**Report 2: Path Traversal Vulnerability**

**Title**: Directory Path Traversal on Check Point Security Gateway  
**Date**: May 30, 2025  
**Platform**: Let’s Defend SOC Simulator  
**Severity**: High  
**Detection** Tool: Chronicle SIEM  
**Category**: Injection / File Disclosure

**Steps Taken:**

* Reviewed query logs in Chronicle SIEM
* Identified payloads attempting file access:
  + ../../../../../etc/passwd
  + ../../../../../etc/shadow
* Scanned source IP (203.160.68.12) in VirusTotal
  + Flagged as malicious on VirusTotal
  + GeoIP traced to Hong Kong

**Final Assessment:**

**True Positive**. The attacker attempted to exploit a directory traversal vulnerability to read sensitive system files (/etc/passwd, /etc/shadow) from the firewall appliance.

**Mitigation**:

* Block the attacker’s IP address and monitor for related IP ranges
* Patch the vulnerable web service or WAF rule allowing traversal
* Implement strict input validation and output encoding on file-access parameters
* Limit web application access to sensitive files via least privilege
* Conduct vulnerability scans to identify similar exposures