ReliaQuest University

RELIAQUEST

ReliaQuest University is a comprehensive development program designed to maximize its customers potential. RQU is our commitment to grooming the industry's most elite security professionals.

As part of our service offering, all ReliaQuest customers are eligible to enroll in ReliaQuest University.

ReliaQuest customers will receive immersive, customized, and instructor-led training around the professional, procedural, and technical standards of a variety of SIEM technology solutions.

RQU

SIEM Program Overview: QRadar

Each participant will engage with QRadar to give them a familiarization with Aerial Query Language(AQL) and the WebUI as it relates to the role of an analyst. While engaging the QRadar curriculum the participants will learn how to effectively conduct pivot searches, rule identification/utilization, and how to engage Offenses. Each learning objective will be supported by a series of hands-on labs that give the participants the necessary experience to engage QRadar more effectively and efficiently from an Incident Response perspective.

SIEM Program Overview: Splunk

Each participant will engage with Splunk to give them a familiarization of Search Processing Language (SPL) and the WebUI with a focus on the Enterprise Security App as it relates to the role of an analyst. While engaging the Splunk curriculum the participants will learn how to effectively use SPL when conducting searching techniques, rule identification/utilization, and how to engage network/asset management modules. Each learning objective will be supported by a series of hands-on labs that give the participants the necessary experience to engage Splunk more effectively and efficiently from an Incident Response perspective.

SIEM Program Overview: LogRhythm and ArcSight

Each participant will engage with the SIEM technology to give them a deep familiarization of both the consoles as it relates to the role of an analyst. While engaging the SIEM curriculum the participants will practice effective searching techniques, rule identification/utilization, and how to engage network/asset management modules. Each learning objective will be supported by a series of hands-on labs that give the participants the necessary experience to engage the specific SIEM more effectively and efficiently from an Incident Response perspective.

ReliaQuest University Program Learning Objectives

ALERT LOGIC

- Gain an understanding of how rules are written within the SIEM including, the logic, syntax and structure of rules or alerts.
- Understand the location of the alert logic contained within the SIEM.
- Ability to identify which rules/alerts have fired within the SIEM.

SEARCHING

- Gain an understanding and practice creating effective search strings using SIEM specific language.
- Gain an understanding and practice using multiple artifacts to create effective and proficient searches. (i.e. Source IP, Destination IP)

SEARCHING

- Gain an understanding of how the SIEM normalizes event logs across different technologies (e.g. failed authentication).
- Understanding of the zones and/or device groups input within the SIEM (e.g. DMZ, Network Devices, User Workstations, etc.).

To learn more about the RQU programs, please contact your Delivery Manager.