Building a Fortune Five CIRT Under Fire

by Richard Bejtlich, 01 June 2010

Q. What is the goal of CIRT activity?

A. The CIRT should not exist for its own good, nor should it continuing growing as incidents increase. My vision for GE-CIRT is "Fire Fighter to Fire Marshall." In other words, we detect and respond to incidents so we can stop intruders but also transition lessons to improve Company security. In other words:

- The Incident Response Center detects and responds to intrusions.
- The Security Assurance Team applies those lessons to the Company to improve security.
- The Support team designs, builds, and runs infrastructure to enable the IRC and SAT.

I depicted my vision using the following graphic.

GE-CIRT vision: fire fighters to fire marshalls through visibility

Figure 1. GE-CIRT Vision

Q: How do I justify building a Computer Incident Response Team?

A. Many CIRTs are built to respond to a crisis. We all prefer to have a team ready to deal with a crisis, however! I offer the following "13 C's" as items you may find helpful when talking to those with budget and authority.

1. **Crisis**. Something bad happens. Although this is the worst way to justify a program, it is often very effective.

2. **Compliance**. An external force compels a security program. This is also not a great way to justify a program, because resources are often misallocated.

3. **Competitiveness**. Please see my blog post Forget ROI and Risk. Consider Competitive Advantage (taosecurity.blogspot.com/2010/03/forget-roi-and-risk-consider.html).

4. **Comparison**. If your company security team is 10% the size of the average peer organization size, it's not going to look good when you have a breach and have to justify your decisions.

5. **Cost**. It's likely that breaches are more expensive than defensive measures, but this can be difficult to capture.

6. **Customers**. It seems rare to find customers abandoning a company after a breach. People still shop at TJX brands. Still, you may find traction here. Compliance is supposed to protect customers but it often is insufficient.

7. **Constituents**. I use this term to apply to internal parties. Large companies often provide services to other business units.

8. **Controllership**. Is your organization well-governed? Can it account for the state of its systems for auditors and so forth?

9. **Conservation**. This is a play on "green IT." What has a lower carbon footprint: 1) flying consultants all over the world to handle incidents, or handling them remotely by moving data, not people?

10. **Consolidation or Centralization**. These themes are likely to enable specialization, more effective internal resource allocation, and improve defenses.

11. **Confidence**. Confidence applies to all parties involved. Can you trust your data?

12. **Counting**. This is a plug for metrics.

13. [Securities and Exchange] **Commission**. This is a play on the 10k- forms shareholders receive in the mail. Please see the linked post for more details.

Q. How can I collect evidence to demonstrate that my organization has a problem worthy of a CIRT?

A. Monitor first. (See Bruce Schneier's 2001 article in Crypto Gram, www.schneier.com/crypto-gram-0107.html#5). Recommended proof-of-concept, free monitoring strategies include:

- Deploy passive Network Security Monitoring sensors using Sguil (www.sguil.net). (See The Tao of Network Security Monitoring, www.taosecurity.com/books.html).
- Collect logs from critical servers in a free instance of Splunk (www.splunk.com, 500 MB/day limit).
- Install OSSEC (www.ossec.net) on a sample of critical servers.

The key is to collect information so you are basing decisions on Fact not Fiction. I use the following image to show a security program that is focused but not paying attention to real threats. By monitoring **your environment** you collect information that matters to **your organization**, not what appears on someone's blog or Web site.

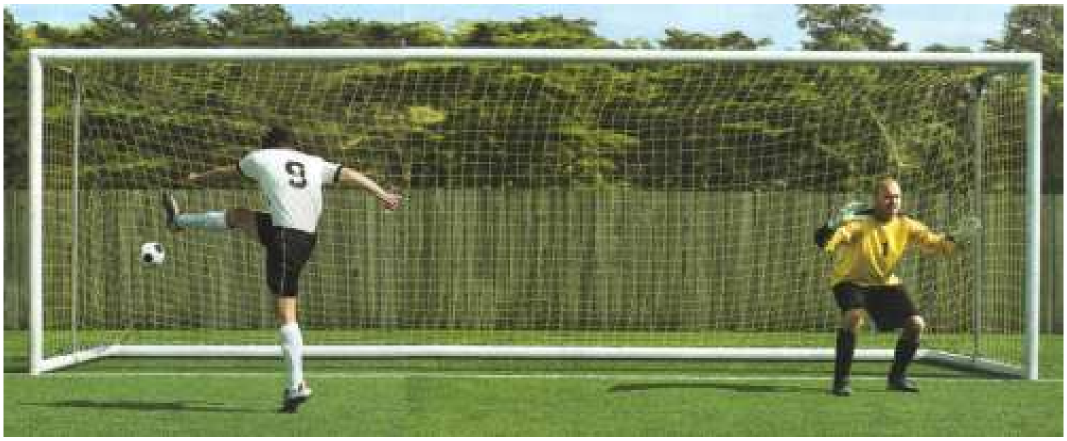


Figure 2. "Soccer-goal Security"; Credit to a 2005 Hitachi storage ad in Network Computing magazine

Q. How should my CIRT be structured?

A. The following depicts the structure of GE-CIRT. I recommend a balance of operations (IRC), project- and longer-term support (SAT) and Support functions.

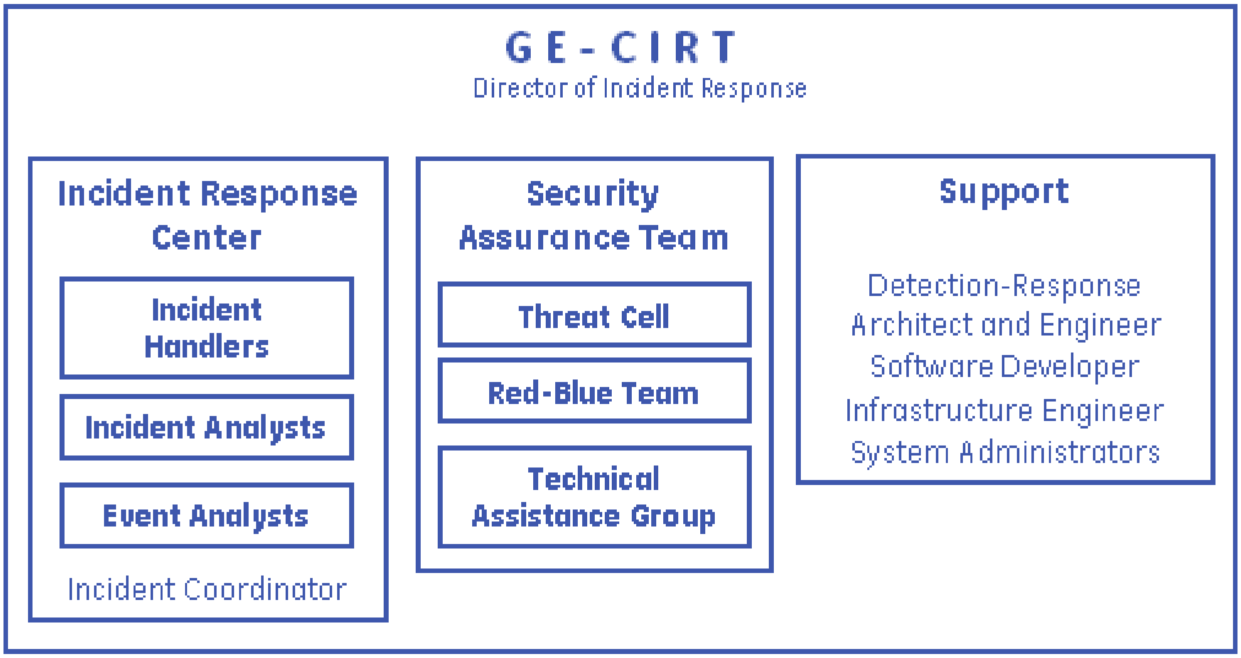


Figure 3. GE-CIRT Structure

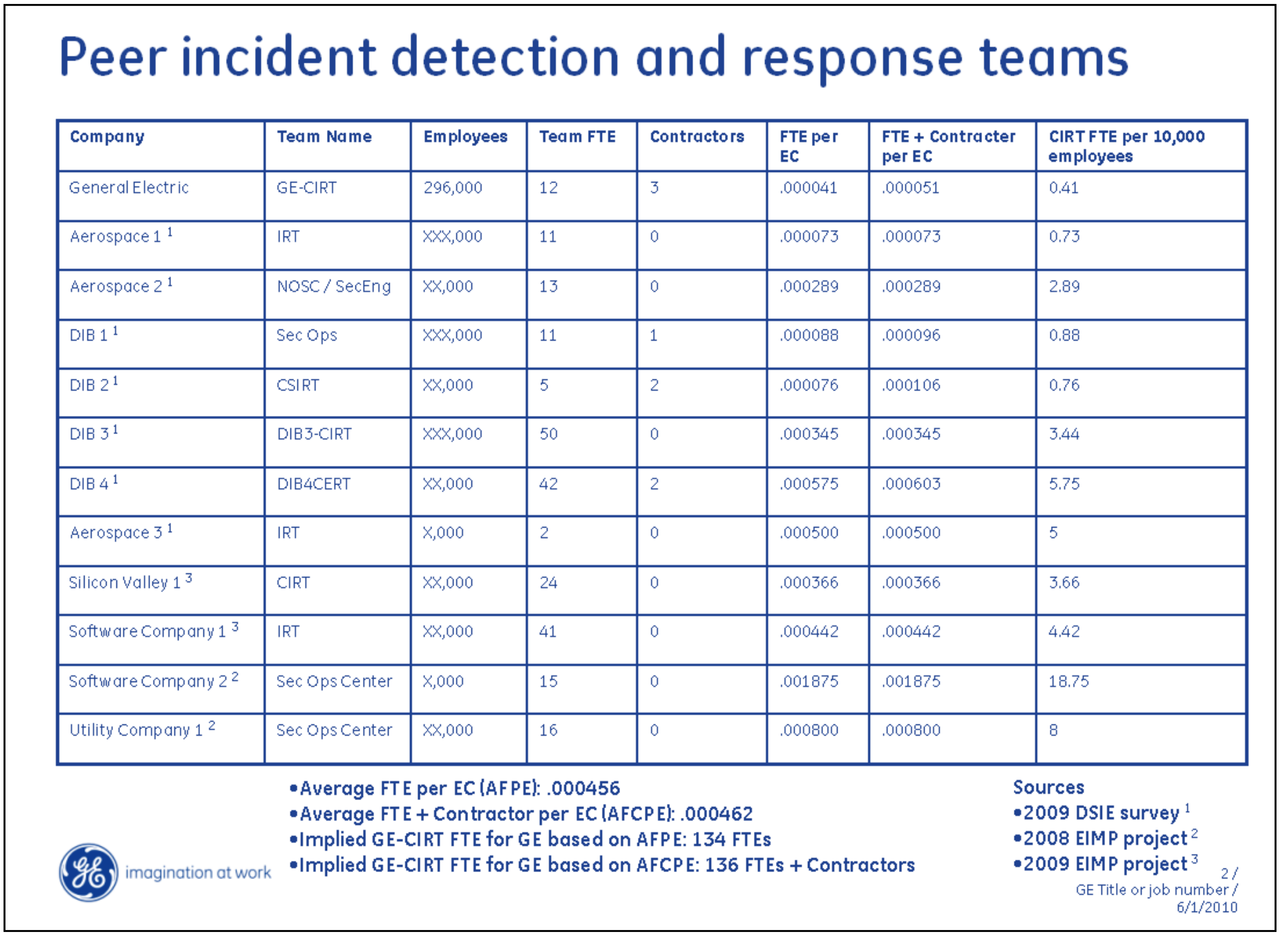
Q. What should be my hiring priorities?

A. I recommend these 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

Q. How can I justify headcount?

A. 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

- **Average FTE per EC (AFPE): .000456**
- **Average FTE + Contractor per EC (AFCPE): .000462**
- **Implied GE-CIRT FTE for GE based on AFPE: 134 FTEs**
- **Implied GE-CIRT FTE for GE based on AFCPE: 136 FTEs + Contractors**

Sources
- **2009 DSIE survey [1]**
- **2008 EIMP project [2]**
- **2009 EIMP project [3]**

imagination at work

2 /
GE Title or job number /
6/1/2010

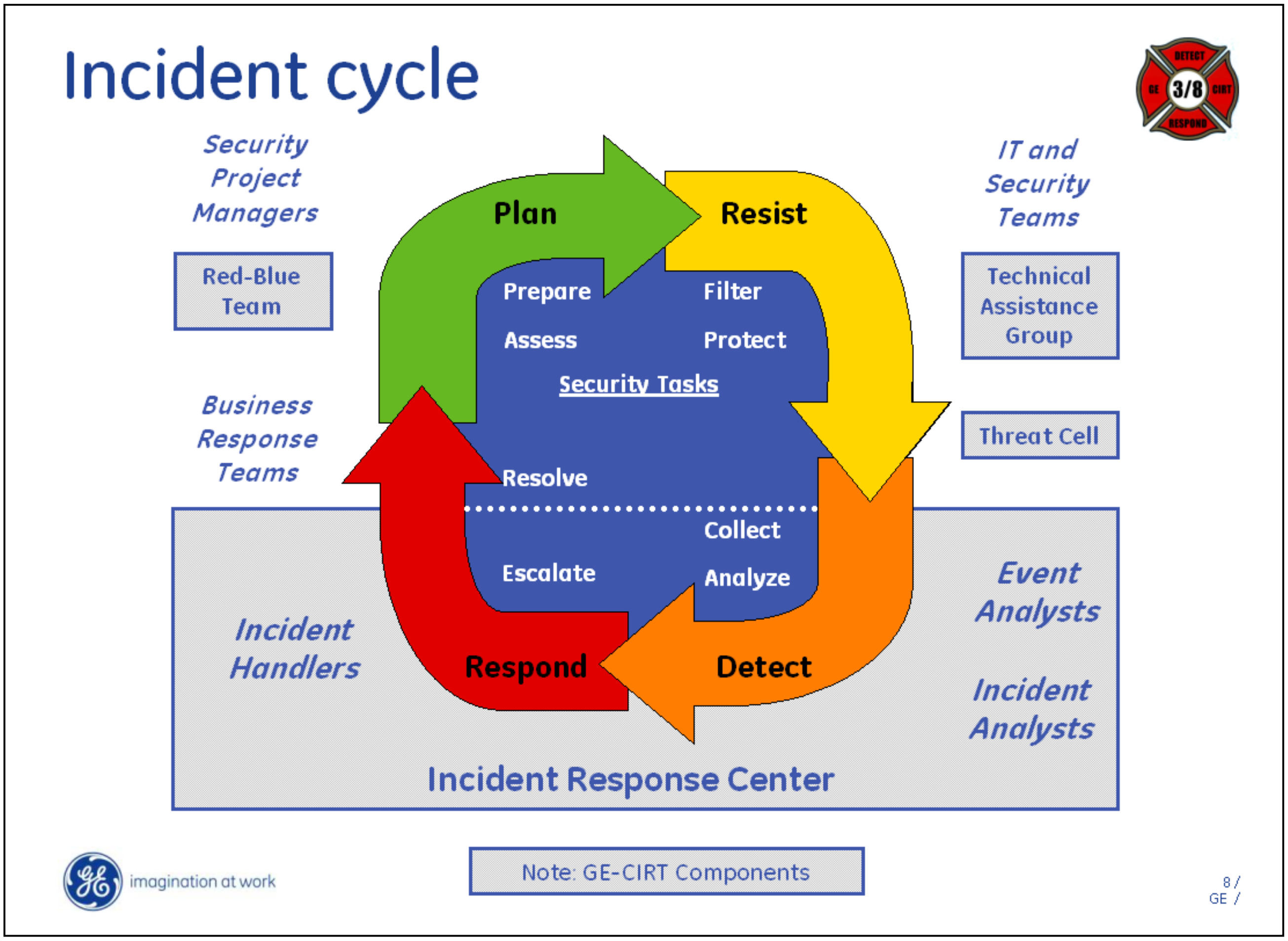
Figure 4. CIRT Staffing Comparison, 2009

Q. How does my CIRT fit into the overall organization's security structure?

A. Our Company security team focuses on four functions:

1. Governance and policy
2. Identity and access management
3. Security operations
4. Incident response

Within incident response, our Company CIRT (GE-CIRT) collaborations with Business Response Teams as shown.



Incident cycle

Security Project Managers

Red-Blue Team

Business Response Teams

IT and Security Teams

Technical Assistance Group

Threat Cell

Plan

Resist

Prepare

Filter

Assess

Protect

Security Tasks

Resolve

Collect

Escalate

Analyze

Respond

Detect

Incident Handlers

Event Analysts

Incident Analysts

Incident Response Center

imagination at work

Note: GE-CIRT Components

8 /
GE /

Figure 5. Incident Cycle

Many organizations focus most of their security resources on the top half of the cycle. 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.

Q. How do I describe what my CIRT does?

A. I believe it is imperative for a CIRT to provide **reporting** and not **tools**. CIRTs should provide a service, namely indicator analysis that results in **actionable reporting to Constituents**. In the figure below, I show that our CIRT analyzes a variety of indicators which result in reports to Constituents. We follow a Collection -> Analysis -> Escalation -> Response process. Notice that appears in the prior figure as well.

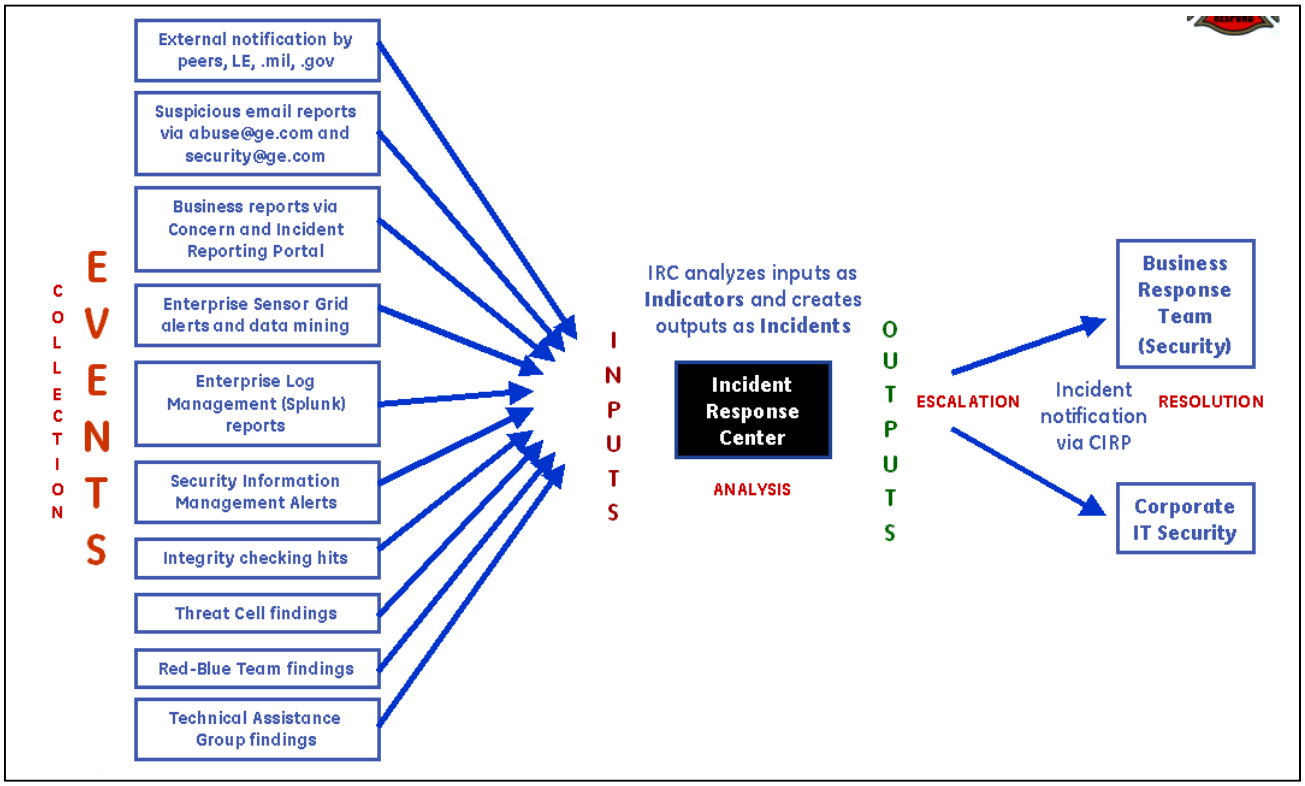

External notification by peers, LE, .mil, .gov
Suspicious email reports via abuse@ge.com and security@ge.com
Business reports via Concern and Incident Reporting Portal
Enterprise Sensor Grid alerts and data mining
Enterprise Log Management (Splunk) reports
Security Information Management Alerts
Integrity checking hits
Threat Cell findings
Red-Blue Team findings
Technical Assistance Group findings
COLLECTION
EVENTS
INPUTS
IRC analyzes inputs as Indicators and creates outputs as Incidents
Incident Response Center
ANALYSIS
OUTPUTS
ESCALATION
Incident notification via CIRP
RESOLUTION
Business Response Team (Security)
Corporate IT Security

Figure 6. Incident Response Center Collection -> Analysis -> Escalation -> Resolution Process

Q. What did I pursue FIRST membership?

A. I pursued FIRST membership for multiple reasons.

1. Having been a FIRST member in the Air Force and at Foundstone, I believed that professional incident responders were FIRST members.
2. I believed FIRST membership would help justify some of our team initiatives. For example, we made a case for a separate, isolated malware analysis network and environment.
3. Applying for FIRST membership forced us to document a variety of processes. We were required to consider how we handled sensitive information from third parties, for example.
4. I believed FIRST membership could be a differentiating factor when recruiting talent.
5. FIRST members share operational practices and information through mailing lists and conferences.

Q. What advice on team-building can you provide?

A. I recommend the following.

- Create a **team logo**. Before I ever had a team I created our logo.
- Create a **team name**. I chose "GE-CIRT" because it would be recognized by other incident responders.
- Be a **leader**, not a manager. Read my post Everything I Need to Know About Leadership I Learned as a Patrol Leader (taosecurity.blogspot.com/2010/05/everything-i-need-to-know-about.html)
- If you are not making progress on executing your vision **within a year**, consider another role.
- Create **documents** justifying your team and have them ready when asked.
- Use **time-based metrics** to explain workload. For example, if it takes 2 weeks for your analysts to review indicators, and that figure continues to increase, use that metric to justify additional hires. It's similar to a manufacturing situation, except the output is incident reporting.