**Blue Team Incident Investigation Cheat Sheet + Example**

**✨ Investigation Foundation (Always Start With These)**

**✍️ The 5 Ws (Investigation Logic)**

When reviewing any alert or anomaly, always start with these:

* **Who** triggered the event? (Which user or system? Was it a known admin or someone unexpected?)
* **What** was done? (Was a suspicious file executed, credentials dumped, or a process injected?)
* **Where** did it occur? (Endpoint? Cloud resource? DMZ host?)
* **When** did it happen? (Middle of the night? Right after a patch cycle?)
* **Why/How** was it possible? (Exploited vulnerability, misconfiguration, stolen credentials?)

🔍 **How Blue Team Uses This:**

* Build incident timeline
* Identify attacker entry point
* Determine lateral scope
* Prioritize response based on risk (critical user? core server?)

**🔎 MITRE ATT&CK (Behavior Map)**

* Helps blue teamers label observed behavior with known attacker tactics/techniques
* Makes detection coverage easier to map
* Enables threat hunting based on behaviors, not just IOCs

🔍 **How Blue Team Uses This:**

* Tag alerts with TTPs (e.g. "This is T1059.001 - PowerShell")
* Predict what the attacker might do next
* Build detection rules and playbooks per tactic

**🌐 Cyber Kill Chain (Attack Storyboard)**

Use this model to understand the attacker’s **overall campaign**:

1. **Recon:** Passive scanning, open-source data gathering
2. **Weaponization:** Crafting malware/payload
3. **Delivery:** Email, exploit, infected site
4. **Exploitation:** Code executes, system exploited
5. **Installation:** Malware installed or persistence gained
6. **Command & Control:** Attacker connects remotely
7. **Actions on Objectives:** Data theft, ransomware, impact

🔍 **How Blue Team Uses This:**

* Visualize entire timeline
* Identify where detection/prevention failed
* Report effectively to non-technical teams (storytelling)

**△ Pyramid of Pain (Detection Value – In Plain English)**

|  |  |
| --- | --- |
| **Indicator Type** | **Value & Action** |
| **Hash** | ❌ **Low Value** – A file’s fingerprint. Easy for attacker to change. Don’t rely on just this. |
| **IP/Domain** | ❌ **Low Value** – Attackers use new ones constantly. Use threat intel but don’t count on it. |
| **Tool** | ⚠️ **Medium Value** – Tools like mimikatz or procdump are known, but attackers can rename them. |
| **Behavior/TTP** | ✅ **High Value** – Detecting *how* they act (like running PowerShell to access credentials) is hard to change. Gold standard. |

🔍 **How Blue Team Uses This:**

* Focus on attacker behavior patterns over simple IOCs
* Build detection rules that catch tactics (like credential theft), not just filenames
* Prioritize time and resources on behavior-based detections

🛠️ **Example Detection Rule (in super plain terms):**

"If someone runs PowerShell, and that command is encoded (looks scrambled or base64), and it tries to look at or dump LSASS (which stores passwords), send an alert."

**Simple detection logic (like in Splunk):**

index=windows\_logs (EventCode=4104 OR EventCode=4688)

(CommandLine="\*powershell\*" AND CommandLine="\*enc\*" AND (CommandLine="\*lsass\*" OR CommandLine="\*procdump\*"))

**Why this works:**

* PowerShell is rarely encoded unless something shady is happening
* Accessing lsass.exe is how attackers steal passwords
* Catching both = high-confidence, high-pain detection

**📊 Baseline + Deviation**

Knowing "normal" is the only way to spot "abnormal."

🔍 **What to Compare:**

* PowerShell usage for standard users
* After-hours activity on critical assets
* Volume of data transferred
* Software usage by department

🔍 **How Blue Team Uses This:**

* Write anomaly-based alerts
* Find stealthy attacks that evade signature rules
* Prioritize alerts based on abnormal context

**💡 Example Incident Walkthrough**

**📅 Scenario: Phishing Email Leads to Remote Access and Data Exfiltration**

**🔍 The 5 Ws:**

* **Who:** User john.smith@company.com
* **What:** Opened a phishing email and Excel attachment
* **Where:** Host CORP-LAPTOP-023 (Finance Dept.)
* **When:** April 21, 2025, 09:22 AM
* **Why/How:** Excel macro launched PowerShell to contact a remote server

**📊 MITRE ATT&CK + Blue Team Actions:**

|  |  |  |  |
| --- | --- | --- | --- |
| Tactic | Technique + ID | What Happened | How Blue Team Investigates |
| Initial Access | T1566.001 | Spearphishing via Excel | Review email headers and attachment, isolate user email, scan for similar threats |
| Execution | T1059.001 | PowerShell from macro | Search EventCode 4104 logs for script content, correlate with process tree |
| Persistence | T1547.001 | Registry Run key added | Investigate Sysmon Event 13, autorun paths, confirm script legitimacy |
| Privilege Escalation | T1134.001 | SYSTEM token impersonation | Check for token use anomalies, high-privilege token elevation logs |
| Defense Evasion | T1027 | PowerShell base64 encoding | Decode payload, search for reuse across enterprise |
| Credential Access | T1003 | LSASS dump with procdump.exe | EDR alert for LSASS access, look for procdump, monitor dump files |
| Discovery | T1082 | Recon commands run | Review PowerShell history, EventCode 4103, look for AD and system enumeration |
| Lateral Movement | T1021.002 | Accessed HR-SERVER-04 | Identify shared credential reuse, unusual login locations and times |
| Collection | T1560.001 | Files zipped with rar.exe | Alert on new use of archivers, especially on non-IT endpoints |
| Exfiltration | T1048 | Upload to C2 over HTTPS | Proxy logs, traffic volume spikes, unknown IP destinations |
| Command & Control | T1071.001 | Beacon to domain evilhost.net | Detect recurring outbound PowerShell web traffic, use DNS logs and firewall logs |

**🔹 Cyber Kill Chain Walkthrough:**

1. **Recon:** Emails collected from LinkedIn
2. **Weaponization:** Excel macro payload crafted
3. **Delivery:** Email sent to finance employee
4. **Exploitation:** Macro runs, executes script
5. **Installation:** Persistence via Run key
6. **C2:** Periodic outbound beacons
7. **Actions:** Zipped data sent to attacker

🔍 **How Blue Team Uses This:**

* Match logs and alerts to each kill chain step
* Fill detection gaps based on missed stages
* Write up a report using this timeline

**△ Pyramid of Pain in Practice:**

* Hash: One-time use, attacker changed the file ✅
* IP: C2 rotated frequently ✅
* Tool: Used public tools (procdump) ⚠️
* Behavior: Encoded PowerShell + LSASS = signature-worthy ❌

🔍 **How Blue Team Uses This:**

* Focus detection effort on behaviors seen here
* Alert on encoded command patterns
* Investigate tools with potential dual-use

**📊 Baseline vs. Deviation:**

* User john.smith never uses PowerShell
* Login at 3AM is out of character
* rar.exe never used in Finance before

🔍 **How Blue Team Uses This:**

* Compare behavior with known profile
* Escalate based on deviation, not just IOC
* Develop anomaly rule for future alerts

**✅ Summary:**

* Used **5Ws** to scope the event quickly
* Mapped attacker behavior to **MITRE ATT&CK** for clarity
* Told the full attack narrative with **Kill Chain**
* Assessed alert value using **Pyramid of Pain**
* Validated suspicion with **baseline deviation**