A Few Considerations and Insights regarding Incident Response

Jeremy Manning
Secureworks: A brief introduction

Counter Threat Unit™ research team
- Focused on emerging threat trends
- Rapid countermeasure development

Current SOC locations
- Atlanta, Georgia
- Chicago, Illinois
- Providence, Rhode Island
- Edinburgh, Scotland
- Kawasaki, Japan
- 24x7, 365 days/year
- SOCs manned with all teams, working from a single queue
- Disaster recovery
- No client dependency on one SOC

Security Center of Excellence

<table>
<thead>
<tr>
<th>250B Events processed daily</th>
<th>~4,400 Clients</th>
<th>59 Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,800+ Incident response engagements last year</td>
<td>1,800+ Consulting engagements performed annually</td>
<td>2,300 Employees</td>
</tr>
</tbody>
</table>

Powered by the Counter Threat Platform™
Introduction

- United States Military Academy
- US Army Signal Corp Officer
- VP Tech. 13+ Years Financial Services
- CIO/CISO 3+ Years Bulk Fuel Distributor
How are Organizations Faring in Countering Cyber Threats?

THE HARD TRUTH?

“" We’re getting better at learning how badly we are losing.”"

Jeff Carpenter, Director of SecureWorks’ Incident Response and Digital Forensics practice

SO WHAT IS THE CRUX OF THE PROBLEM?

“" Basic health and hygiene across the IT estate is still an area where most organizations fall short.”"

Don Smith, Director of the CTU Cyber Intelligence Cell at SecureWorks
Agenda

1. Plan Ahead

2. Know Yourself

3. Eviction is not an action taken lightly

4. Visibility is key
Current State of Incident Response?
A Look at the Numbers

71%  
Respondents say that the focus of their company’s incident response capabilities fall into a reactive category.

43%  
Say there is no agreed communication strategy or plan in place in the event of a significant attack.

44%  
Say they do not conduct incident response exercises involving their business leaders.

66%  
Say that their organization does not have enough employees to address the increasing level of threats coming their way.

#1  
barrier to achieving high cyber resilience is insufficient preparedness.

1 in 4  
organizations will experience a data breach in next 24 months.

---

1. Source: Secureworks Cyber Threat Report 2023
Challenges Faced By Security Leaders

You need to continuously take the right action and check your posture

How can I **develop** and stress **test** my team’s incident response **processes** for the latest cyber threats?

How can we quickly and efficiently **respond** to complex cyber events globally - **24x7x365** with limited resources?

Is there a threat actor hiding in my environment today? After evicting them, how do I **prevent** this from happening in the future?
The Challenge is Evolving

Detection, investigation, and response actions need to be carried out daily.

Digital forensic experts especially difficult to hire and retain.

Adversaries are getting more difficult to detect.
Rely not on the likelihood of the enemy’s not coming, but on our own readiness to receive him.

Sun Tzu
In preparing for battle, I have always found that plans are useless but planning is indispensable.

(Dwight D. Eisenhower)
Figure 6-2. Intelligence preparation of the battlefield process.
Key Components of a Mature Incident Response Program

1. Prepares for an incident
2. Responds quickly and efficiently to an incident
3. Follows up on an incident to ensure proper remediation
4. Uses findings from response activities to improve and prevent more in the future
“If you know the enemy and **KNOW YOURSELF**, you need not fear the result of a hundred battles.”

~ Sun Tzu
Know Yourself

Key Elements

**Current Document of Environment**
- Knowing is half the battle.
- Partial is better than nothing.

**Identify Log Sources**
- Log source drives prioritization of incidents.
- Assists in validating visibility, correlation.
- Helps identify possible gaps

**Validate Logs are being Captured**
- Are all systems logging.
- Are all systems enabled with appropriate level of logging.

**Asset Valuation/Risk Tolerance**
- Helps prioritize escalations.
- Adds context to events and incident telemetry
Cisco Says VPNFilter Attacks Bigger Than Originally Thought

Russian hackers behind the VPNFilter attacks are targeting even more vendors' networks, including ASUS, D-Link, Huawei, Ubiquiti, UPVEL, and ZTE, according to Cisco. Talos threat researchers first disclosed details about the malware late last month. APT28, a Russian-state sponsored hacking group that is also known as Fancy Bear, is behind the malware. Fancy Bear is one of the two Russian groups responsible for hacking in the Struts campaign.

Shortly after Talos' original public disclosure of the malware threat, the FBI obtained a court order to seize the VPNFilter malware command and control infrastructure. The order shut down the infrastructure, bringing the malware to a halt for a short time.

The vulnerability could lead to arbitrary code execution.

Adobe on Wednesday released several unscheduled patches for Flash Player, including a critical vulnerability that is said to be exploited in the wild. The critical vulnerability, CVE-2018-15982, is a use-after-free flaw enabling arbitrary code execution.

Unfortunately, changing application frameworks isn’t as easy as adopting a new pizza chain or even buying a new car. Rather, it’s more akin to dumping
Don't fight a battle if you don't gain anything by winning.

Erwin Rommel
What is Eviction?

**Dictionary**

- The action of expelling someone, especially a tenant, from a property

**Cyber Security Dictionary**

- The action of expelling an adversary from a computing environment
Why are we Talking About it?

Requires a different approach

- Intelligence driven incident response
- Extended planning and execution
- Possible significant business impact
- Requires support of executive management
- Conduct in “Orchestration and Simultaneously”

“Whack a Mole “Approach

- Failed sense of accomplishment
- Failure to fully remediate
- Significant contributor to costs and risk
- “Tip one’s hand” – Reveal knowledge to the threat actor
**Incident Response Eviction**

**Common Missteps**

- **MITIGATING THE AFFECTED SYSTEMS TOO EARLY**
  - Can cause the loss of volatile data such as memory and other host based artifacts
  - Adversary will notice and change TTPs

- **TOUCHING ADVERSARY INFRASTRUCTURE (PINGING, NSLOOKUP, BROWSING, ETC)**
  - These actions can tip off the adversary that they have been detected

- **PREEMPTIVELY BLOCKING ADVERSARY INFRASTRUCTURE**
  - Network infrastructure is fairly inexpensive. Adversary can easily change to new C2 and you will lose visibility of their activity.

- **PREEMPTIVE PASSWORD Resets**
  - Adversary likely has multiple credentials – or worse owns your entire AD
  - Adversary will use other credentials, create new credentials, or forge tickets

- **FAILURE TO PRESERVE OR COLLECT CRITICAL LOG DATA**
  - Learn what log types would be critical to an investigation in your organization.
  - Collect and retain these logs for at least 1 year.
Top 10 Logs To Collect in Support of Incident Response

1. External/Internal DNS Requests
2. VPN Logs
3. Web Proxy Logs
4. Outlook Web Access (All SMTP for Non-Microsoft shops)
5. All protocols used for Administrative Purposes (SSH, RDP, etc)
6. Firewall Logs
7. IDS/IPS Logs
8. Antivirus Logs
9. Application Whitelisting Logs
10. Authentication Logs (Switch, Router, Server, All Privileged Accounts, Syslog, Windows Event, etc..)
Successful Eviction

1. Identification
   • Planning

2. Execute

3. Restoring Operations

4. Implement Strategic Changes
When to Evict

How to decide when the timing is right

Ask yourself:

- Do we understand enough about the incident to properly contain it?
- Is the eviction plan ready to be completed in its entirety, or are there outstanding actions?
- Do we have the visibility to see if/when the adversary re-enters the network?
- What are the business risks involved with containment actions?
380

Average days that threats remained undetected in victim networks

Secureworks 2017 Incident Response
You can only alert on what you see.....
Initial Access Vector - How do they get in?

“We are routinely encountering incidents where threats are getting access to networks through internet facing services that only require a single password to gain access.”

Jeffrey Carpenter, Senior Director, Secureworks' Incident Response Consulting Practice

“The idea that attacks are leveraging zero-day vulnerabilities which defenders are powerless to prevent is a myth. In almost every case where software vulnerabilities were exploited to gain access to a network or system, the vendor had released security patches for those vulnerabilities months beforehand.”

Don Smith, Senior Director, Secureworks Counter Threat Unit (CTU) Operations & Analysis

Source: SecureWorks incident response
Incident Response - Failure to detect

Common Roadblocks

- Threat Activity Confirmed (e.g. Recon) But No Intrusion: 12%
- Additional Analysis Was Out of Engagement Scope: 8%
- Excessive Dwell Time, Evidence Legitimately Overwritten or Deleted: 38%
- Insufficient Logging / Instrumentation: 42%

“If you have logs, make sure you are monitoring them... especially if you are thinking about investing in another technology that generates more logs.”

Don Smith, Senior Director, Secureworks CTU Operations & Analysis

Source: SecureWorks incident response
Is that employee really an employee?

Threat Actor TTPs- Blending In and “Living Off the Land”

Definition:

Using a victim organization’s own system credentials and legitimate software tools to move freely throughout their network.

Effective detection requires monitoring all user activity/behavior and differentiating known/authorized from unknown/malicious.
“Living off the Land”

Tracking behavior vs identifying known malware....

An example:

1. Malicious office document drops malicious LNK file
2. Execute PowerShell script
3. Injects PowerShell Backdoor into running processes
4. Net share / scheduled tasks for lateral movement
5. xCopy to stage data for exfiltration on web server
6. eXfil via web browser

ZERO MALICIOUS EXECUTABLES
ALL INBUILT PROGRAMS
The 25 most prevalent native Windows tools used by targeted threat actors

Much of the functionality applies to the following phases of an intrusion:

- discovery (e.g., ping, quser, whoami)
- defensive evasion (e.g., del, taskkill)
- lateral movement (e.g., net, schtasks)
- collection (e.g., findstr)

Source: SecureWorks incident response
Muti-faceted Tool - Windows ‘net’ command-line

50% native tool use observed in 2018 by Secureworks Incident Responders

```
net use \<internal IP address> "password" </user:[domainname]\username>
```

Source: SecureWorks incident response
Paradigm Shift - What makes you a victim?

It’s not* WHO YOU ARE
Or WHAT YOU DO
It’s WHAT YOU HAVE
What makes me a target?

- Cash
- Financial Data
- Personal Data
- Access to Files
- Computing Power
- R&D
- IP
- Gov’t Policy
- Defence
- Opposition
- Dissidents
- High-profile individuals, Websites, Organisations
- Access to orgs with any of the above
Types of Threats

Source: SecureWorks incident response
Observed Threat Categories: (2017-2018)

- Insiders: 8%
- Nation-state Sponsored Threat Actors: 9%
- Financially Motivated Criminals: 83%

Source: SecureWorks incident response

Together, Business Email Compromise, Ransomware, and Banking Trojans accounted for 1/3 of all incidents. Secureworks supported in 2017
RECENT BEC TARGETING

- W-2/PII Data Theft
- Real Estate Transactions
Growth of the ransomware threat

Over the past year, ransomware activity has dramatically increased across the world as cybercriminals have realized its relative simplicity of use and virtual untraceability. Secureworks CTU® researchers observed nearly 200 new, named ransomware variants in 2016, up from 90 the year prior (see FIGURE 2).

CTU® researchers observed nearly 200 new, named ransomware variants in 2016, up from 90 the year prior.
SamSam (Threat Group)

- **GOLD LOWELL** accesses victim networks with brute forced credentials, typically through RDP (Port 3389)
- Dwell time inside network measured in days to weeks
- **Actor focuses on:**
  1. Capture of Domain administrator privileges
  2. Movement to Domain Controller for reconnaissance and malware staging
  3. Identification of file backup assets to manually delete backups
  4. Enumeration of accessible hosts
- Accessible host lists moved outside network so actor can generate **per-host RSA keys**, which are brought back into network
- Malware deployed to hosts and executed with **PSEnc** and/or **WMIExec**
Incident Response Findings

• Organizations are overlooking fundamental security practices and “hygiene”, leaving gaps that are being exploited
  • > 80% of recommendations by Secureworks are for patching, complex passwds, MFA, & disabling unused protocols

• A general lack of visibility into environments allows threat actors to go largely undetected
  • 50% of companies had insufficient endpoint and/or network visibility

• A need to mature incident response plans by testing & exercising plans
  • 70% of IR engagements identified deficiencies in access to and/or quality of logs – slowing down response
Key Points

1. Plan Ahead
   - Documented and needed clarity. Management approved.
   - Regular testing of a plan is key to efficient incident response
   - Predetermined ownership and communication

2. Know Yourself
   - Fully document your environment, asset management is a key lynch pin
   - Ensure relevant logs are being captured appropriately
   - What systems are of higher value or lower risk tolerance than others

3. Eviction is not an action taken lightly

4. Visibility is key
   - Endpoint is crucial element in logging
   - Log all activity – Good and Bad
You can’t ignore the boring stuff......

• Use 2FA for anything external-facing, with no loopholes. Expand to all systems as quickly as possible.
• It’s important to know your own environment better than the adversary.
• Segment your network.
• Limit user permissions.
• Patch your systems- timely.
• Make sure you have the right visibility.
  • Leverage the visibility you already have.
• Be aware of the bigger picture in a incident.
• Not all attacks use malware.
  • Don’t rely on antivirus.
• Continuous Vulnerability Scanning/Testing
• Robust Change Management Process
• Your 3rd parties will be used against you.
Incident Response Reports


2017 Top IR Recommendations - Prevention

- Implement two-factor authentication (2FA)
- Implement web application firewall or web content filtering
- Manage user account privileges
- Implement password management system
- Educate users
- Improve regularity of software updates/patching
- Implement vulnerability/penetration test network
- Resolve network architecture issue
- Remove shared accounts
- Reconfigure internet-facing services
- Implement application whitelisting
- Configure existing security controls
2017 Top IR Recommendations - Detection

- Review existing logs/alerts
- Implement endpoint security technology
- Implement antivirus

2017 Top IR Recommendations - Response

- Enhance logging
- Develop or enhance incident response plans
- Enhance backup regime
Questions

Jeremy Manning
Advisory Security Engineer
Secureworks | Counter Threat Unit (CTU)
jmanning@secureworks.com / www.secureworks.com
O:+1 770.870.3160 / C:+1 832.817.8239