Sam Perez

Module Title: T100: Overview of Falcon Next-Gen SIEM: Unify, Detect, and Automate

Learning Objective: By the end of this module, a learner will be able to:

1. Describe Falcon Next-Gen SIEM's key features such as:configure basic data ingestion and search, integrate with third-party tools, interpret alerts and metrics, analyze dashboards for emerging trends, and demonstrate its value through AI-powered detection and automated workflows.

Module Outline – CrowdStrike Falcon Next-Gen SIEM

1. **Introduction to Falcon Next-Gen SIEM**
   - Overview of capabilities, use cases, and benefits over legacy SIEMs.
2. **Architecture & Data Flow**
   - Overview of ingestion pipelines, Falcon Log Collector, and index-free search architecture.
3. **Data Onboarding & Log Ingestion**
   - Deploy Falcon Log Collector, onboarding Windows/Linux/macOS logs, and verifying data flow.
4. **CQL (CrowdStrike Query Language) Basics**
   - Query structure, syntax, and practical examples for incident detection.
5. **Search & Investigation Workflows**
   - Running searches, filtering events, and pivoting for deeper investigation.
6. **Dashboards, Alerts & Reporting**
   - Create visualizations, setting alerts, and generating incident reports.
7. **Best Practices & Optimization**
   - Tuning queries, managing ingestion limits, and aligning with security operations workflows.

Lab Title: "From Logs to Insights: Rapid Detection with Falcon Next-Gen SIEM"

Description:
Participants simulate an insider threat scenario. They ingest simulated Windows security logs via the Log Collector, search for anomalous login failures using CQL, build a custom dashboard tracking failed logins per user, and then configure a simple automated response using Fusion SOAR (e.g., trigger an email alert or quarantine user). The lab emphasizes speed, clarity, and automation.

Lab questions to check for knowledge application

Question 1:
In the lab, why is it important to verify data ingestion in the Data Onboarding dashboard before running CQL queries?
Expected Answer:
To confirm that log data is flowing into Falcon SIEM correctly, ensuring searches return accurate and complete results.

Question 2:
How can building a custom dashboard of failed logins per user help in detecting insider threats?
Expected Answer:
It provides a visual trend of suspicious activity over time, helping identify unusual patterns like spikes in login failures from specific accounts.

CROWDSTRIKE

Falcon Next-Gen SIEM – T100 Course Module
(Log Event Extended Format) LEEF

```
`event.type: "login failure" | top count by user_name`
```

```
LEEF:1.0|CrowdStrike|FalconHost|1.0|Suspicious Activity|
devTime=2016-06-09 02:57:28^src=10.1.1.1^srcPort=49220^dst=10.1.1.2^
domain=I^cat=NetworkAccesses^usrName=test^devTimeFormat=yyyy-MM-dd
HH:mm:ss^connDir=0^dstPort=443^resource=<Resource>^proto=TCP^url=http
s://example.com/url
```

AI Voiceover Script:

Let's walk through your first Falcon Next-Gen SIEM use case—ingesting Windows Event Logs and exploring search. First, deploy the Falcon Log Collector agent on your Windows endpoints. This lightweight component securely forwards logs to the SIEM.

Next, let's search. Using CrowdStrike's intuitive CQL (CrowdStrike Query Language), you can easily query for suspicious events. For instance, you might enter:

`event.type: "login failure" | top count by user_name`

CrowdStrike's Falcon SIEM Connector can be used to forward event data to a SIEM in Log Event Extended format or LEEF in short. During configuration, you need to specify the necessary API keys and select LEEF as the output format in the connector's configuration. Take a look at this an event log of a suspicious activity. What data points can you identify. Take a moment and analyze. (Pause for 5 seconds.)

This log captures a monitored outbound HTTPS request from **10.1.1.1** to **10.1.1.2** over port 443. CrowdStrike flagged this as "Suspicious Activity" based on its detection rules and possibly due to:

- Known malicious domain/URL
- Unusual connection behavior from the user test
- Policy violation such as attempting to access restricted resource