

BUILDING A DETECTION ENGINEERING LAB

Hackers Teaching Hackers 2024

Michael Miller



Agenda

- Introductions
- Home Labbing Recap
- Why Build a Detection Engineering Lab
- Detection Engineering
- The Lab Environment
- Creating Detections
- Generating Badness (Testing)
- Summary
- Bonus?



\$> whoami

- IT/Cybersecurity for 13+ years in a variety of industries
 - Worked with companies ranging in size from <\$1M ARR to >\$200B ARR
 - BS Cybersecurity & Information Assurance from WGU
AAB Network Administration & Computer Programming from NSCC
 - CISSP, CCSP, SSCP, GDSA, GISP, CEH, ECES, CySA+, and many more
 - Participate in InfraGard, ISSA, (ISC)2, SANS Advisory Board, NSCC IT Advisory Board, CAMO at NSCC, Adjunct Teacher at NSCC
 - I enjoy spending time with my wife and kids, traveling, cooking, public speaking, and tinkering with my home lab
-

\$> who

- Cybersecurity Professionals?
 - Students?
 - Have a home lab?
 - Have experience doing detection engineering?
 - Are red teamers/penetration testers?
-

Home Labbing Recap

- Home labs are nonproduction environments where you can test out new ideas and concepts to evaluate solutions, or teach yourself new concepts, technologies, and skills
 - They can be any combination ranging from a single system like a laptop to a full datacenter of enterprise infrastructure
 - Can be physical systems, containers, virtual machines, cloud systems – or any combination of these
 - You can then replicate real world environments or host “productionized” solutions for home
-

Home Labbing Village



COME WITH ME IF YOU WANT TO LAB

imgflip.com



- <https://lexcilius.github.io/hth2024labbing/>



Why Build a Detection Engineering Lab

- Detection engineering requires an understanding of the systems in which you are building detection logic for
 - Each environment is unique so every company will likely have different detection logic
 - Advanced detection engineering requires understanding common tactics, techniques, and procedures (TTPs) which are constantly changing
 - This is a skill that can set you apart amongst other professionals in the field (aka resume building)
-

Word of Warning (Considerations & Caveats)

- What this session is not
 - An in-depth course on engineering detections
 - An in-depth presentation on how to build home labs
 - What this session is
 - An introduction to the concepts of detection engineering
 - Some fundamental specifications to develop detections based on a variety of source data
 - Provides some design patterns on how you can construct a home lab to facilitate developing, testing, and refining detections that could benefit you, your career, and your company
-

DETECTION ENGINEERING

What is Detection Engineering

- Detection engineering is the process of designing, developing, testing, and maintaining threat detection logic to identify and respond to potentially malicious events
 - Leverages threat intelligence for a combination of indicators of compromise (IoCs) and/or indicators of attack (IoAs)
 - Usually presented in the form of rules, signatures or complex queries
 - Usually involves a SIEM and/or IDS as main components
-

What Makes a “Good” Detection



Repeatable



High fidelity

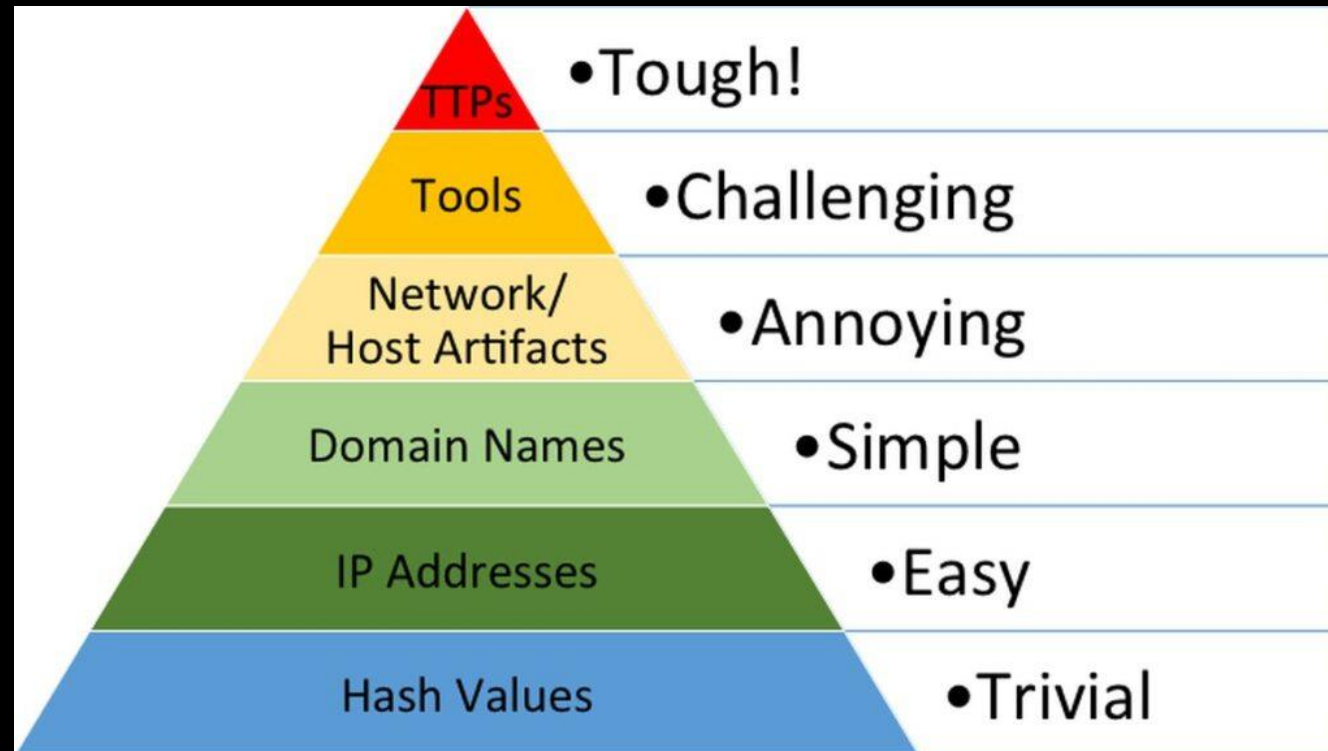


Applicable and
relevant



Scalable

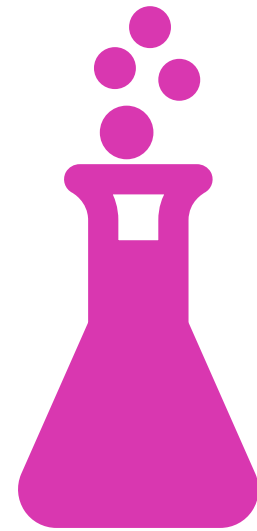
The Pyramid of Pain



Data Sources

- Authentication Logs
 - Network traffic logs (NetFlow, proxy logs, etc)
 - Intrusion Detections System (IDS) logs
 - Firewall logs (network and host)
 - Endpoint Detection and Response (EDR) logs (process executions, network connections, etc)
 - DNS Logs
 - Application Logs
 - Many more....
-

THE LAB

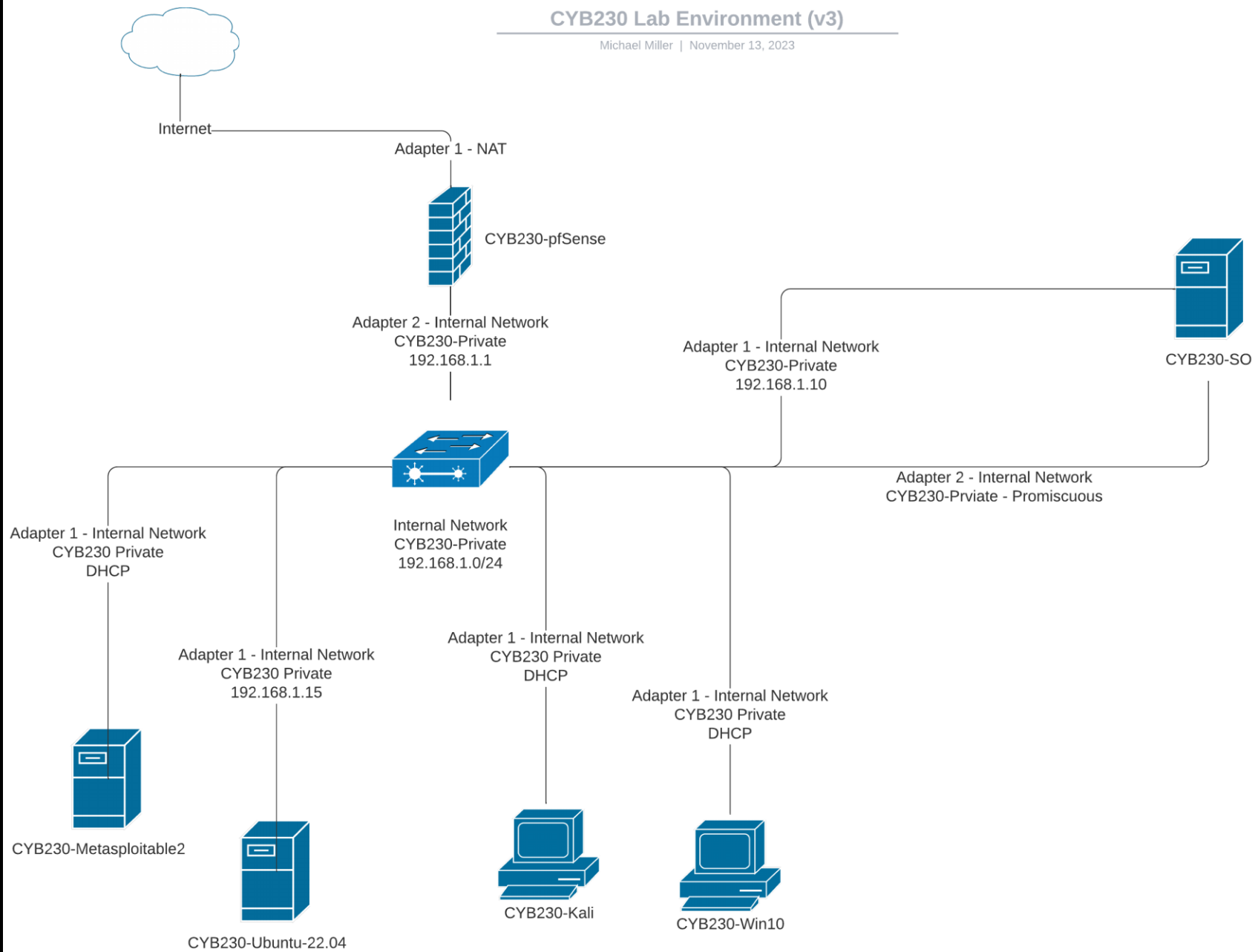


The Lab Environment

- Firewall – pfSense, OPNsense - REQUIRED
 - SIEM/Log Collector – Security Onion, ELK Stack, Splunk - REQUIRED
 - NIDS – Security Onion, Suricata, Snort - RECOMMENDED
 - Windows System(s) – Windows endpoint(s), Windows server(s) - OPTIONAL
 - Linux System(s) – RHEL or Debian based system(s) - OPTIONAL
 - Attack Machine(s) – Kali - OPTIONAL
-

CYB230 Lab Environment (v3)

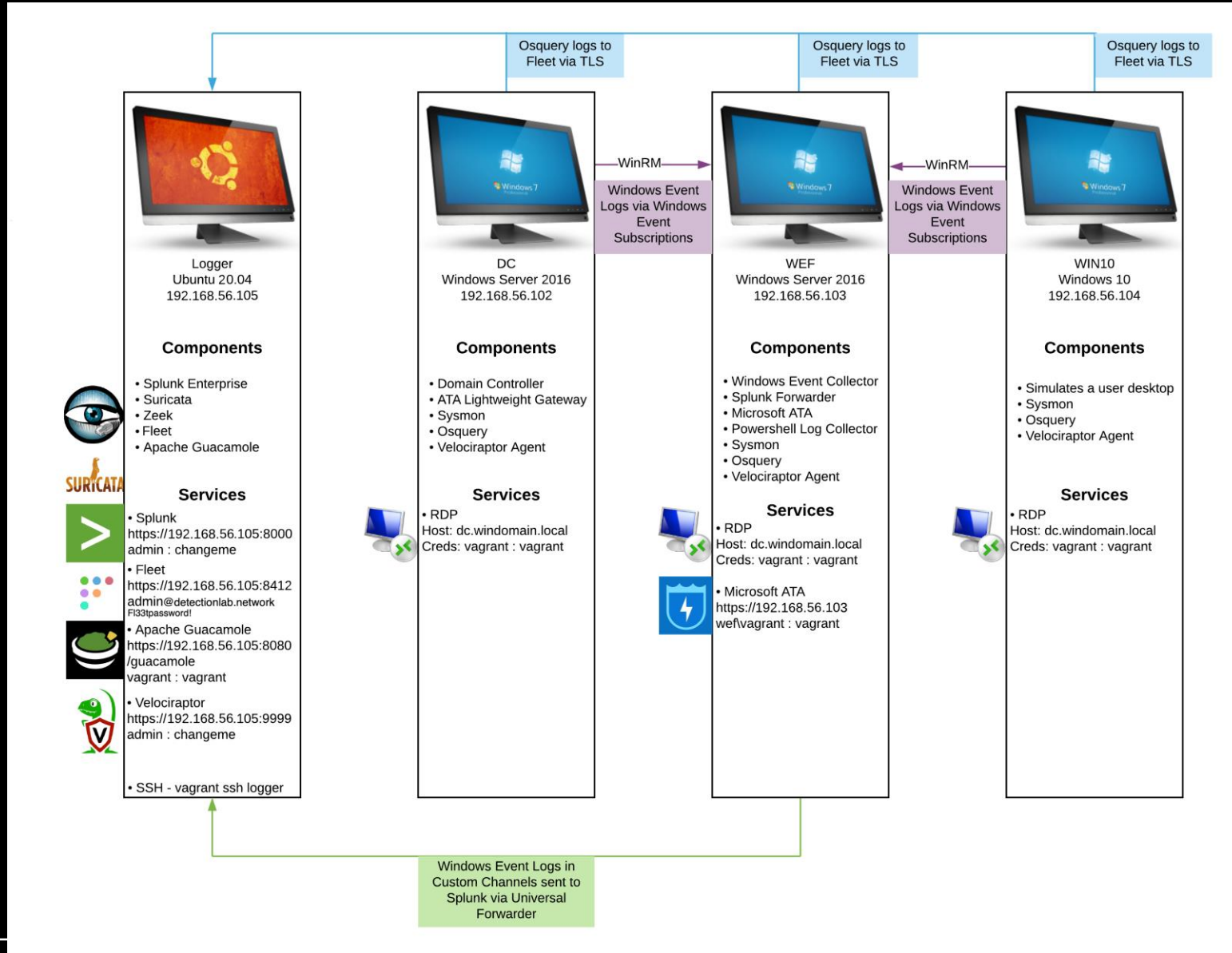
Michael Miller | November 13, 2023



Detection Lab



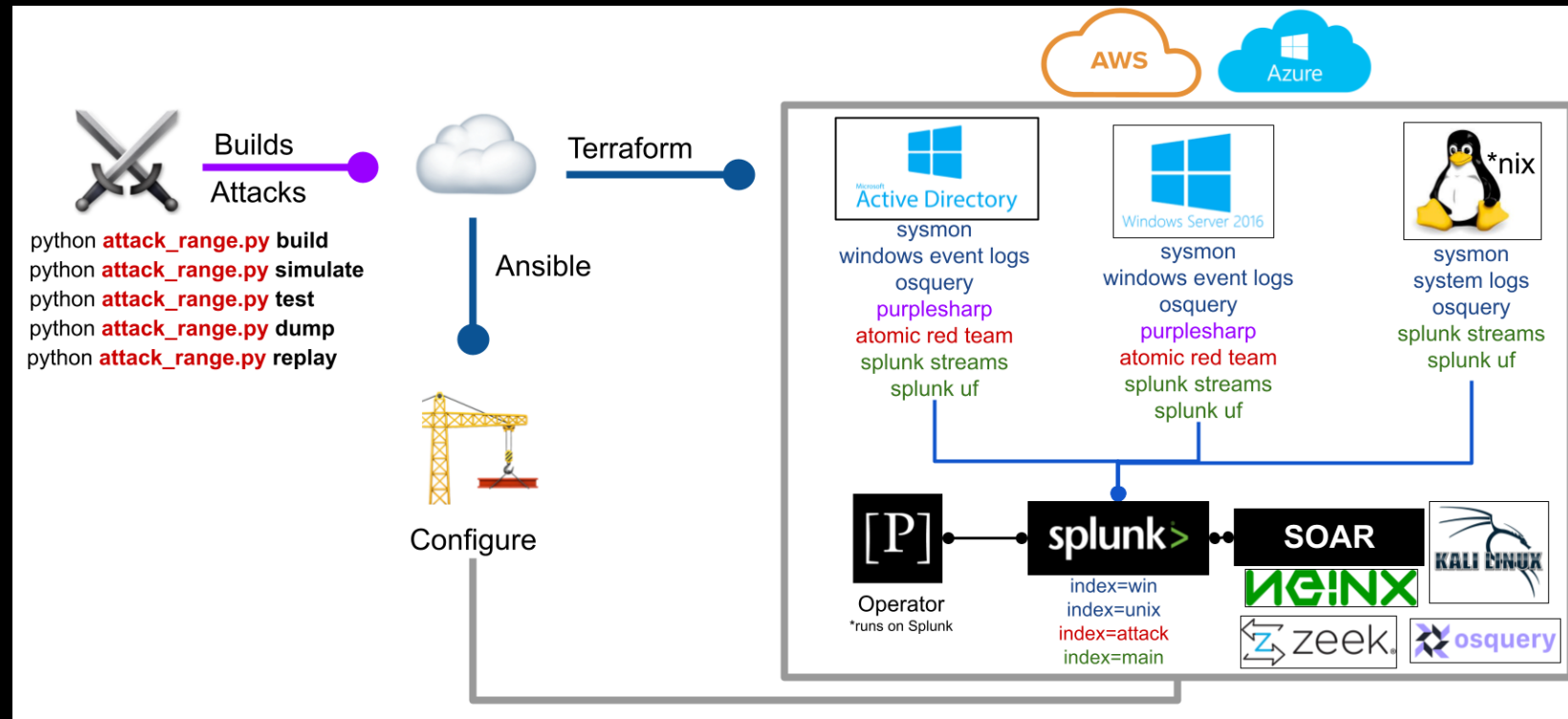
<https://www.detectionlab.network/>



Splunk Attack Range



https://github.com/splunk/attack_range

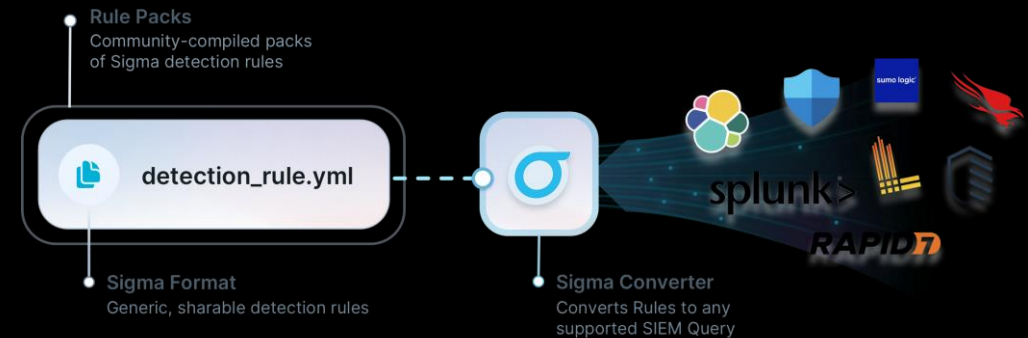


CREATING DETECTIONS



Sigma – Log Based Detections

- Open source, YAML based, portable signature format
- Vendor agnostic
- Large baseline rulesets (generic, threat hunting, emerging threats)
- <https://sigconverter.io/>



Creating Sigma Rules

```
title: a short capitalised title with less than 50 characters
id: generate one here https://www.uuidgenerator.net/version4
status: experimental
description: A description of what your rule is meant to detect
references:
  - A list of all references that can help a reader or analyst understand the meaning of a triggered rule
tags:
  - attack.execution # example MITRE ATT&CK category
  - attack.t1059      # example MITRE ATT&CK technique id
  - car.2014-04-003   # example CAR id
author: Michael Haag, Florian Roth, Markus Neis # example, a list of authors
date: 2018/04/06 # Rule date
logsource:
  category: process_creation # In this example we choose the category 'process_creation'
  product: windows          # the respective product
detection:
  selection:
    FileName: 'StringValue'
    FileName: IntegerValue
    FileName|modifier: 'Value'
  condition: selection
fields:
  - fields in the log source that are important to investigate further
falsepositives:
  - describe possible false positive conditions to help the analysts in their investigation
level: one of five levels (informational, low, medium, high, critical)
```

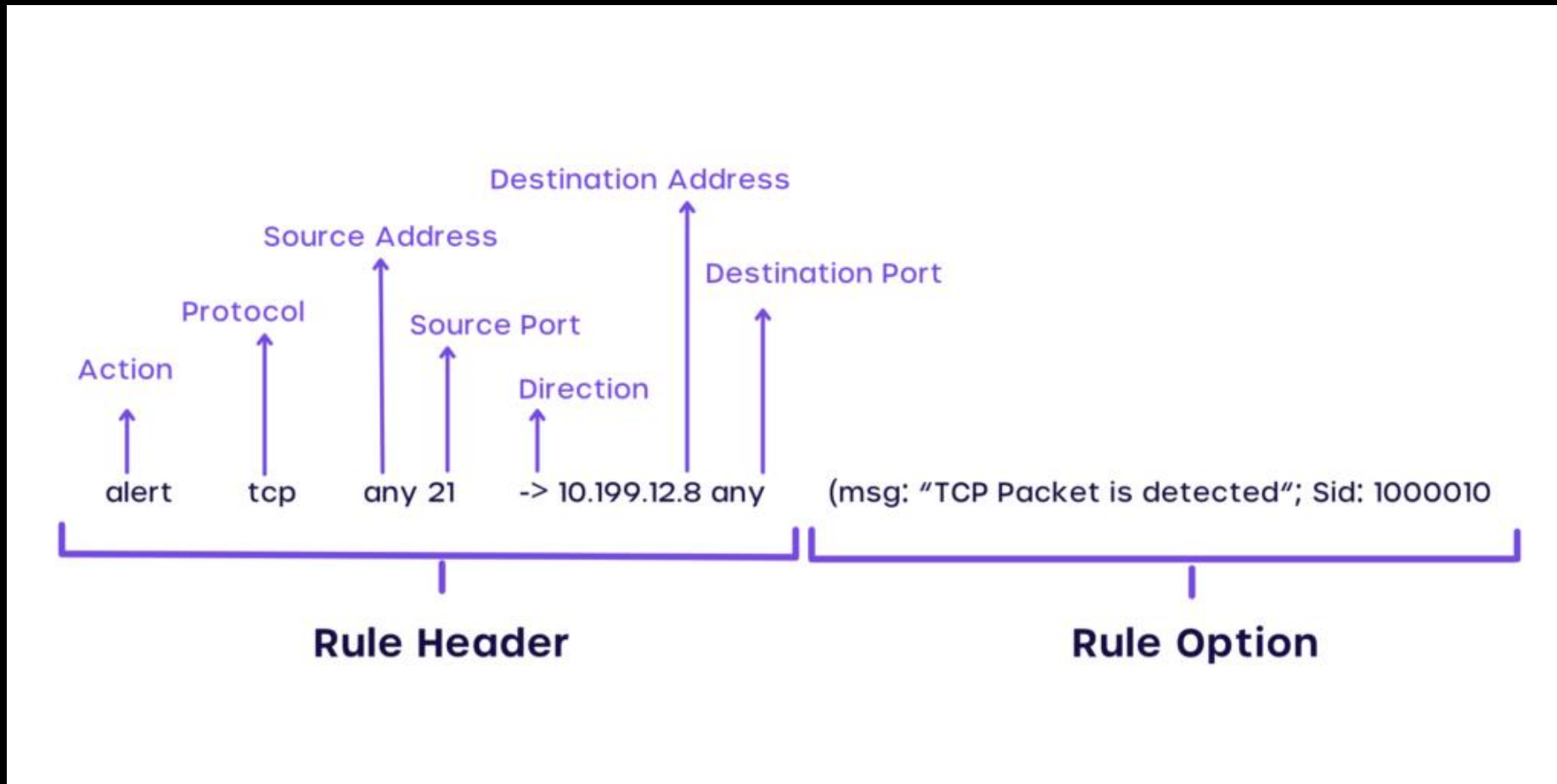
Sigma Example

```
1  title: Network Connection Initiated Via Notepad.EXE
2  id: e81528db-fc02-45e8-8e98-4e84aba1f10b
3  status: test
4  description: |
5      Detects a network connection that is initiated by the "notepad.exe" process.
6      This might be a sign of process injection from a beacon process or something similar.
7      Notepad rarely initiates a network communication except when printing documents for example.
8  references:
9      - https://web.archive.org/web/20200219102749/https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492186586.pdf
10     - https://www.cobaltstrike.com/blog/why-is-notepad-exe-connecting-to-the-internet
11  author: EagleEye Team
12  date: 2020/05/14
13  modified: 2024/02/02
14  tags:
15     - attack.command_and_control
16     - attack.execution
17     - attack.defense_evasion
18     - attack.t1055
19  logsource:
20     category: network_connection
21     product: windows
22  detection:
23     selection:
24         Image|endswith: '\notepad.exe'
25     filter_optional_printing:
26         DestinationPort: 9100
27     condition: selection and not 1 of filter_optional_*
28  falsepositives:
29     - Printing documents via notepad might cause communication with the printer via port 9100 or similar.
30  level: high
```


Snort – Network Based Detections

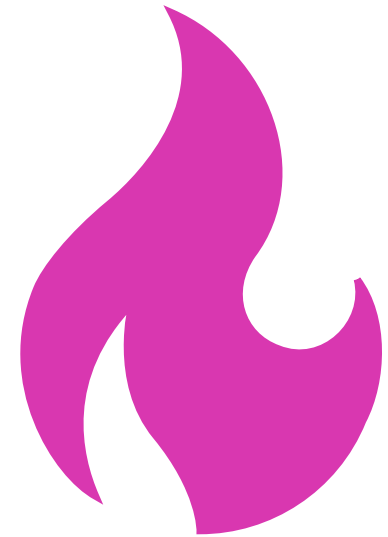
- Open source intrusion detection/prevention system (IDS/IPS)
 - Rule can be header based, payload based, or both
-

Snort Example



Generating Badness

- Useful for testing the efficacy of your detections
- Manual intervention – using things like Kali, nmap, Metasploit
- Automated AE tools
 - Caldera
 - Atomic Red Team



Summary

- Home labs are a great way to test things out and learn new things
 - Detection engineering is the process of creating detection logic
 - A good detection is repeatable, relevant, scalable, and high fidelity
 - The Pyramid of Pain can be a measuring stick for detection efficacy/complexity
 - A detection engineering lab requires a “network” and a SIEM/Log Collector, but an IDS and an array of different machines are recommended
 - Sigma (logs) and Snort (network) are two effective ways to start creating detections
 - You can generate “true positives” for your detection logic to test it
-



BONUS #1 - CYBERCHEF

CyberChef

- Data Formats (Base64, Hexdump, etc)
- Encryption/Decryption/Public Key
- Math
- Networking (IP Addresses, MAC Addresses, Domains, TCP, UDP, fang/defang)
- Timestamp conversions
- Hashing
- Code beautification
- YARA
- Steganography (LSB)
- Many, Many More...

- <https://github.com/gchq/CyberChef>



- <https://gchq.github.io/CyberChef/>



A photograph of various laboratory glassware on a shelf. From left to right, there is a beaker with a dark red liquid, a graduated cylinder with a green liquid, an Erlenmeyer flask with a yellow liquid, and another Erlenmeyer flask with a green liquid. The background is blurred, showing more glassware. A diagonal grey and white graphic element is overlaid on the right side of the image.

BONUS #2 - LAB ENVIRONMENT!

Splunk BOTS Docker

- More “Threat Hunting” than ”Detection Engineering”
- Splunk BOTS versions 1-3 in a single Docker Compose file
 - All addons and apps included in the repo
- Great way to learn Splunk
- <https://github.com/lexcilius/splunk-bots-docker>



Q & A

Thank You!

Resources

- <https://attack.mitre.org/>
 - <https://github.com/SigmaHQ/sigma>
 - <https://github.com/SigmaHQ/sigma/wiki/Rule-Creation-Guide>
 - <https://sigconverter.io/>
 - <https://www.snort.org/>
 - <https://caldera.mitre.org/>
 - <https://www.kali.org/>
 - <https://atomicredteam.io/>
 - <https://github.com/gchq/CyberChef>
 - <https://github.com/lexcilius/splunk-bots-docker>
-