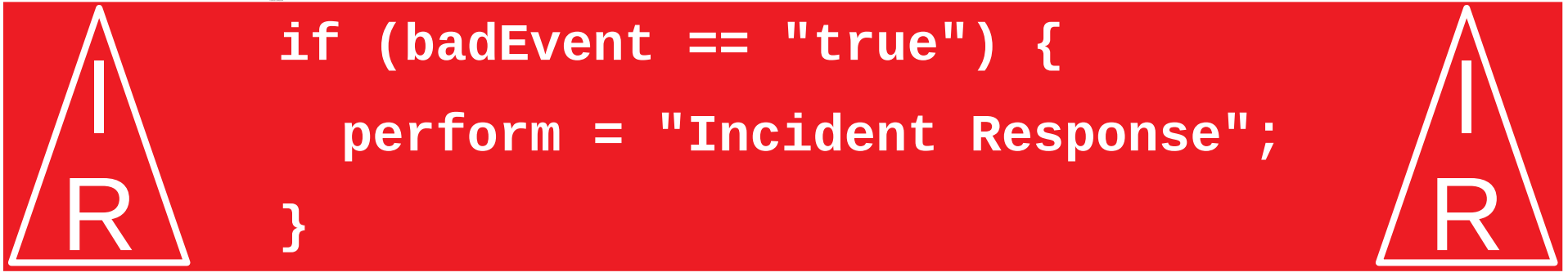
Matt Scheurer

Presents:


https://twitter.com/c3rkah


https://www.linkedin.com/in/mattscheurer

http://slides.dfirmatt.com



What I do...

I work for a big well-known organization...

**As an Information Security (InfoSec) Engineer,
Performing Digital Forensics & Incident Response (DFIR)
On a Computer Security Incident Response Team (CSIRT)**

I am also a Podcast Host for

ThreatReel

https://threatreel.com

Where I volunteer...

I am an Official

HACKING IS NOT A CRIME

Advocate

https://www.hackingisnotacrime.org/

I am also a

WOMSA
Empowering Women in Cybersecurity

Women's Security Alliance (WomSA) Technical Mentor

https://www.womsa.org/

Disclaimer

Yes, I have a day job. However…

Opinions expressed are based solely on my own independent security research and do not express or reflect the views or opinions of my employer.

Agenda

1) Incident Response (IR) Essentials

Covering basic technical skills and baseline knowledge required for Incident Response investigative analysis.

2) Q&A

Why this talk?

This talk is inspired by job candidates I've interviewed for Level 4 (IV) / Principal Security Engineer Incident Response (IR) positions. Finding experienced IR candidates ready for that level of work is challenging. The purpose of this talk is to help fill the knowledge and skill gaps I've seen by covering where aspiring IR analysts and engineers should start and then build upon their knowledge.

Role of Incident Response

Incident Responders investigate security incidents, events, and alerts to answer the classic “Who?”, “What?”, “When?”, “Where?”, “Why?”, and “How?” questions.

Aspiring Incident Responders

A good IR candidate possesses a working level of knowledge (preferably firsthand) in each of the following Information Security disciplines:

- Defensive Security
- Offensive Security
- Digital Forensics

When IR starts

Some security investigations begin with a user reporting suspicious activity within an Enterprise Environment. However most investigations start through alerts from a Security Incident Event Management (SIEM), automated triggers configured within systems, Anti-Virus, Endpoint Detection and Response (EDR/XDR), Network Detection and Response (NDR/XDR), Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) alerts.

Diving Deep

While working with information from an organization's SIEM, Anti-Virus, EDR, NDR, XDR, and IDS/IPS solutions are critical in an enterprise environment; please don't become too reliant on any of those security tools alone! Learning and developing a better understanding of the properties of files and underlying activities that trigger those alerts is paramount to becoming a better Incident Responder.

IR Skill: Alert Dispositions

The following table illustrates detection and conditions of security alerts and events...

	True (Detection)	False (Detection)
Positive (Condition)	**True Positive:** Correctly classifying malicious activity as malicious	**False Positive:** Incorrectly classifying benign activity as malicious
Negative (Condition)	**True Negative:** Correctly classifying benign activity as benign	**False Negative:** Incorrectly classifying malicious activity as benign

IR Skill: OS basics

Know how to review the processes, services, or daemons that are running and their impacts on system CPU and memory utilization

- Windows:
  - Task Manager (**taskmgr.exe**)
  - **services.msc**
- Linux
  - “**ps**” command
  - **“top”,** or “**htop”** if it’s installed/available

IR Skill: Filesystem basics

Knowing where things are supposed to be located on an endpoint is vitally important to Incident Response. This requires a working knowledge of:

- The Microsoft Windows filesystem
- The Linux filesystem
- Potentially MacOS, depending on the environment and prevalence

Filesystem basics: User directory

- On Windows
  - C:\Users\<USERNAME>
  - %UserProfile%
- On Linux
  - /home/<USERNAME>

Filesystem basics: Windows

Most configuration settings are stored in the Windows Registry

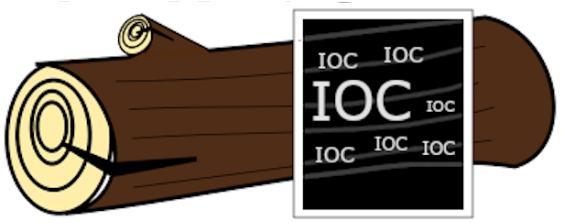
- Hives: HKEY_LOCAL_MACHINE\Software, HKEY_LOCAL_MACHINE\System, HKEY_LOCAL_MACHINE\SAM, HKEY_LOCAL_MACHINE\Security, HKEY_USERS\DEFAULT, HKEY_CURRENT_CONFIG
- Important Registry Hive file paths
  - %SystemRoot%\System32\Config
  - %SystemRoot%\System32\config\RegBack
  - %UserProfile%\NTUSER.DAT
- Open with "**RegEdit.exe**", "**RegEdt32.exe**", or other 3rd party tools / forensics tools

Filesystem basics: Linux

- Most Linux configuration files are stored under the "***/etc***" directory or within sub-directories inside the "***/etc/***" directory
  - Noteworthy files there include: **passwd** and **shadow** among others
- The Linux Foundation maintains the "Filesystem Hierarchy Standard" (FHS), which is a fantastic reference for paths on Linux hosts
  - https://refspecs.linuxfoundation.org/FHS_3.0/fhs-3.0.html

IR Skill: Logs & PCAPs

The bedrock and starting point of most security investigations begins with any available logs and packet captures files (PCAPs).



MATT SCHEURER
and the WIRESHARK WORKSHOP

SIEM's are great, but...

While centralized logging is very important, SIEMs aren’t perfect. Often due to resource constraints and either bad or missing inputs. SIEM’s are often only configured to capture specific events or event types. Important details might be tuned out, filtered out, or simply parsed incorrectly. Input sources might become broken. Automated searches and correlations might also get skipped.

Native Logs

Understanding where logs exist on various endpoints is vitally important

- Windows Logs
- Linux Logs
- Server Logs
- Application Logs

Windows Logs

- The 4 primary Windows logs are: **Application**, **Security**, **Setup**, and **System**.
  - Though there are lots of others now, *if enabled*
- They exist as .evtx files under
  - %System32%\winevt\Logs
- They can be opened using the Windows Event Viewer (**eventvwr.exe**)

Windows Log Knowledge

- At a high level, understand that Windows does log types of events using specific “**Event ID**” numbers.
  - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor
- At a high level, understand that Windows records various “**Logon type**” conditions
  - https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/reference-tools-logon-types

Linux Logs

- Most Linux log files exist under the “**/var/log**” folder
  - For example: /var/log/syslog
- Typically, viewable using any preferred text editor, the **cat** command, the **more** command, the **less** command, the **head** command, or the **tail** command
  - “tail -f” options may also be used to follow a log live

Linux Log Knowledge

- Many Linux logs are timestamped in Epoch time
  - Throwback to the old Unix timestamps that are a numeric string in relation to the date of January 1, 1970
  - These are not human understandable
  - Use a converter to translate Epoch timestamps into a human readable time
    - Reference GMT or local time
  - Time-lining and time-stamping files and activities is crucial for incident response investigations

Server Logs

- Be aware that various server applications might store their own logs independently of the host OS' native logging
  - Default log paths and names are also sometimes changed
- By default, Windows IIS server logs are stored in numbered "**W3SVC**" folders under the following directory
  - %SystemDrive%\inetpub\logs\LogFiles

Application Logs

- Be aware that various applications might store their own logs independent of the host OS' native logging
  - Default log paths and names are also sometimes changed
- Some application logs reside on the endpoint itself, but others might be stored in a centralized management platform of some sort
  - Sometimes both conditions are true

IR Skill: Networking basics

- Understand the differences between TCP (3-way handshake) and UDP (connectionless) protocols
- Learn the common TCP and UDP ports numbers
  - i.e., TCP: 22, 80, 443, 445, 3389; UDP: 53
  - https://packetlife.net/media/library/23/common_ports.pdf
- Learn port scanning (i.e., Nmap)

IR Skill: Network packets

- Being able to analyze network traffic data is an important IR skill
- Learn how to create, save, and analyze packet capture files (PCAPs)
  - i.e., Wireshark, tshark, tcpdump, windump, etc.
- Obtaining decrypted packets is always best, but may not always be feasible

IR Skill: OWASP Top 10

- The **Open Web Application Security Project** (**OWASP**)
  - The **OWASP Top 10** is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.
  - https://owasp.org/www-project-top-ten/

IR Skill: Web requests

- Most common HTTP request methods
  - **GET**, **HEAD**, **POST**, **CONNECT**
- Potentially concerning HTTP request methods
  - **PUT**, **DELETE**
- Lesser seen HTTP request methods
  - **OPTIONS**, **TRACE**, **PATCH**

IR Skill: HTTP response codes

- Web server response codes
  - **200** series responses
    - Request was recognized by the server
      - Results may or may not be as expected
  - **300** series response codes
    - Redirects
  - **400** series responses
    - Client error response
  - **500** series responses
    - Server error response

IR Skill: SQL Basics

- Understand “Structured Query Language” (SQL) to help identify “injection” (SQLi) attacks
- Free online training
  - https://www.sqlcourse.com/beginner-course/
  - https://www.sqlcourse.com/advanced-course/

IR Skill: Data Encoding

- Learn to recognize and identify the most popular data encoded string traits
  - Encoded examples of “**Hello attendees!**”
    - Base64: SGVsbG8gYXR0ZW5kZWVzIQ==
    - ROT13: Uryyb nggraqrrf!
    - Hex: 48 65 6c 6c 6f 20 61 74 74 65 6e 64 65 65 73 21

NOTE: All 3 encoding methods are commonplace

IR Skill: File Type Identification

- Understand file signatures, magic bytes, magic numbers, file headers, or whatever you prefer to call them…
  - Because file extensions can be altered or removed
- "**MZ**" Windows executable, "**PK**" Zip file, etc.
- https://www.garykessler.net/library/file_sigs.html

IR Skill: Understand Persistence

- There are numerous methods for threat actors to ensure persistence in order to greatly reduce their risk of losing access to an endpoint that they've compromised
  - Some of these are unique to Windows or Linux
  - Be sure to understand some of them
- https://attack.mitre.org/tactics/TA0003/

IR Skill: Identify File Execution

- Understand how to know if a file executed on a Windows endpoint
  - Some Examples: EDR/XDR, Registry “HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count” (*ROT 13*), Memory Dump, ShimCache, Prefetch (%windir%\Prefetch), etc.

Why Windows is hard to secure

- There are lots and lots of file types and extensions that execute on Windows by default
  - In fact, nobody likely knows exactly how many there are, but there's at least 50 or more of them...
  - https://www.howtogeek.com/137270/50-file-extensions-that-are-potentially-dangerous-on-windows/

IR Skill: Evidence Collection

- **RFC 3227: 2.1 Order of Volatility**
  - https://www.rfc-editor.org/rfc/rfc3227.html
    - “When collecting evidence you should proceed from the volatile to the less volatile. Here is an example order of volatility for a typical system.”
      - registers, cache
      - routing table, arp cache, process table, kernel statistics, memory
      - temporary file systems
      - disk
      - remote logging and monitoring data that is relevant to the system in question
      - physical configuration, network topology
      - archival media

IR Skill: Understand Volatile Data

- "**National Institute of Standards and Technology**" (**NIST**)
  - *Guide to Integrating Forensic Techniques into Incident Response*
    - https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf
      - The recommended order in which volatile data generally should be collected, from first to last
        1) Network connections
        2) Login sessions
        3) Contents of memory
        4) Running processes
        5) Open files
        6) Network configuration
        7) Operating system time

IR Skills: Tools for skill building

- CyberChef
  - https://www.ohioinfosec.org/files/2021/CyberChef_Workshop.zip
- Incident Response & Forensics tools in
  - Kali Linux (Yes, really!)
  - REMnux (Linux)
  - SANS SIFT Workstation (Linux)
  - FireEye's FLARE VM (Windows)

IR Skills: Ways to build skills

- ENISA Training Labs
  - https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
- Participate in Capture-The-Flag (CTF) events
- Periodically review the Tactics, Techniques, and Procedures (TTP's) in the **MITRE ATT&CK** framework
  - https://attack.mitre.org/

IR Skills: Offensive Security

- Learn Offensive Security skills
  - Examples: Bug Bounty programs, Pen Testing, Red Teaming, or Purple Teaming
  - Learn everything you can to improve your IR skills
    - Figure out what "**Indicators of Compromise**" (IOC's) and artifacts those offensive security TTP's generate and look for ways to monitor and detect that type of activity

IR Skills: Hands-on experience

- Be extremely careful about it, but **safely** have a look at bad stuff...
  - Publicly shared data breach dumps
    - Including: any.run, GitHub, VirusTotal, etc.
  - Phishing Emails & Sites
    - https://www.phishtank.com/
  - Or better yet, be your own DIY-style (1-person Purple Team)

Questions

Who?

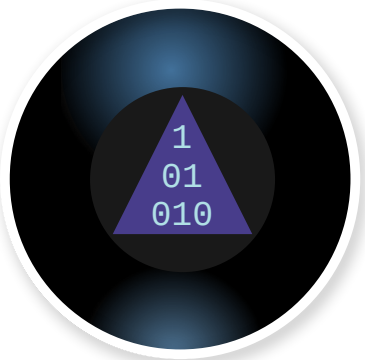
What?

When?

Where?

Why?

How?



Thank you for attending!


https://twitter.com/c3rkah


https://www.linkedin.com/in/mattscheurer

http://slides.dfirmatt.com