Blue Team Perspectives
The Business of Incident Response
Putting Myself in Context

› **Professional**
  
  • High tech IT consultant for startups
  
  • Independent computer forensics practitioner
  
  • Now global consulting firm incident response manager, designer, implementer

› **Personal**
  
  • Volunteer search and rescue
  
  • Pilot – sailplanes, fixed wing, rotorcraft, FPV, UAV, ....
Incident Response Context

Incident Response

CIRT

Security Program

You are the tip of the pyramid ...

Supported by your team ...

Standing on top of a much larger continuous business process
<table>
<thead>
<tr>
<th>Working Assumptions</th>
<th>1</th>
<th>Monitoring</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is an Incident?</td>
<td>2</td>
<td>Investigation</td>
<td>8</td>
</tr>
<tr>
<td>Indicators and Threat Intelligence</td>
<td>3</td>
<td>Containment</td>
<td>9</td>
</tr>
<tr>
<td>People and Groups</td>
<td>4</td>
<td>Remediation</td>
<td>10</td>
</tr>
<tr>
<td>Planning and Prep</td>
<td>5</td>
<td>Closing Incidents</td>
<td>11</td>
</tr>
<tr>
<td>Documentation</td>
<td>6</td>
<td>Business Case for IR</td>
<td>12</td>
</tr>
</tbody>
</table>
Working Assumptions
Compromise is inevitable

Something truly malicious has been in, is in, and will be in your environment
Working Assumptions

Incident Response is Part of Continuous Business Process

- Response is a misnomer - it must be proactive to succeed at being reactive
- The CIRT does not stand apart, or exist in a vacuum
- Someone needs to represent CIRT to the business, and vice versa
Working Assumptions

People > Processes > Tools

- People are more important than tools
- Good processes are more important than tools
- Good teams are more important than tools
- That said, you still need to invest in good tools
<table>
<thead>
<tr>
<th>Working Assumptions</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What is an Incident?</strong></td>
<td>Investigation</td>
</tr>
<tr>
<td>Indicators and Threat Intelligence</td>
<td>Containment</td>
</tr>
<tr>
<td>People and Groups</td>
<td>Remediation</td>
</tr>
<tr>
<td>Planning and Prep</td>
<td>Closing Incidents</td>
</tr>
<tr>
<td>Documentation</td>
<td>Business Case for IR</td>
</tr>
</tbody>
</table>
What Is An Incident?

What is in scope for your incident response program?

- Stolen laptop
- DDOS
- Commodity malware
- APT
- RBN
- Espionage
- Generic phishing
What Is An Incident?

Define “incident” yourself lest others define it for you

- Put it down in writing
- Once defined, stick to it
  - Don’t get sucked into stolen laptops and HR issues
  - You can support, but not own, related issues
- Feature creep and scope drift apply
Now that you’ve defined what an incident is, you can determine the scope of your incident response program.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Assumptions</td>
<td>1</td>
</tr>
<tr>
<td>What is an Incident?</td>
<td>2</td>
</tr>
<tr>
<td>Indicators and Threat Intelligence</td>
<td>3</td>
</tr>
<tr>
<td>People and Groups</td>
<td>4</td>
</tr>
<tr>
<td>Planning and Prep</td>
<td>5</td>
</tr>
<tr>
<td>Documentation</td>
<td>6</td>
</tr>
<tr>
<td>Monitoring</td>
<td>7</td>
</tr>
<tr>
<td>Investigation</td>
<td>8</td>
</tr>
<tr>
<td>Containment</td>
<td>9</td>
</tr>
<tr>
<td>Remediation</td>
<td>10</td>
</tr>
<tr>
<td>Closing Incidents</td>
<td>11</td>
</tr>
<tr>
<td>Business Case for IR</td>
<td>12</td>
</tr>
</tbody>
</table>
Indicators and Threat Intelligence

Data is not threat intelligence

- Determine what “Threat Intelligence” is for you
- Find sources that apply to your organization
  - Business and services
  - Geography
  - Politics
- Learn to develop, track, and share IOCs
Kill Chains

With thanks to Lockheed Martin for the cyber version

Incident + Incident + Incident = Campaign
... and when experience is not retained, as among savages, infancy is perpetual. Those who cannot remember the past are condemned to repeat it.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Assumptions</td>
<td>1</td>
</tr>
<tr>
<td>What is an Incident?</td>
<td>2</td>
</tr>
<tr>
<td>Indicators and Threat Intelligence</td>
<td>3</td>
</tr>
<tr>
<td>People and Groups</td>
<td>4</td>
</tr>
<tr>
<td>Planning and Prep</td>
<td>5</td>
</tr>
<tr>
<td>Documentation</td>
<td>6</td>
</tr>
<tr>
<td>Monitoring</td>
<td>7</td>
</tr>
<tr>
<td>Investigation</td>
<td>8</td>
</tr>
<tr>
<td>Containment</td>
<td>9</td>
</tr>
<tr>
<td>Remediation</td>
<td>10</td>
</tr>
<tr>
<td>Closing Incidents</td>
<td>11</td>
</tr>
<tr>
<td>Business Case for IR</td>
<td>12</td>
</tr>
</tbody>
</table>
Who is Part of Your Immediate Team

People and Groups

Who is part of your direct team?

- Incident response team
- Computer forensics
- Malware analysis
- Firewall and proxy team
- Endpoint protection
Who is in Your Extended Family

People and Groups

Who is part of your extended family?

- Helpdesk
- Network services
- Security architects
- Human Resources
- Legal
- Public Relations
- Crisis Communications
Who are Your Clients
People and Groups

Who are your internal and external clients?

- Business unit leaders
- Business partners
  - Vendors, dealers, suppliers, contractors
- Unions?
What Other Agencies Are Involved

People and Groups

- Law enforcement
- SEC, FCC, FTC, other TLAs
- CERTS
  - Force multiplier
  - Information clearing house
  - Additional monitoring and threat intelligence source
Working with IT may be a special case, and special challenge

- May own much of the infrastructure and budget
- Different definitions of “incident”
- Business continuity and 99% uptime at odds with IR
- Metrics may not align
Chain of Command
People and Groups

- Who supports you?
- Who can tell you what to do?
- Who can you tell what to do?
- Who do you need to communicate with?
- Who do you need help from?
Train Everyone
People and Groups

- External training
  - (e.g. SANS)
- Internal training
  - Tabletop exercises
  - Class or conference summaries
- What is common to all team members
- What is specific to certain team members/roles

- Train your organization (aka your sensors)
  - User security awareness
  - What to report, when, and how
  - Policy – BYOD, use of corporate resources, etc
Tying It All Together – The SOC

People and Groups

- **Structure**
  - IR, malware, forensics, threat intelligence, ...
  - What services are in, what services are out

- **Centralized or global**

- **All hazards**

- **Staffing**
  - Team composition
  - 8-5 or 24/7
<table>
<thead>
<tr>
<th>Working Assumptions</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is an Incident?</td>
<td>Investigation</td>
</tr>
<tr>
<td>Indicators and Threat Intelligence</td>
<td>Containment</td>
</tr>
<tr>
<td>People and Groups</td>
<td>Remediation</td>
</tr>
<tr>
<td>Planning and Prep</td>
<td>Closing Incidents</td>
</tr>
<tr>
<td>Documentation</td>
<td>Business Case for IR</td>
</tr>
</tbody>
</table>
Know Your Data
Planning and Preparation

- Know your data, where it is, where its been, its value, ....
  - Where it lives
  - How it moves
  - What is its value
  - Who values it
  - Know how to protect it at rest and in motion
  - Know how to monitor it
Resources Required - Technology

Planning and Preparation

- Ticketing systems
- Documentation systems
- SIEM
- Network and host monitoring tools
- Investigative tools – forensics, malware, ediscovery
- Laptops, desktops, screens, write blockers, ....
- Out of band communications
Resources Required – Physical Space

Planning and Preparation

- Normal work areas
- Abnormal work area - War Room
- Forensics lab
- Evidence storage
- Server room
- Whiteboards, displays, projectors, phones
Resources Required – Logistics
Planning and Preparation

- Credit cards, and permission to use them
- Hotels, travel arrangements
- Catering and kitchen facilities
- Comp time, overtime, flex time, play time
- Remote teams and/or partners
- Remote tools
Resources Required – Data
Planning and Preparation

Know and document your environment

• Asset database
  - Host to user or group
  - For fixed assets, device to physical location

• User database - user to role, business unit, location

• Network devices –
  - IP database - DHCP, DNS - IP to host
  - Bandwidth, protocols, services
<table>
<thead>
<tr>
<th>Working Assumptions</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is an Incident?</td>
<td>2</td>
</tr>
<tr>
<td>Indicators and Threat Intelligence</td>
<td>3</td>
</tr>
<tr>
<td>People and Groups</td>
<td>4</td>
</tr>
<tr>
<td>Planning and Prep</td>
<td>5</td>
</tr>
<tr>
<td>Documentation</td>
<td>6</td>
</tr>
<tr>
<td>Monitoring</td>
<td>7</td>
</tr>
<tr>
<td>Investigation</td>
<td>8</td>
</tr>
<tr>
<td>Containment</td>
<td>9</td>
</tr>
<tr>
<td>Remediation</td>
<td>10</td>
</tr>
<tr>
<td>Closing Incidents</td>
<td>11</td>
</tr>
<tr>
<td>Business Case for IR</td>
<td>12</td>
</tr>
</tbody>
</table>
Critical Documents

Critical documents and their volatility

- **Tactical Notes**: Volatile information, everyone responsible for keeping current, kept in a wiki or SharePoint.
- **Processes**: Day to day operations, lab management, firewall rule changes, .... Monitor and update regularly.
- **Org Chart**: The organization of the incident response team as well as the incident response team’s place in the larger organization.
- **Service Plans**: Service descriptions, high level delivery plans, and business relationship descriptions. Should only change after much thought.
- **Charter**: Role and responsibility of the incident response team. Most importantly, its authority to act. Not subject to change.
Have a plan, keep it up to date.

- If you cannot keep a complex, overly detailed plan up to date, start high and simple
- As your organization matures, so will your plans

You will need detailed plans to be mature, if only because the business process around you is mature and wants details from you

If you get too detailed, your plans will rapidly stop reflecting reality and will also be much more difficult to keep up to date
Why Written Plans are Important

- When something goes wrong, you don’t want to be asked “Why didn’t you follow the plan?”
- Good for delegating or involving outside resources
- Good for onboarding new staff
- Good for “I’ve been awake for 36 hours, am out of coffee, and just got another incident.”
- Good for diplomatically telling someone that their request is out of scope
Other Documentation Thoughts

- Don’t redefine terms
- Use plain English (or German, or Arabic, or ....)
- Use clean, informative graphics
- Create templates for common reports
- Nothing goes according to plan, so Sempre Gumbi
Severity Levels

Documentation

- Best used to frame discussions and do triage
- Do not get bogged down in detail, many variables are too hard to calculate

- Items to consider:
  - Number of systems compromised
  - Confidential or sensitive data
  - Reporting requirements
  - Mission critical systems
  - Resources available
Metrics

You cannot manage what you cannot measure

➢ Good for concise, regular communication upwards
➢ Tune metrics to stakeholders
➢ Metrics should be actionable
➢ Bad if “gamed” – Metrics will define your operations
➢ Possible metrics
  • Number of incidents
  • Number of malware samples submitted
  • Time to detect
  • Time to remediate
Keep Reporting In Mind

Status Report
C-Level Briefing
TLAgency Report
Metrics
Remediation Plan

C-Levels
Operational Management
Internal
External
Team
<table>
<thead>
<tr>
<th>Working Assumptions</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is an Incident?</td>
<td>2</td>
</tr>
<tr>
<td>Indicators and Threat Intelligence</td>
<td>3</td>
</tr>
<tr>
<td>People and Groups</td>
<td>4</td>
</tr>
<tr>
<td>Planning and Prep</td>
<td>5</td>
</tr>
<tr>
<td>Documentation</td>
<td>6</td>
</tr>
<tr>
<td>Monitoring</td>
<td>7</td>
</tr>
<tr>
<td>Investigation</td>
<td>8</td>
</tr>
<tr>
<td>Containment</td>
<td>9</td>
</tr>
<tr>
<td>Remediation</td>
<td>10</td>
</tr>
<tr>
<td>Closing Incidents</td>
<td>11</td>
</tr>
<tr>
<td>Business Case for IR</td>
<td>12</td>
</tr>
</tbody>
</table>
The Big Picture
Monitoring

Monitoring should be done as soon as possible.

- It doesn’t need to cost a lot
- It helps you answer other questions (e.g. tools to use)
- It provides actionable data now
- It doesn’t depend on many other factors
- It adapts to a dynamic environment, which any network is
- Setting it up teaches you about your environment

You can’t tell what is going on in your network without monitoring

You cannot tell if your controls are working without monitoring
What to Monitor - Host data

Monitoring

- Antivirus
- SCCM
- Event logs
- Registry changes
- New services
What to Monitor - Network data

Monitoring

- Event, content, full session, statistical
- IDS
- Netflow
- Firewall
- Proxy
What to Monitor - Application data

- Active directory
- Web server and web application logs
- Source code repository access logs
- Database logs
Users are Sensors - Internal
Monitoring

Internal Users

- Email
- Phone
- Trouble tickets
- Hallways
External Users – Joe Blow, TLAs, business partners ...

- Email
- Phone
- Blogs
- Pastebin
- Shodan HQ
- Conferences
- Social media
Monitor the Monitors

Monitoring

- Security of monitoring systems
- Health of monitoring system
- Testing the monitoring system
- Access and ethics
Continuous vs. Security Monitoring

- Continuous monitoring
  - Big in .gov and NIST
  - Monitoring for vulnerabilities

- Security monitoring
  - Identify activity that may indicate malicious behavior
Process vs. Hunting

Monitoring

- Monitor via process
  - Indicators of compromise
  - Honeypots
  - IDS alerts

- Hunting - incident discovery
  - Let analysts go look for stuff that is of interest to them
Bring Your Own Devices

Monitoring

– **Legal**
  * What can you legally watch and collect
  * Get this addressed early and in writing
  * Keep pushing for more access

– **Device**
  * What can you require for endpoint security
  * Access to logs
  * Lots of noise, unknown default state

– **Network**
  * Often wireless, harder and easier to monitor
Lessons Learned & Threat Intelligence

Monitoring

Need to keep monitoring environment current

- Fold in threat intelligence
- Add lessons learned from after action
- Engage with security architects to bake in monitoring
<table>
<thead>
<tr>
<th>Working Assumptions</th>
<th>Monitoring</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is an Incident?</td>
<td>Investigation</td>
<td>2</td>
</tr>
<tr>
<td>Indicators and Threat Intelligence</td>
<td>Containment</td>
<td>3</td>
</tr>
<tr>
<td>People and Groups</td>
<td>Remediation</td>
<td>4</td>
</tr>
<tr>
<td>Planning and Prep</td>
<td>Closing Incidents</td>
<td>5</td>
</tr>
<tr>
<td>Documentation</td>
<td>Business Case for IR</td>
<td>6</td>
</tr>
</tbody>
</table>
The Questions that Must Be Answered
- Who, what, when, why, where, how

Scope Determination
- Monitor and update

Root Cause Analysis
- May not be necessary every time
Triage – How Bad, What Next

Investigate

- Very quick process
- Validate, investigate, escalate
- Define and use severity levels to guide triage process
  - How bad is it
  - What is the indicator
  - Adjust over time
  - Helps with resource allocation
What Happened, and is Happening

Investigate

- Network – FOR572
- Host – FOR408, FOR508
- Malware – FOR610
Threat Actors and Attribution

Investigate

- Do you really need attribution
- How do you investigate threat actors and indicators
- No SANS course ... yet
- pDNS, VirusTotal, Google, CRITS, ....
<table>
<thead>
<tr>
<th>Working Assumptions</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is an Incident?</td>
<td>2</td>
</tr>
<tr>
<td>Indicators and Threat Intelligence</td>
<td>3</td>
</tr>
<tr>
<td>People and Groups</td>
<td>4</td>
</tr>
<tr>
<td>Planning and Prep</td>
<td>5</td>
</tr>
<tr>
<td>Documentation</td>
<td>6</td>
</tr>
<tr>
<td>Monitoring</td>
<td>7</td>
</tr>
<tr>
<td>Investigation</td>
<td>8</td>
</tr>
<tr>
<td>Containment</td>
<td>9</td>
</tr>
<tr>
<td>Remediation</td>
<td>10</td>
</tr>
<tr>
<td>Closing Incidents</td>
<td>11</td>
</tr>
<tr>
<td>Business Case for IR</td>
<td>12</td>
</tr>
</tbody>
</table>
Stop The Bleeding

Containment

- Short Term
- Long Term
Keep It From Spreading

Containment

- Business Consideration
- Communications
- Monitoring
  - You know what to look for now
- Contain vs Investigate
<table>
<thead>
<tr>
<th>Working Assumptions</th>
<th>1</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is an Incident?</td>
<td>2</td>
<td>Investigation</td>
</tr>
<tr>
<td>Indicators and Threat Intelligence</td>
<td>3</td>
<td>Containment</td>
</tr>
<tr>
<td>People and Groups</td>
<td>4</td>
<td>Remediation</td>
</tr>
<tr>
<td>Planning and Prep</td>
<td>5</td>
<td>Closing Incidents</td>
</tr>
<tr>
<td>Documentation</td>
<td>6</td>
<td>Business Case for IR</td>
</tr>
</tbody>
</table>
Return Affected Systems to Normal

Remediation

Technically simple, logistically complex

- Execution plan
- Tactical vs Strategic
- Secure Communications
- Resources Required
- Scheduling
- Mini D-Day
They’re trying to get back in

- You have some indicators
- Unlikely that they will go with 100% new TTP
- Heightened state of awareness
- Remember kill chains

Monitor completeness of remediation efforts
<table>
<thead>
<tr>
<th>Topic</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Assumptions</td>
<td>1</td>
</tr>
<tr>
<td>What is an Incident?</td>
<td>2</td>
</tr>
<tr>
<td>Indicators and Threat Intelligence</td>
<td>3</td>
</tr>
<tr>
<td>People and Groups</td>
<td>4</td>
</tr>
<tr>
<td>Planning and Prep</td>
<td>5</td>
</tr>
<tr>
<td>Documentation</td>
<td>6</td>
</tr>
<tr>
<td>Monitoring</td>
<td>7</td>
</tr>
<tr>
<td>Investigation</td>
<td>8</td>
</tr>
<tr>
<td>Containment</td>
<td>9</td>
</tr>
<tr>
<td>Remediation</td>
<td>10</td>
</tr>
<tr>
<td>Closing Incidents</td>
<td>11</td>
</tr>
<tr>
<td>Business Case for IR</td>
<td>12</td>
</tr>
</tbody>
</table>
When Do You “Call” the Incident?

Closing Incidents

- Positive closure
  - Don’t let it just fade out
  - Don’t call it because something else came up
- Positive hand off of lessons learned
- Closure with all involved partners
- Expectations met, or reset
- Not over until the documentation is done
Lessons Learned

Closing Incidents

- No fault, open discussion
- As close to end as possible
- Review CIRT documentation and update
- Update threat intelligence
- Update monitoring systems
- Positive hand off of lessons learned
Documentation

Closing Incidents

- What documents do you need
- How much time and effort for documentation
  - What expectations are you setting
  - Value of templates
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Assumptions</td>
<td>1</td>
</tr>
<tr>
<td>What is an Incident?</td>
<td>2</td>
</tr>
<tr>
<td>Indicators and Threat Intelligence</td>
<td>3</td>
</tr>
<tr>
<td>People and Groups</td>
<td>4</td>
</tr>
<tr>
<td>Planning and Prep</td>
<td>5</td>
</tr>
<tr>
<td>Documentation</td>
<td>6</td>
</tr>
<tr>
<td>Monitoring</td>
<td>7</td>
</tr>
<tr>
<td>Investigation</td>
<td>8</td>
</tr>
<tr>
<td>Containment</td>
<td>9</td>
</tr>
<tr>
<td>Remediation</td>
<td>10</td>
</tr>
<tr>
<td>Closing Incidents</td>
<td>11</td>
</tr>
<tr>
<td>Business Case for IR</td>
<td>12</td>
</tr>
</tbody>
</table>
Business Case for Incident Response

Who Is Involved?

- Preparation – involves the entire organization
- Identification – CIRT, IT, and business unit
- Contain – CIRT, IT, and business unit
- Eradicate – CIRT and IT
- Remediate – CIRT, IT, and business unit
- Lessons learned - involves the entire organization
Business Case for Incident Response

- Metrics

- Cost of an incident
  - Be careful if you calculate or report this
Contact
David Kovar

dkovar@gmail.com
@dckovar
http://integriography.wordpress.com/