Let Espionage Drive Your Security

APPLYING INTEL AGENCY TRADECRAFT AND BEST PRACTICES TO MAXIMIZE YOUR ENTERPRISE CYBER SECURITY

Steven Bay
Booz | Allen | Hamilton
The Problem

We get hacked ... But we can’t do anything in retaliation.

There is little we can do to make it painful for the hackers

- We can’t hack back
- Attribution is hard and never exact
- We can’t prosecute (mostly)
- We can’t freeze bank accounts (we’re not the government)
- ...
So we build a “Castle on a Hill”

Active defense is our only option:
- Firewalls
- Multi-Tiered Networks
- IDS and Monitoring Systems
- Security Operations
- Analytics
- DLP / Encryption
- ...

But this gets us no closer to knowing what’s coming or how to prepare.
Intelligence is key: Know your enemy

Where is your organization?

- Do you know your networks? Do you see what is going on?
- Do you know who the largest threats are to your org?
- Do you know what malware is out there that is likely to affect you?
- Are your employees trained? Do they know what to look for?
- What are the trends in hacking? How are attackers operating?

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle”

— Sun Tzu
How do we know our enemy?

We must think like them.

If you were the adversary, how would you hack into the network?
How would you get the information you need?

Starting with that in mind, you can build an intel program that fits your organization’s goals and budget

The key is applying best intelligence practices learned from the Intelligence Community married with corporate information security
Who/what is your biggest threat?

1. Insider Threat: A common threat
   a. Malicious Intent
   b. Unwitting user

2. External: Threat depends on your company/industry

Your intel capability must include internal data. Your intel team must be synced with the SOC.
Espionage Driven
Want your IC
China is the major player
Do you have anything of value to them?

Financially Driven
Want your company’s $$, your customer’s $$, and anything they can monetize

Driven by a Cause
Loud, want attention.
Seek to embarrass your company or make you less desirable to consumers

Advanced Tech
Pharma / Health
Financial Services
Defense
Energy

Retail
Services (Consumer)
Financial Services
Health

Defense
Police
Oil & Gas
Counter to a Cause
Large Corporations
Opinions and approaches to intel

- CTI is trendy
- Newly required by many regulatory and standards bodies
- Some think it’s a waste of money or see little return from it
- But it’s only as good as the People, Data, Processes, and Technology you have

<table>
<thead>
<tr>
<th>Company 1</th>
<th>Company 2</th>
<th>Company 3</th>
<th>Company 4</th>
<th>Company 5</th>
</tr>
</thead>
</table>
| No Intel capability, not even security operations! | - 2 Intel Staff;  
- Staff came out of security team; no intel background  
- Only source is the ISAC and whatever hits the news  
- No integration with InfoSec team | - 2 Intel staff  
- 1 tech expert, 1 Intel Analyst  
- Feed IOCs to SOC  
- Monthly Intel Product  
- Limited Integration  
- Vendor Data sources | - 5 Intel Staff  
- Mix of tech experts and Intel experts  
- Produce various intel products  
- Employ tradecraft  
- Multi-sourced  
- Collaboration with various teams | - 15 Intel staff  
- Intel driven CSIRT  
- 24/7 integration with SOC  
- Advanced tradecraft  
- Multi-Sourced  
- Advanced tech analysis  
- Threat focused analysis  
- Multiple products |
Intelligence Best Practices
+ Corporate Enterprise

- Priority Intelligence Requirements
- Analytic Tradecraft
- Collection Management & Data Sources
- Intel Driven Security Operations
- Effective IOC Processing
- Invested Leadership
- Team Composition
- Knowledge Management
- “Covering Analyst Program”
- Metrics and Justifying Your Existence
Intelligence Life Cycle

**Planning and Direction:** Invested Leadership, Priority Intel Requirements, Governance

**Collection:** External and Internal Data Sources, Collection Management. Raw data gathering

**Processing:** Processes in place to make data usable. E.g. IOCs ingested into SIEM

**Analysis and Production:** Analyzing and documenting information and turning it into actionable intelligence through production of products.

**Dissemination:** Useful and actionable products are sent to the correct customers with an effective feedback loop.

U.S. Intelligence Community Developed: Process is simple and equally applies to corporate intelligence capabilities
To think like the enemy and be prepared for attacks, an intel team must be equipped with as much info as possible.

It should have:

- Asset Inventory (incl Hardware, Applications, IP addresses, device names, VLANs, etc.)
- Network Maps
- Ingress/Egress points
- Details of externally facing / DMZ devices and apps
- Access to SIEM / Security Logs
- …
Commander’s Critical Information Requirements (CCIR)

Elements of CCIR

- Priority intelligence requirement (PIR).
  - Information about the enemy.
  - How I see the enemy.*
- Friendly force information requirements (FFIR).
  - Information about his or adjacent unit capabilities.
  - How I see myself.*
- Essential elements of friendly information (EEFI).
  - Friendly capabilities or assets which, when location is known by the enemy, provides him an advantage if he interdicts that asset

CCIRs translate to everything the CISO needs to know to protect the Enterprise

PIRs = Essential to an effective Intel team

FFIRs = What does your enterprise network and security infrastructure look like? What are your security capabilities? Etc.

EEFI = What is your attack surface that is discoverable by the adversary? Vulnerabilities?

FM 5-0, 2005, p. 3-8
Priority Intelligence Requirements

- CISO and Senior Leadership Determine what is essential to know to protect the enterprise
- Must be prioritized
- ALL work performed by CTI team addresses one or more of the PIRs, otherwise don’t waste time doing it
- PIRs can focus on threat actors, malware, industry events, and anything else that falls within the Cybersecurity Domain.
- Beware of scope-creep

**PIR**

- An intelligence requirement associated with a decision that will affect the overall success of the commander’s mission.
- PIR are prioritized among themselves and may change in priority over the course of the operation’s conduct.
- Can be information about the enemy or terrain.
- Effective PIR . . .
  - Provide intelligence required to support a single decision.
Cyber Specific Analytic Tradecraft

**Adversary**
- Capabilities
- Infrastructure
- Victim

**Diamond Model of Intrusion Analysis**: Ideal for categorizing seemingly disparate threats and attribution

**The Cyber Kill Chain**: Ideal for analyzing attacks from an adversarial points of view and for identifying gaps in detection, prevention, and security controls.
Common Analytic Tradecraft

- **Analysis of Competing Hypotheses (ACH)**
  Identification of alternative explanations (hypotheses) and evaluation of all evidence that will disconfirm rather than confirm hypotheses.

- **Devil’s Advocacy**
  Challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation.

- **Outside-In Thinking**
  To identify the full range of basic forces, factors, and trends that would indirectly shape an issue.

- **Red Team Analysis**
  Models the behavior of an individual or group by trying to replicate how an adversary would think about an issue.

Goal is to prevent bias and produce **ACCURATE** intelligence.

Never produce a product based on what you think someone wants to hear.
Collection Management & Data Sources

- You don’t need every vendor and you don’t need every tool
- Determine what works best for your team.
- Each vendor produces slightly different intel; some will tailor collection; some focus on deep web
- CM monitors value of each through metrics and drops what they don’t need
- Perform Open Source research: RSS, Twitter, Reddit, PasteBin, VirusTotal…

Sample Intel Providers

Sample Intel Tools
You will never optimize your CSIRT/SOC without an intelligence feedback loop.

There are too many IOCs and most of them are old.

Constantly looking outward, Intel identifies the most pertinent threats to the enterprise and obtains the latest indicators.

Intel feeds these to the SOC for monitoring and alerting.

Incidents are addressed by the SOC, Intel provides context.

SOC provides Intel with current incidents to drive intel collection.

Put an Intel guy in your SOC and have a strong partnership with Vulnerability Management.

Often Intel Folks may be a little better communicators due to a liberal arts background, so feeding comms through intel may be valuable.
Example: Phishing

**Option 1:**
Simply remove Email

**Result:**
Threat gone. No valuable information gathered

**Option 2:**
Share email with Intel then remove

**Result:**
Threat gone.
New leads for bad stuff:
- IP Addresses
- Domain Names
- User Names
- Email Addresses
- Mail Servers

Perform Intel Analysis on these, run through Maltego, and find more indicators. Feed valid indicators into SIEM.
IOC Vetting and Processing

IOCs seem easy and like low-hanging fruit, but they’re not!
Yes, you can API them into your SIEM from multiple vendors
But if you do too many you’ll…
- Flood your SOC with Alerts
- Have a high Percentage of false positives
- Overwhelm your intel analysts
But if you have too few you risk missing important events

Recommendations:
1. Confirm how the vendor vets the IOCs before ingestion.
2. Develop a semi-automated vetting process
3. Age off IP addresses and domains after 60-90 days, but keep a knowledge store
4. Ignore IOCs for threats that likely won’t target you
Conclusion

Military/Government intel is not the end-all be-all for intelligence, but there are many strategies that have been tested and proven that can improve processes, efficiencies, and overall intelligence quality if adopted into a corporate environment.

THANK YOU!

Steven Bay
Bay_steven@bah.com or ssbay6@outlook.com
Twitter: @stevebayx6
Add me on LinkedIn