Incident Response 101

- Prateek Vutkur

•••

> It takes 20 years to build a reputation and a few minutes of a cyber incident to ruin it.
>
> – Does not matter who said it. It's the truth.

Decoding Incident Response begins with the basics

- What is an event? What is an alert?
- What is an incident?

User logging into his computer using his credentials.

Outgoing request to Blacklisted IP.

A new software is installed on a company's server.

User Login Failed.

Data has been compromised via unauthorized access

- Why is it important to assess the alert?

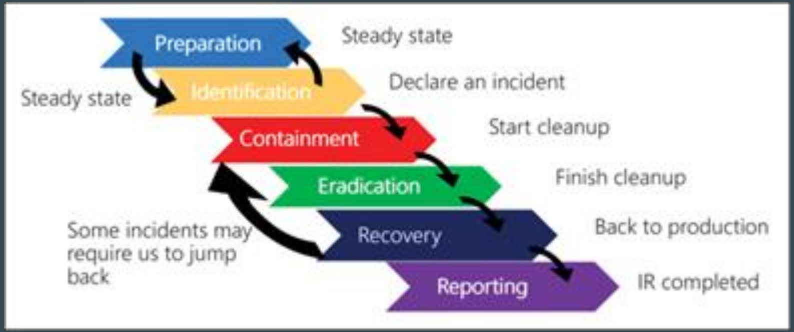
Why do we need Incident Response in the first place?

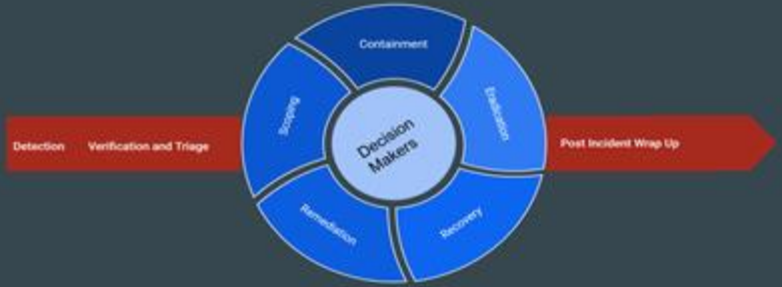
- Minimize damage, Maintain business continuity and reduce future risk.
- Instills confidence in stakeholders - Customers, Business partners and Regulators.

What are the two main types of IR?

- Anti Fire Paint (Security Control)
- No smoking inside the house (Policies)
- Inspecting Electrical Wiring (Vuln Assessment)

The IR Lifecycle - Linear or Dynamic?





Preparation

Knowing your organization (What does business care about? People, Policies and Procedures?

Visibility into network and host artifacts.

Having recovery plans and backups.

Tabletop exercises for the IR team.

Identification

Detection - Network Devices, Host, Threat Intel Feeds, User and third party notifications.

Verification - True / False Positive

Triage - Understanding the type of incident.

Containment

Scoping the incident.

Short term vs long term containment based on business impact and evidence collection.

Patching, network isolation, removing backdoor accesses, filters on devices, altering DNS entries, etc.

Eradication

Removing attacker activity (Processes and accounts, tools)

Vulnerability assessments are performed.

Recovery

Restoring systems from trusted backups.

Focus is on business impact.

Restore or Rebuild (Apply fixes and harden systems)

Bringing back systems online is crucial (Timing varies on several factors)

Lessons Learned

Creating a report of the incident.

Capitalizing on the impact to request upgrades.

Follow up review meetings on what has been implemented.

IR Playbooks - How do we build one?

- Introduction and Scope : (Objective, Incident Classification)
- Members involved in IR process (All the team members involved in PICERL stages)
- IR plans and procedures (Step by step guide on the PICERL stages)
- Communication Procedures (Protocols and Channels used for communicating with stakeholders)
- Tools and Technologies (Centralised Logging, SIEM, Network and Host Tools, Forensic Toolkit,
- Documentation (Templates for reporting)
- Post Incident Observations (Constant log of improvements)

Playbooks require collaboration with HR, Legal and compliance teams as well! (GDPR and PCI-DSS)

Understanding the roles of Security Team Members involved in IR

Security Analyst -
Responsible for monitoring and analysing security events and alerts to identify potential security incidents.

Incident Response Specialist / Incident Handler -
Performs Root Cause Analysis of the whole incident. Involved in Containment, Eradication and Recovery Phases.

Malware Analyst -
Understanding the behavior of malware through static and dynamic analysis.

Digital Forensics Specialist -
Conducts in depth analysis of the memory and file system to identify and recover data.

Threat Hunter -
Determine the TTPs used by an attacker using the MITRE framework and help contain or eradicate attacker presence.

Threat Intel Analyst -
Provide Contextual Information about the threat (Attacker motivation and Profile, attack type, etc based on gathered IOCs)

Security Manager -
Presents an unified front for the entire incident response lifecycle execution through coordinating efforts between the Security Team.

CISO -
Responsible for ensuring alignment of IR with the organization's overall security strategy.
Communicates with Senior Management regarding incident and impact.

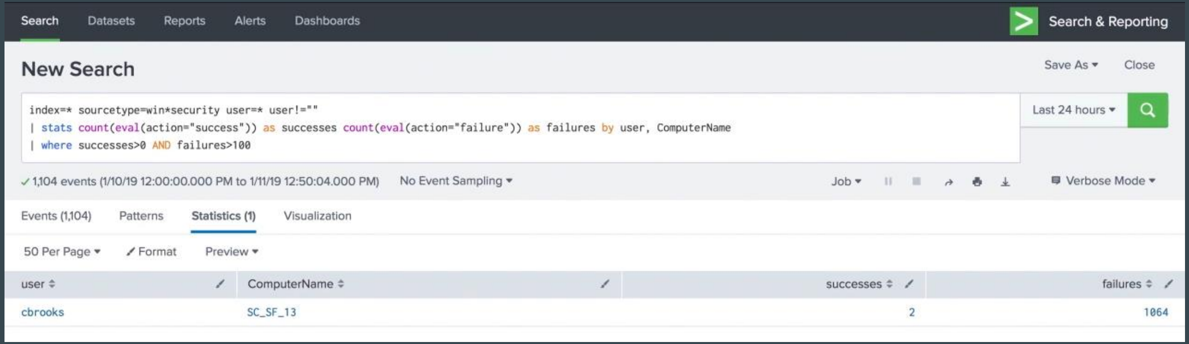
Security Analysis using SIEM Tooling (Splunk)

Analyst looks at the alert that has been generated by the SIEM tool.
Use cases - Phishing, Malware Detected, Outgoing Request to Blacklisted URL, etc.

Integration with JIRA can create automatic tickets with severity, description and timestamp.

Verify with the visible indicators/logs from open source tools. (URLVoid, Virustotal, IPVoid, MXToolbox, Hybrid Analysis, etc)

Provides initial analysis on alert (true / false positive) and escalates to IR Specialist/Handler.



```
index=* sourcetype=win*security user=* user!=""
| stats count(eval(action="success")) as successes count(eval(action="failure")) as failures by user, ComputerName
| where successes>0 AND failures>100
```

✓ 1,104 events (1/10/19 12:00:00.000 PM to 1/11/19 12:50:04.000 PM)   No Event Sampling ▾

user	ComputerName	successes	failures
cbrooks	SC_SF_13	2	1064

Incident Response Specialist - Primary point of contact

Responsible for RCA (Root Cause Analysis)

Shift Handover (8 hours timeline. Part of a 24/7 setup)

Liason for the Security Manager

Co-relating information from reports obtained from various members on the team.

Forensic Investigator - Forensic Toolkit

Creates bit by bit image of hard disk using Write Blocker and tools like FTK Imager, Encase

Performs system Forensic Analysis - Volatility, Autopsy, Registry Ripper, Zimmerman's tools for analysing Shellbags (Folder execution on local machine, network and removable media), LNK files (Files accessed grouped by machine ID) and JMP lists (Applications run on the system and path) and Prefetch (Programs that were executed on the system and their frequency).

Follows chain of custody - Extremely important to make evidence eligible.

Prepares report of investigation for relevance in IR process.

SUSPICIOUS EMPLOYEE BEHAVIOR (DATA EXFILTRATION ATTEMPTS)

Malware Analyst - Decoding Malware Samples

Static Analysis

Disassemblers (IDA pro and Ghidra) - Convert Machine code into Assembly language
To understand code functionality.

Signature based detection (YARA Ruleset) - Detection of malware families using binary or textual patterns.

Dynamic Analysis

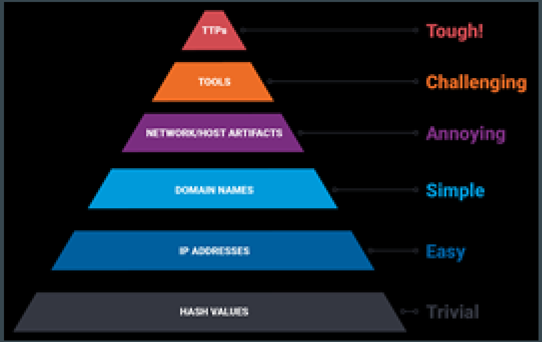
Debuggers (OllyDbg) - Analysing behavior of the program as it runs. Uses breakpoints to discover how it communicates with remote servers, system modification, etc.

Cuckoo Sandbox - File and Process Creation, Network Activity (HTTP requests, DNS queries), Windows Hook creation (Keylogger), Malicious URLs and Anti forensic activity.

Threat Intelligence Analyst - Providing Context

Strategic Threat Intel -

Who and Why (Attacker Profile and Motivation) - Long term planning.
Target Audience - Senior Management and Leadership.



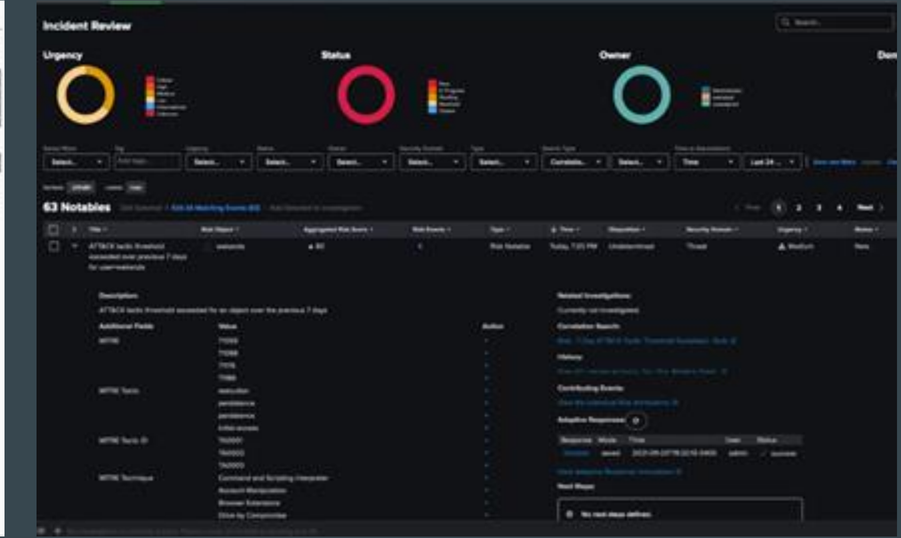
Operational Threat Intel -

Focus is on How (TTPs employed by the threat actor) - Long term
Target Audience - SIEM Team, Threat Monitoring on endpoints.

Tactical Threat Intel -

Focus is on What (IOCs associated with the Threat Actor) - Immediate value
Target Audience - SOC Team

Threat Hunting Analyst - MITRE Framework



The Importance of MITRE framework cannot be ignored!

Integration with splunk enterprise is possible.

IR Scenario - Phishing (The most common attack vector)!

Let us simulate the steps that are taken by the various team members under different scenarios.

Remember that IR is a mindset. We must be willing to consider all possibilities to effectively create a playbook.

Know your environment -
What logs are accessible? How is the visibility?
What tools are configured? What vendor software can we access?
Start with the analyst POV.

Focus on the P**ICERL** - Start with Identification and move to Lessons Learned.

Be prepared to perform some activities single handedly in the absence of a specialist.

Phishing - Let us Begin!

Assume the Preparation steps have been taken already :

- Phishing email awareness campaigns and articles to users.
- Regular email infrastructure is in place.
- SIEM tools are up and running with use cases in place based on threat intelligence platforms and phish-score.

Identification (Detection and Analysis) :

Initial alert :
A user has forwarded an email to the security inbox.

The incident response begins now. Put yourself in the shoes of the Analyst first!

Phishing Scenario - Continues..

Triage (Checking to see if the alert can be categorized as an incident and assign a severity to the same) -

Email Header Analysis

- Sender and Recipient email address
- Email Subject
- Sender's IP Address
- X-Originating IP Address (Originating Server IP)

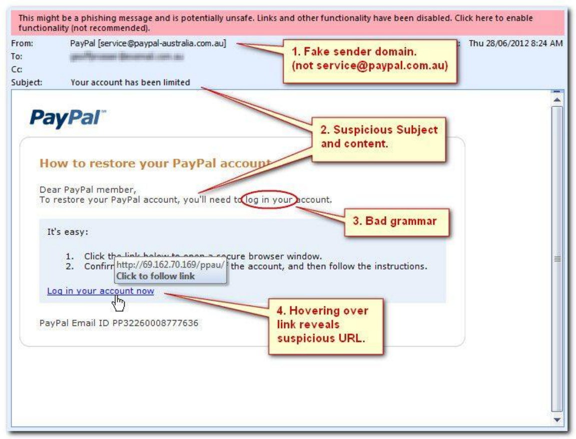
Examine for the following Phish Attributes :

- Return path field contains an email address that is not related to the name shown in the sender field in the original mail.
- The X-Authenticated User field contains an email address that is suspicious.
- The mail server IP address is malicious.
- The email domain is suspicious.

Phishing IR

Message Content Analysis

- Look at the body of the mail to verify if its contents appear to be Spam or suspicious (like the language)
- If there is an attachment, collect it and store it in a password protected zip file "infected".
- If there is a malicious URL in the email body, we can do the necessary steps for that.



This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au] Thu 28/06/2012 8:24 AM
To: [redacted]
Cc:
Subject: Your account has been limited

PayPal

How to restore your PayPal account

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm the account, and then follow the instructions.

http://69.162.70.169/ppau/
Click to follow link

Log in your account now

PayPal Email ID PP32260008777636

1. Fake sender domain. (not service@paypal.com.au)

2. Suspicious Subject and content.

3. Bad grammar

4. Hovering over link reveals suspicious URL.

Known False Positive

- Close the case

Sandbox

- Submit the attachment to the sandbox for dynamic analysis

Phishing or Malicious mail

- Identify the category of the mail and follow the respective IR plans.

Recipients list

- Review the email transaction logs to view the recipient list and the numbers. Profile them based on Username, Employee ID, Email Address, Department, Location, Designation.

Decide the kind of attack

- Based on the user profiling understand the nature of the attack (spear-phishing, SPAM, whaling, etc).

Create a case in the case management tool

- Create a case ID and assign a priority based on the information gathered.

Phishing – The process Continues

Analyze the URL/Attachment

- Use tools like urlvoid, urlscan.io to understand the reputation of the URL.
- Identify the maliciousness of the IP Address using tools like IPVoid.
- Create a hash of the malware file and investigate on virustotal.com.

Determine the scope and Impact

- Review proxy logs in SIEM - To see the number of users who have clicked on the URL.
- Review firewall logs - To identify the Source IP Addresses that have connected to the phishing URL.
- Review AV logs to look for any alerts.

Profile the impacted users

- Create a list of the users with their Username, Dept, Location and EMP ID.

Phishing – Containment, Eradication, Recovery, Post Incident Activity

Containment :

- Block the sender at the email gateway.
- Block the IP address at the Firewall.
- Block the URL at the Central/Local proxy.
- Send User Awareness emails to the whole organization.
- Monitor the impacted user accounts for potential misuse.

Eradication and Recovery :

- Delete email from users mailboxes - send an order to the messaging team.
- Change impacted users credentials.

Post Incident Actions :

- Send out an advisory to the entire company based on the impact of the incident.
- Include changes to phishing awareness section in subsequent cybersecurity campaigns to employees.

Ransomware - IR

Method of Initial Attack :

- Phishing mails
- Drive-by downloads
- Unprotected RDP lines exposed to the Internet

Identification:

- Sudden appearance of software like AngryIP and Advanced Port scanner to scan for network vulnerabilities and weaknesses like open ports.
- Tools like Mimikatz can be used for Credential harvesting and Privilege Escalation.
- The attacker will also use PowerShell to gain access to other systems via lateral movement.

Containment and Eradication:

- Disable RDP Access to cut off the point of command and control for the attacker.
- Centrally push the password change policy to the core systems on priority.
- Look for Rogue user accounts and delete them.
- Delete traces of the attacker tools to prevent further damage.
- Isolate the affected systems and reinstall the images and reinstate them to backup domain controllers.
- Delete any suspicious running PowerShell processes and thoroughly investigate the system for any suspicious network activity.

Ransomware - IR

Recovery :

- Restore the clean systems back to the network. Apply all software application patches and keep the operating systems up to date.
- Perform regular scans to detect any redundant attacker activity.

Prevention Strategies:

- Disable the enable content in macros on documents.
- Keep your system up-to-date with the latest software patches.
- Implement a zero-trust model.
- Use intrusion detection and prevention systems.
- Implement strong password policies.
- Educate employees on cybersecurity best practices.

How do I get started with a career in IR?

- Have an understanding about the entire security posture of an organization.
  - Understand the architecture and existing tools and technologies.
    - SIEM tools (Splunk)
    - SOAR tools (Splunk Phantom)
    - EDR and XDR tools (Crowdstrike)
    - Host Analysis (Microsoft Sysinternal Tools)
    - Network Analysis (Wireshark and TCPDump)
    - Logging (Sysmon, Velociraptor)
- Familiarize yourself with people, policies and procedures.
  - An effective IR requires effective communication and critical thinking.
- Cultivate a questioning mindset.
- Remember that business comes first. Always!
- Learn about security controls that are implemented within your Org.

Resources for IR

Youtube Channels - CBT nuggets, SANSForensics, EC Council

Podcasts - Darknet Diaries, The Incident Response Podcast, Digital Forensics Survival Podcast

Websites - https://cyberdefenders.org/ , https://cyberdefenders.org/ , https://www.crowdstrike.com/blog/

Twitter - @DFIRTraining, @MalwareJake, @ForensicFocus, @TheCyberMentor, @BrianKrebs

Cheat Sheets - https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/

The future is Cloud IR and Forensics - AWS Security Incident Response Guide
Collection of Threat Detection rules and rule engines - https://lnkd.in/dRWeUWba

Certifications -

- CompTIA: Security+
- CompTIA: CySA+ (Cybersecurity Analyst
- Cisco: CCNA Cyber Ops
- EC-Council: Certified Ethical Hacker (CEH)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Network Forensic Analyst (GNFA)
- GIAC Reverse Engineering Malware (GREM)
- EC-Council: Certified Forensic Hacking Investigator (CHFI)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Certified Forensic Examiner (GCFE)
- EnCase Certified Examiner (EnCE)
- Certified Computer Examiner (CCE)
- Certified Forensic Computer Examiner (CFCE)

Some cool movies/TV shows you can watch!

Don't F**k with Cats: Hunting an Internet Killer - A cybercrime investigation

CSI: Crime Scene Investigation - Digital forensics and cybercrime investigation