TAOSECURITY
THE WAY OF DIGITAL SECURITY

CIRT-Level Response to Advanced Persistent Threat

Richard Bejtlich (richard@taosecurity.com)

I. Assumptions

- You have discovered, or learned from an external party, that your organization is an Advanced Persistent Threat (APT) victim. Call the time of discovery D-Zero.
- You care. You take compromise *personally.* At least some others in your organization do too, or can be convinced to care.
- You are at least hopeful that your organization can take steps to defend itself.

II. Critical Themes

- "Prevention eventually fails." (I coined this phrase in 2004 when I published The Tao of Network Security Monitoring. This is not a coincidence!)
- Persistent threats are named as such because they either
  - Maintain their presence in the victim organization or
  - Repeatedly seek to regain that presence
- Therefore, "winning" against APT does not mean preventing compromise. Rather, winning means:
  - *Increasing the cost the adversary must pay for each MB stolen* (credit: Tony Sager, NSA)
  - *Predicting the adversary's next move* (credit: Kevin Mandia, MANDIANT)
  - *Tracking the adversary as he changes tools, tactics, and procedures*
  - *Intrusion suppression* is one way to describe counter-APT operations (credit: Robert Rounsavall from Terremark)

III. Recent quotes on APT by Kris Harms from Mandiant (FIRST 2010 conference)

- "Compliance is the floor upon which you're going to fall when you get hacked."
- "Today a B [grade] is not good enough."
- "Do not get in a battle over knowledge of Windows with an intruder. You will lose."

IV. During the first hour after D-Zero.

- Document everything. Write everything down, in a notebook, because *facts* need to become your currency, not *beliefs*.
- Change communication patterns when discussing the incident. Don't use email. Don't use VoIP. Consider your computing infrastructure untrustworthy. Communicate in person or use cell phones.
- Activate your incident response plan. If you don't have one, contact a small group of trusted representatives from IT, security, legal, and other groups you feel should be involved. Share what you know and institute strict information sharing policies.

V. During the first day after D-Zero.

- Provision and configure alternative computing infrastructure. Build your own IR laptop running an operating system you trust and feel confident configuring. Start with clean hardware and new media. Build the gear off the organization's network.
- Develop trusted means of electronic communication among IR members.
- Inventory the security and IT evidence at hand to determine what data sources you possess. The goal is to gather data that corroborates or expands upon the indicator(s) of compromise associated with the initial APT discovery.

VI. During the first week after D-Zero.

- Decide if you need external help. Factors which encourage enlisting experienced consultants include:
  - Lack of staff in your organization
  - Lack of leadership buy-in
  - Lack of technical expertise in your organization
- Provide an initial briefing to decision makers. Key points should include:
  - *Facts* available -- don't speculate!
  - *Rules of engagement* to try to preserve operational security (OPSEC)
  - *Initial plan* to address the APT incident, stressing that *once APT is found, it's generally a problem forever*
- Analyze available evidence for indicators of compromise.
- Begin deployment of additional data collection systems to improve available evidence. Options include:
  - Deploy network security monitoring platforms at key network egress locations
  - Deploy log forwarding and log storage platforms to collect logs from critical computers
  - Deploy live response scripts to collect key data from suspected victims
  - Selectively shut down and image hard drives from suspected victims

VII. During the first month after D-Zero.

1. Determine the scope of the incident. Develop a victim list, identify stolen credentials, recognize internal and external communication methods, etc.
2. Evaluate the effectiveness of existing security instrumentation and plan for deployment of improved capabilities.
3. Plan a remediation effort. The focus of the remediation should be to, simultaneously, contain victims, change credentials, deny communication, etc. Plan the effort on equipment not associated with the victim organization, or expect the plan to fall into adversary hands. Prepare leaders to accept that even a "successful" remediation is likely to be only the first battle in a protracted campaign.

VIII. During the first year after D-Zero.

- Evaluate the effectiveness of the IR capability. Plan to justify and then hire additional personnel, and professionalize the team.

- Institutionalize counter-APT activities within the organization. Provide threat briefings to senior leaders and gain support for security initiatives.
- Develop and embed counter-APT security improvements into organizational security programs and budgets. Using the lessons and data learned during the first few months of counter-APT operations, build plans based on facts, recognized gaps, and expected improvements.
- Contact peer organizations to share tools, techniques, and procedures.
- Expand the security instrumentation program as team resources allow.
- Begin hiring additional staff as budgets permit.

IX. During the second year after D-Zero.

- If one does not already exist, create a Red-Blue Team to conduct adversary simulation/replication exercises and vulnerability and exposure assessments. Identify organizational weaknesses.
- Develop an internal security intelligence capability to look beyond technical aspects of APT intrusions.
- Contribute knowledge of counter-APT activities to broader, trusted peers.
- Continue hiring additional staff as budgets permit.

X. Containment vs Honeynet: Aside from selective shut down to collect hard drive images (and live collection is also an option), *for new APT victim* organizations, I do not recommend immediately disconnecting suspected victims from the network. Why?

1. You are unlikely to know all of the victims at this stage in the incident response. Disconnecting the few victims you know fails to truly deny the adversary.
2. Disconnecting the few victims you know removes the main source of intelligence on adversary activity. Disconnecting the few victims you know usually hampers IR team efforts to learn the scope of the intrusion.
3. The adversary will definitely notice when the organization disconnects multiple victims from the network. This action will likely prompt the adversary to change tactics and further frustrate IR actions.

So when do you start disconnecting victims as policy? Answer: when you begin to meet your *winning criteria*.

XI. Suggested CIRT Structure.

I organized GE-CIRT using the following structure.

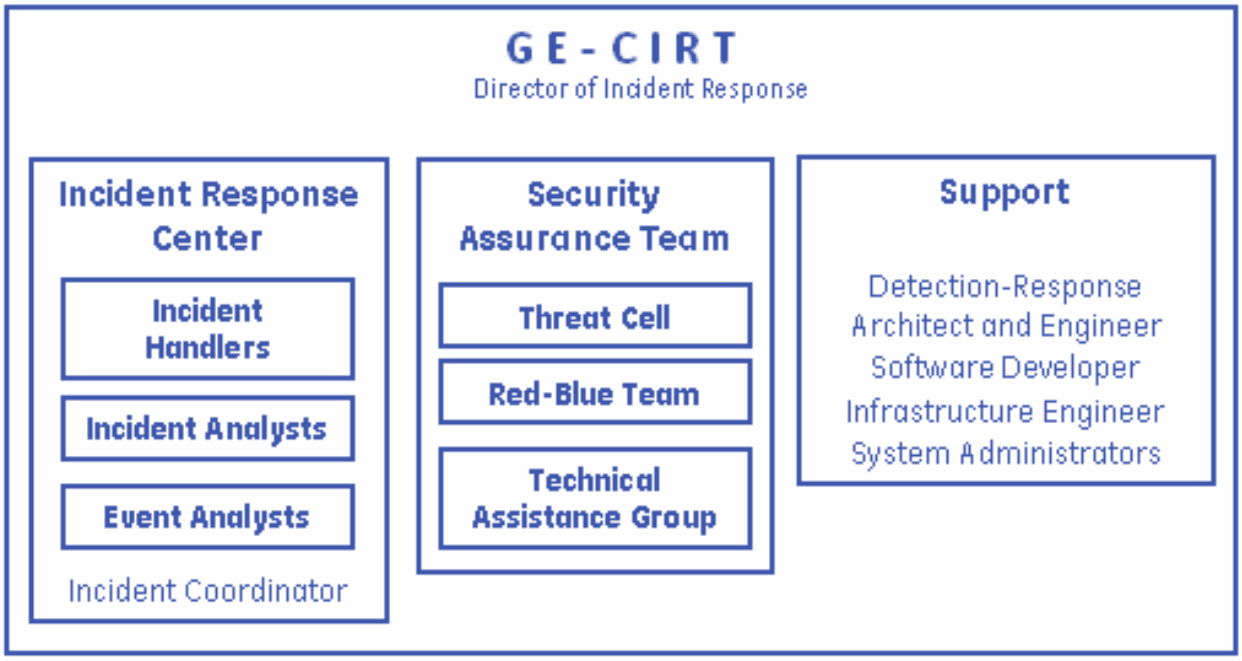


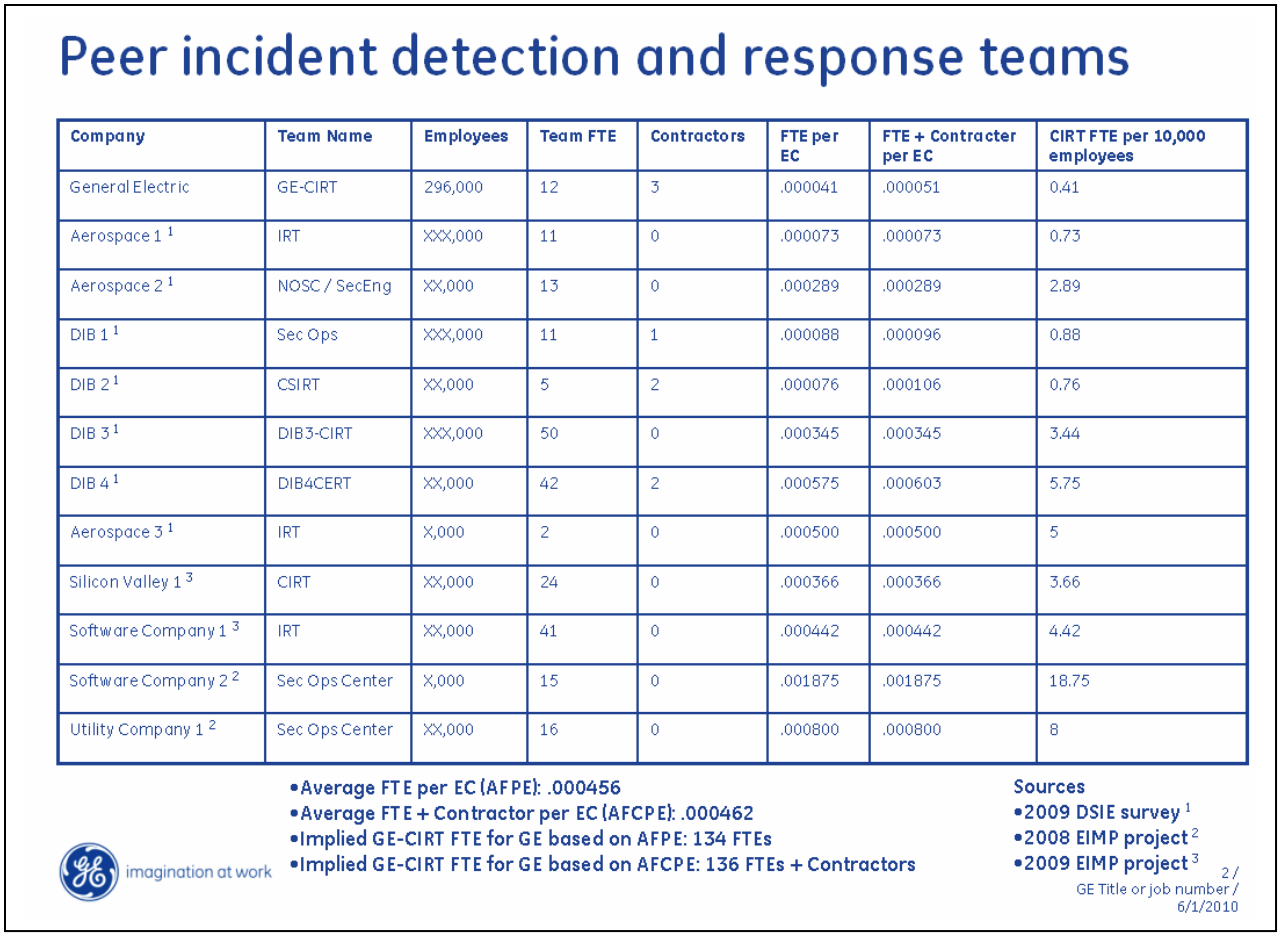
Figure 1. GE-CIRT Structure

XII. Suggested Hiring Priorities

1. Incident Handlers - subject matter experts who will establish early credibility and competency
2. Event Analysts - 24x7 coverage to support more routine work
3. Incident Analysts - assume the natural balance between IH and EA work
4. Support team - transfer design, build, and run activities from the IRC to Support
5. Threat cell - profile adversaries and professionalize reporting
6. Blue team - provide collaborative assessment assistance
7. Technical Assistance Group - internal security consulting
8. Incident Coordinator - quality control for IRC operations
9. Red team - adversary replication and simulation

XIII. Headcount Justification.

In 2009 I surveyed peer CIRTs and collected the following data. Using the information below I calculated that GE-CIRT required 134 team members to meet the average size of our peers. I told our CIO that I would be happy to "drop the 1" and reach 34 people. I presented a version of the CIRT structure showed earlier with numbers attached to each role. Later when our CIO, CTO, and CISO made the decision to increase team size, they used my documentation.



Peer incident detection and response teams

Company	Team Name	Employees	Team FTE	Contractors	FTE per EC	FTE + Contracter per EC	CIRT FTE per 10,000 employees
General Electric	GE-CIRT	296,000	12	3	.000041	.000051	0.41
Aerospace 1 [1]	IRT	XXX,000	11	0	.000073	.000073	0.73
Aerospace 2 [1]	NOSC / SecEng	XX,000	13	0	.000289	.000289	2.89
DIB 1 [1]	Sec Ops	XXX,000	11	1	.000088	.000096	0.88
DIB 2 [1]	CSIRT	XX,000	5	2	.000076	.000106	0.76
DIB 3 [1]	DIB3-CIRT	XXX,000	50	0	.000345	.000345	3.44
DIB 4 [1]	DIB4CERT	XX,000	42	2	.000575	.000603	5.75
Aerospace 3 [1]	IRT	X,000	2	0	.000500	.000500	5
Silicon Valley 1 [3]	CIRT	XX,000	24	0	.000366	.000366	3.66
Software Company 1 [3]	IRT	XX,000	41	0	.000442	.000442	4.42
Software Company 2 [2]	Sec Ops Center	X,000	15	0	.001875	.001875	18.75
Utility Company 1 [2]	Sec Ops Center	XX,000	16	0	.000800	.000800	8

Figure 2. CIRT Staffing Survey

XIV. Incident Cycle.

Many organizations focus most of their security resources on the top half of the cycle, shown in the following figure. They devote resources to planning and resisting, but do not know what to do when an incident occurs. Alternatively, they adopt what I call a "volunteer fire fighter" model. When they detect an incident, the security planners and resisters transition from their normal roles to that of incident responder. When the incident is "over," they transition back. Unfortunately, this model fails when 1) incidents never really end and 2) professionals are required to combat modern threats.

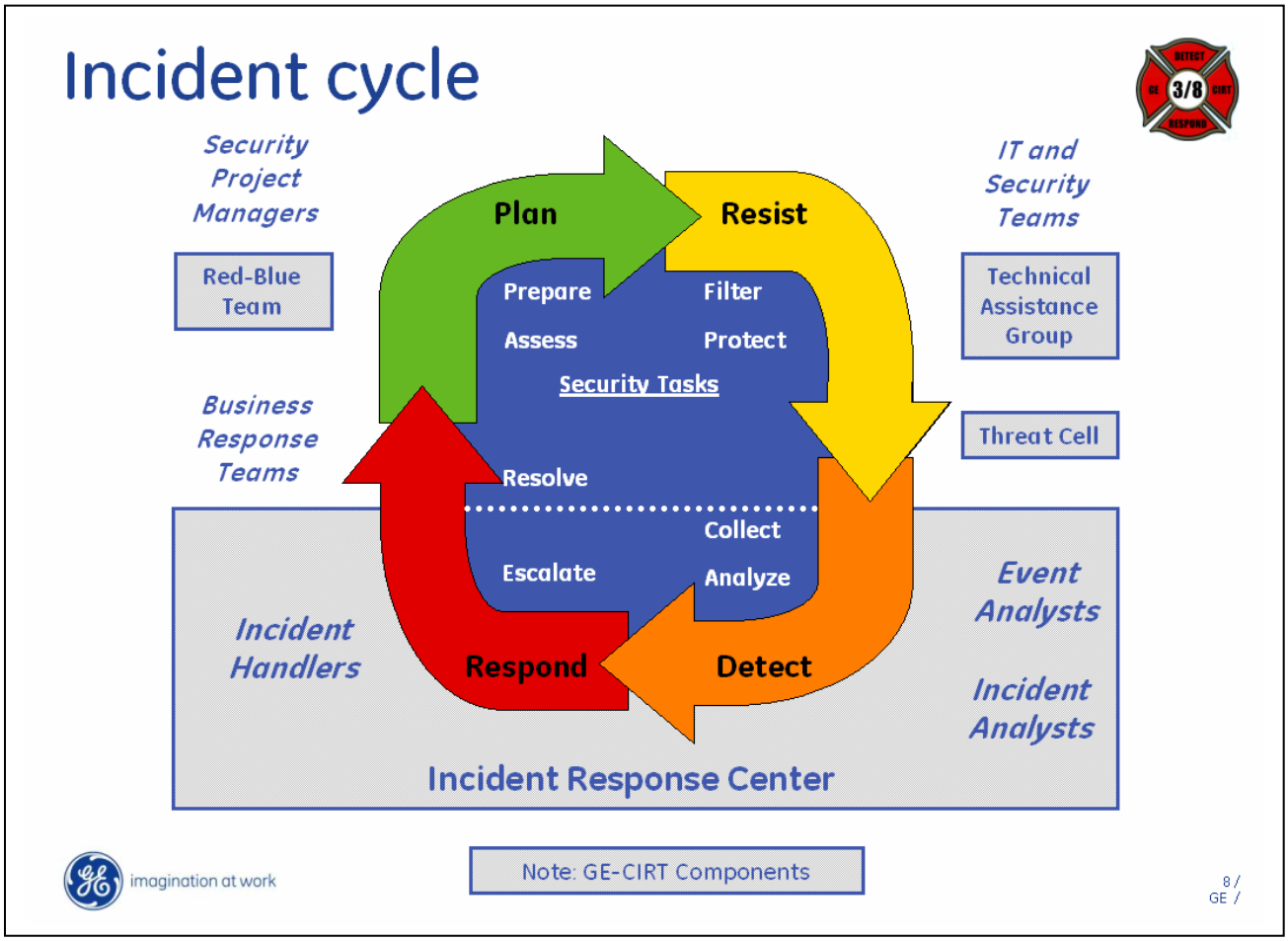


Figure 3. Incident Cycle

XV. Recommended APT Reading.

- M-Unition (MANDIANT blog): http://blog.mandiant.com/
- Mike Cloppert (via SANS): http://blogs.sans.org/computer-forensics/author/mikecloppert/