Chronicle SIEM Fundamentals

Category: Networking & Security | **Vendor:** Various

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

- Module 1: Chronicle Access
- Module 2: Searching with Chronicle

Hands-On: Raw Log & UDM Search

- Module 3: Chronicle Data On Boarding

Hands-On: Collect Linux Syslog

- Module 4: Parsing Data In Chronicle
- Module 5: Curated Detections
- Module 6: Visualizing Alerts With Chronicle

Hands-On: Navigating and Reviewing using Alert Graph

- Module 7: Entity Graph

Hands-On: Search – Asset\User Enrichment

- Module 8: Advance Searching With Chronicle

Hands-On: Advanced Search

- Module 9: Building Rules For Chronicle

Hands-On: Building Rules

- Module 10: Visualizing Alerts (Advance)
- Module 11: Entity Graph (Advance)
- Module 12: Visualizing Data in Chronicle Hands-On: Building Dashboard In Chronicle

About This Course

- Module 1: Chronicle Access
- Module 2: Searching with Chronicle

Hands-On: Raw Log & UDM Search

- Module 3: Chronicle Data On Boarding

Hands-On: Collect Linux Syslog

- Module 4: Parsing Data In Chronicle
- Module 5: Curated Detections
- Module 6: Visualizing Alerts With Chronicle

Hands-On: Navigating and Reviewing using Alert Graph

- Module 7: Entity Graph

Hands-On: Search – Asset\User Enrichment

- Module 8: Advance Searching With Chronicle

Hands-On: Advanced Search

- Module 9: Building Rules For Chronicle

Hands-On: Building Rules

- Module 10: Visualizing Alerts (Advance)
- Module 11: Entity Graph (Advance)
- Module 12: Visualizing Data in Chronicle Hands-On: Building Dashboard In Chronicle

Who Should Attend

Individuals who need a basic introduction to Chronicle SIEM

Prerequisites & Entry Requirements

General Prerequisites:

Basic knowledge about what is SIEM & SOAR

Learning Outcomes

Upon successful completion of this course, participants will be able to:

Explore the essentials of Chronicle, a powerful Security Information and Event Management (SIEM) solution offered as a cloud service on the robust Google infrastructure. The Chronicle Fundamentals course provides an in-depth overview of the key functionalities, data analysis capabilities, and security aspects of Chronicle SIEM.

- Chronicle Access – Role-Based Access Control (RBAC) in Chronicle. Why Audit logging is important and how to implement it in your Chronicle instance.
- Learn about Raw Log Search and UDM Search, how to use Search for investigation.
- Chronicle Data On Boarding: forwarders, feed management, ingestion API, and direct ingestion.
- Introduction to Chronicle Parsers – What is a parser, versioning, and parser extension.
- Walkthrough of Chronicle Curated Detection rules.
- Navigating Alerts using the Alert Graph: Entity data, releted alerts, alert context.
- Learn about Entity data – Data enrichment in Chronicle, Entity types (Users & Assets), Resources, Geo IP Enrichment.
- Advanced Search Capabilities: Reference Lists, Group Fields, Pivot, Search for Alerts.
- Parsing data in Chronicle – What are parsers and how can we manage them: Parser update, versioning, parser extensions.
- Building rules for Chronicle: YARA-L 2.0 syntax, Rules UI, Single event rules, Multi-event rules, using entity data in rules, Outcomes, Functions & Lists, best practice.
- Building dashboards in Chronicle.

Detailed Course Outline

Module 1: Chronicle Access

Module 2: Searching with Chronicle (Hands-On: Raw Log & UDM Search)

Module 3: Chronicle Data On Boarding (Hands-On: Collect Linux Syslog)

Module 4: Parsing Data In Chronicle

Module 5: Curated Detections

Module 6: Visualizing Alerts With Chronicle (Hands-On: Alert Graph)

Module 7: Entity Graph (Hands-On: Search - Asset/User Enrichment)

Module 8: Advance Searching With Chronicle (Hands-On: Advanced Search)

Module 9: Building Rules For Chronicle (Hands-On: Building Rules)

Module 10: Visualizing Alerts (Advance)

Module 11: Entity Graph (Advance)

Module 12: Visualizing Data in Chronicle (Hands-On: Building Dashboard)

Skills You Will Learn:

Explore the essentials of Chronicle, a powerful Security Information and Event Management (SIEM) solution offered as a cloud service on the robust Google infrastructure. The Chronicle Fundamentals course provides an in-depth overview of the key functionalities, data analysis capabilities, and security aspects of Chronicle SIEM.

- Chronicle Access – Role-Based Access Control (RBAC) in Chronicle. Why Audit logging is important and how to implement it in your Chronicle instance.
- Learn about Raw Log Search and UDM Search, how to use Search for investigation.
- Chronicle Data On Boarding: forwarders, feed management, ingestion API, and direct ingestion.
- Introduction to Chronicle Parsers – What is a parser, versioning, and parser extension.
- Walkthrough of Chronicle Curated Detection rules.
- Navigating Alerts using the Alert Graph: Entity data, releted alerts, alert context.
- Learn about Entity data – Data enrichment in Chronicle, Entity types (Users & Assets), Resources, Geo IP Enrichment.
- Advanced Search Capabilities: Reference Lists, Group Fields, Pivot, Search for Alerts.
- Parsing data in Chronicle – What are parsers and how can we manage them: Parser update, versioning, parser extensions.
- Building rules for Chronicle: YARA-L 2.0 syntax, Rules UI, Single event rules, Multi-event rules, using entity data in rules, Outcomes, Functions & Lists, best practice.
- Building dashboards in Chronicle.

Frequently Asked Questions

Q: What delivery options are available for Chronicle SIEM Fundamentals?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 3-day Chronicle SIEM Fundamentals course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Chronicle SIEM Fundamentals training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Chronicle SIEM Fundamentals?

Yes, we provide corporate training, dedicated training, and closed classes for Chronicle SIEM Fundamentals. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Chronicle SIEM Fundamentals, Networking & Security, CSIEMF

Q: Why choose Nexus Human for Chronicle SIEM Fundamentals?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Chronicle SIEM Fundamentals training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)