Scenario 1: Performing a Query with Chronicle

Date: **November 05 2024.**	**Entry:** # 1
Description	This report documents an investigation into phishing activity targeting employees at the company. The investigation focuses on identifying impacted assets, employee interactions with the malicious domain, and indicators of compromise.
Tool(s) used	• **Chronicle:** Used for log analysis, domain investigation, and identifying indicators of compromise.
The 5 W's	• **Who:** A malicious actor leveraging a spoofed domain to steal employee credentials. • **What:** A phishing security incident involving the domain `signin.office365x24.com`. • **Where**: Affected assets include three employee machines and accounts at a financial services company. • **When**: Activity was observed from January 31, 2023, to July 8, 2023. • **Why**: The attackers used a spoofed domain resembling a legitimate Office 365 login page (`login.office365x24.com`). Employees unknowingly entered their credentials, resulting in POST requests to `/login.php`, indicating successful phishing attempts.
Additional	**Domain Context:** VirusTotal flagged the domain as malicious with

notes	reports from 12 security vendors. **Resolved IPs:** Two IP addresses associated with the domain (`104.215.148.63 and 40.100.174.34`). **Sibling Domains:** `login.office365x24.com` was identified as a related domain. **Key Findings:** **Malicious Domain:** `signin.office365x24.com` was identified as malicious by multiple security vendors. **Affected Assets:** Three employee machines accessed the domain and interacted with it via `POST` requests. **Infrastructure Reuse:** The attackers reused the same IP address across multiple phishing domains, indicating a broader campaign. **Credential Compromise:** `POST` requests suggest that credentials were likely exfiltrated.

Reflections for Scenario 2: Follow-Up Analysis and Actions	**Employee Awareness:** The success of this phishing attack highlights the need for enhanced employee training on identifying suspicious emails and domains. **Phishing Campaign:** The attacker's use of infrastructure reuse suggests a broader campaign that may target other organizations. **Log Analysis:** Chronicle's detailed log analysis and procedural filtering were instrumental in tracing the interactions with the malicious domain.

Follow-Up Actions	1. **Employee Training:** Conduct mandatory phishing awareness training sessions. 2. **Network Monitoring:** Increase monitoring of network traffic to detect suspicious domains or unauthorized data exfiltration attempts. 3. **Threat Intelligence Sharing:** Share findings with relevant industry threat intelligence groups to prevent similar incidents elsewhere. 4. **Blocking Malicious Domains:** Update firewall and DNS rules to `block signin.office365x24.com`, `login.office365x24.com`, and associated IP addresses. 5. **Credential Reset:** Require impacted employees to reset their passwords immediately and enforce multi-factor authentication (MFA).