data Loss Prevention Systems
• Open Source Intelligence and Public News Sources

Advanced Sources
• Baseline behavior analytics and anomaly detection
• Threat hunting and proactive investigation techniques
• Third-party monitoring services and Threat Intelligence firms
• Dark Web forums and criminal exchanges

REACTIVE
MOSTLY “PROTECT” SYSTEMS

PROACTIVE
LOOKING FOR WHAT GOT PAST “PROTECT”
Threat Hunting

The Diamond Model for Intrusion Analysis

Diamond Model -
Proactively Hunting for the Threat

The Hunting Loop

CREATE Hypotheses

INFORM & ENRICH Analytics

INVESTIGATE Via Tools & Techniques

UNCOVER New Patterns & TTPs

HUNTPEDIA - https://www.threathunting.net/files/huntpedia.pdf
Investigating and Following the Trail

Clearing the fog of war

Known Facts
• Log file events
• Artifacts and attacker remnants/tools
• Malware

Speculative Facts
• Loosely connected events
• Tool and malware attributes
• Moderate confidence intelligence
Investigating and Following the Trail

Clearing the fog of war

Theories

- General Attacker Type TTPs
- Artifacts and attacker remnants/tools
- Malware

Unknowns

- All of the Who, What, Where, When, Why and How’s that you don’t know
Cold File vs. Active Attacker Incidents

2018 Verizon Data Breach Investigations Report

Long timelines of Compromise, Exfiltration and Discovery
Active Attacker Incidents

There will come a time when you are face-to-face (virtually) with the attacker

Special considerations:

• If activity goes dormant – have they gone dark or just gone away?
• Should you observe activity to learn about entry paths – or just start slamming doors?
• If you disrupt the primary objective will they go scorched earth on you?
• If using an outsourced DFIR firm, discuss these options so that chain of command decisions doesn’t delay tactical execution.
Exfiltration – The Battle May Not Be Lost

Criminal Forums and the Dark Net

Special considerations for data types:

- Financial instruments can be de-valued - reissuing credit cards or account information can prevent fraud losses
- Login credentials can be changed to prevent account takeover and business email compromise
- Weigh the costs and take actions to de-value data that is easily changed, even if you aren’t able to see the dark net brokerage of data
- Discovery of the dark net exchange can validate impact, attribute to attacker, and potentially aid law enforcement
Executing the Response Process – Containment, Eradication & Recovery Stage

When the Alarm Bell is Sounded
The Organization Incident Response Plan

Incident Response. It’s not just for InfoSec anymore.

- Inclusion of non-IT functions in formulation and exercise of IR plan
- Even though those functions are experts in their field, they’re not experts in cybersecurity or privacy
- External Communications - Everyone that can use Word will want revision rights
- Consider how and when to loop in key government leadership
Did Things Just Get Better…

Or worse

Legal Considerations for the Incident Response Plan

- Legal Team
- Privacy Officer
- Law Enforcement(s)

Litany of evidentiary concerns

- Who makes the call to Law Enforcement?
- When?
- Who has jurisdiction?
- Who will be most helpful?

Law Enforcement’s goals are not always aligned with your goals
Containment, Eradication & Recovery Stage

Stop – Drop – and Roll. Putting out the fire.

- Identifying Sources of Attacks and Attacking Hosts
- Tracking the Attacker
- Monitoring the Response Process

<table>
<thead>
<tr>
<th>Known Facts</th>
<th>Speculative Facts</th>
<th>Theories</th>
<th>Unknowns</th>
</tr>
</thead>
</table>

Communication and Escalation

No surprises – communicate early and often

- Develop thresholds of notifications and appropriate audiences
- Define escalation processes and levels
- Round up estimates, but don’t exaggerate
- Share Known-Knowns
- Describe Known-Unknowns – with what actions will confirm and when you anticipate confirming

<table>
<thead>
<tr>
<th>IR Steps</th>
<th>Anticipated</th>
<th>Actual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Occurrence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification/Classification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR Initiated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contained</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post Action Completed</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Incident Handlers Log
Create a journal template for members of the incident response team

<table>
<thead>
<tr>
<th>Incident Timeline and Critical Timestamps</th>
<th>Activity Log</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Occurrence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR Initiated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contained</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post Action Hotwash</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Communication Channels                   |              |       |
| Conference Bridge Line                  |              |       |
| Mobile Numbers                           |              |       |

| Incident Handlers Log Incident Number: 20180531-0001 |

<table>
<thead>
<tr>
<th>Hotwash Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>What went well?</td>
</tr>
<tr>
<td>What didn’t work well?</td>
</tr>
<tr>
<td>What information was needed sooner?</td>
</tr>
<tr>
<td>What protective measures would prevent the incident from occurring in the future?</td>
</tr>
<tr>
<td>What detective measures would have alarmed sooner?</td>
</tr>
</tbody>
</table>
Incident Status Reporting

Clearing the fog of war.

- Incident Type – Categories previously defined in terms the audience understands
- Incident Classification – Severity levels previously defined in impact terms meaningful to the organization
- Potential risks that the type and classification present – potential impact
  What data or business function is impacted or potentially compromised?
- Brief description of what has happened
  When did it happen? When did we detect it? How did we detect it?
- What is being done to mitigate
- Timeline, anticipated next steps, and when will next update occur
External Communications Can Save the Day

Or make the incident situation far worse

Media Relations
Public Relations
Customer Relations
Government Relations
Every Company Employee with a computer, smartphone and social media account
Terminology is Important

Clearly establish definitions and terms for the organization

Breach – It has a distinct meaning for regulated data and privacy

Intrusion – Unauthorized access

Attempted Intrusion – Unsuccessful attempt at access

Probe or Scan – Exploring technology resources looking for weaknesses

Vulnerability / Threat / Exploit

Risk / Impact / Likelihood
Putting the Response in Incident Response

It’s a race to the prize – use your advantages to your advantage.

- Containment strategies
- Watching the egress points
- Consider the attacker motives and observed actions
- Investigate ground-zero and monitor the inner sanctum
Containment and Eradication

Tough times call for tough choices.

Limiting damage or impact can sometimes require quick decisions with consequences.

- Try to make decisions during the planning stage, then you’re just executing during the containment and eradication stage.
- Establish decision authority during the planning stage – the distance between hero and zero is far but covered quickly.
- Defenders should have the upper hand – know the landscape, choke points, strength and weaknesses better than the attacker.
Ransomware

A category of its own

Special considerations - Ransomware:

• Ransom payment – rule or guideline?
• Setting up a bitcoin wallet while the encryption countdown clock is ticking is maybe too late
• What does adding a new vendor in your ERP system look like, can it be expedited, and what if it’s a hacker?
• Consider the City of Atlanta use case
  • Test backups regularly
  • Keep backups as offline as possible
  • Ransomware attackers continue to evolve – see bullet one above
Protecting IR Communications
Beware unfriendly eyes and ears

Protect communication channels

• Email may be compromised
• Scheduled update calls and incident bridge conference lines may become listening parties
• Web collaboration service credentials may be suspect
Post-Incident Activity Stage

At the end of the day is tomorrow.
Getting ready to do it all over again.
Post-Incident Activities

No one likes paperwork – but the job isn’t finished until the report is compiled

Gather data from the process:

- Time to detect
- Time to respond
- Time to contain
- Time to eradicate
- Time to remediate
- Time to full recovery
- Effort hours and costs
**Information Security Incident Report**

**Instructions:** This form is to be completed as soon as possible following the detection or reporting of an Information Security incident. All items completed should be based on information that is currently available. The report should be updated and modified during the course of the incident response process.

1. **Incident Description.**
   
   Provide a brief description:

2. **Incident Details**
   
   **Date and Time the Incident was discovered:**
   
   **Has the incident been resolved?**
   
   **Physical location of affected system(s):**
   
   **Number of sites affected by the incident:**
   
   **Approximate number of systems affected by the incident:**
   
   **Approximate number of users affected by the incident:**
   
   **Are non-Aunt Berthe systems, such as business partners, affected by the incident? (Y or N – if Yes, please describe):**

3. **Impact / Potential Impact**

   Check all of the following that apply to this incident:

   - Loss / Compromise of Data
   - Damage to Systems
   - System Downtime
   - Financial Loss
   - Other Organizations’ Systems Affected
   - Damage to the Integrity or Delivery of Critical Goods, Services or Information
   - Violation of legislation / regulation
   - Unknown at this time

4. **Sensitivity of Data/Information Involved**

   Check all of the following that apply to this incident.

   **Sensitivity of Data**

<table>
<thead>
<tr>
<th>Category</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.</td>
</tr>
<tr>
<td>Internal Use Only</td>
<td>Internal Use information is information originated or owned by your organization or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company’s business interests.</td>
</tr>
<tr>
<td>Confidential</td>
<td>Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by your organization.</td>
</tr>
<tr>
<td>Restricted (Potential Privacy Violation)</td>
<td>Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.</td>
</tr>
<tr>
<td>Unknown/Other</td>
<td>Describe in the space provided</td>
</tr>
</tbody>
</table>

5. **Provide a brief description of data that was compromised:**
Incidents vs. Breaches

- Incident – A security event that compromises the integrity, confidentiality or availability of an information asset.
- Breach – An incident that results in the confirmed disclosure – not just potential exposure – of data to an unauthorized party.

About the cover

The arc diagram on the cover is based on the data in Appendix C: Beaten paths. It illustrates the actors, actions, and attributes as nodes; and the order of their occurrence in attack paths as edges—see the callout on page 54 for more information. We’ve counted how many times each node occurs in each path and sized them accordingly—the larger the node, the more times it appeared. The edges between nodes are represented as arcs between points. The color of each arc is based on how often an attack proceeds from one node to the next.
• VERIS Community Database (VCDB) – open and free repository of publicly-reported security incident in VERIS format - raw data available for your own research

• SCHEMA – Includes incident tracking, victim demographics, incident description, discovery & response and impact assessment detailed elements

• Highlight – The Discovery and Response data includes incident timeline, discovery method, root causes, corrective actions, targeted vs. opportunistic flag and additional guidance
  • TIP – Just reviewing the database data in this area can help identify processes to prioritize based upon frequency of occurrence for organizations that look like yours

VERIS - http://veriscommunity.net
Evidence Gathering and Preservation

Data Forensics and Material Handling

- Evidence may need to be kept for future law enforcement or civil cases
- Part-time response personnel can be trained and appropriately handle evidence – but experience and certified professionals with extensive background providing testimony stands up to rigor better
- If outsourcing DFIR services, consider engaging through general counsel for attorney-client privilege protections
- Obtain evidentiary gathering materials and prepare chain of custody materials including secure storage in the preparation phase
Post-Incident Activities

We now return you to your regularly scheduled programming. Immediately after the incident temperature allows and before the troops scatter, conduct a hotwash session.

- What went well?
- What didn’t work well?
- What information was needed sooner?
- How and where could we get it sooner?
- What information can we share with peers, partners, and industry sharing groups?
- What protective measures, controls or countermeasures would prevent the incident from occurring in the future?
- What measures would provide better detection or mitigation?
- How effective and timely were communications during the incident?
Incident Handlers Log

Create a journal template for members of the incident response team

<table>
<thead>
<tr>
<th>Incident Timeline and Critical Timestamps</th>
<th>Activity Log</th>
<th>Incident Number: 20180531-0001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Occurrence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR Initiated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contained</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post Action Hotwash</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication Channels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conference Bridge Line</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Numbers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Notes                                      |              |                                |
| What went well?                            |              |                                |
| What didn’t work well?                     |              |                                |
| What information was needed sooner?       |              |                                |
| What protective measures would prevent the incident from occurring in the future? |              |                                |
| What detective measures would have alarmed sooner? |              |                                |
The Incident Response Program

The Program, the Plan, and the Processes
Fighting Above Your Weight Class

Going from good to strong.
Most businesses have minimal IT resources, and even fewer dedicated security staff, yet are faced with essentially the same breadth of control requirements that larger organizations have been attempting to enable and mature.

Threat actors and criminals do not discriminate by size or wait for organizations to get cybersecurity capable. Everyone is in need of effective ways of increasing capabilities faster, more efficiently, and without breaking the bank.
Information Sharing – It’s better to give and receive

- ISAC’s
- ISAO’s
- Threat Forums

Establish fusion center sharing with the supply chain, vendors and partners

- Coordinate detection, indicators and precursors
- Include in exercises to prepare for inclusion in actual incident response
- Expect partners to do the same
Next Level Detection

➢ External sources, forums and the darknet
➢ Establish metrics for quality, effectiveness, timeliness and relevance
➢ Anomalous behavior analysis and proactive threat hunting

Consider the client/citizen/customer in the response process

➢ Communications and messaging – the clock is ticking and they may be at risk now
Military Grade Cybersecurity

Preparation Includes Training, Exercises and Drills

- Training the part time incident response team
- Drill like it’s the real thing
- Use real world events to create scenarios
- Build hunting into the exercise
A Trusted Guide and Advisory Partner
CyberDefenses is enabling organizations to fight in the asymmetric cybersecurity battlefield with Military-Grade Cybersecurity

WHAT WE DO

Guidance and Advisory
- Assessment and Analysis Consulting
- Strategy and Roadmap Development
- Incident Preparedness
- Risk Management
- Compliance Preparedness

Security Operations
- Event Monitoring and Detection
- Incident Response & Forensics
- Threat Intelligence Services
- Managed Security and Operations

Academy
- Instructor Led Courses
- Virtual, Onsite, at Conferences
- Heavy Lab/Practical Components
- Certification Courses
- CPE Credits
- Privacy Training