NETWITNESS XDR

HUNTER

NETWITNESS PLATFORM FOUNDATIONS

- Fundamental concepts of the NetWitness Platform
- Threat visibility and analysis capabilities
- Email reconstruction, event and file analysis, and meta keys
- Basic architecture and data flow
- Drawing data from logs, packets, and endpoint

NETWITNESS PLATFORM ANALYSIS

- Responding to incidents with the ananlysis of logs, packets and Advanced Endpoint
- Investigating incidents in the queue, documenting incidents, and escalating or closing incidents
- Analyzing incidents using recommended processes

NETWITNESS PLATFORM INTRODUCTION TO HUNTING

- Describing threat hunting and incident response roles
- Using hunting techniques, methodology, and tools to detect threats
- Describing the NetWitness Hunting Cards
- Identifying protocol and service anomalies
- Responding to incidents and reporting findings

NETWITNESS PLATFORM HUNTING CHALLENGE

- A private group Instructor-led class that gives you the opportunity to hunt for adversaries in a realistic environment
- Identifying targeted and compromised systems, reconstructing the sequence of events, and proposing a remediation plan
- Competing with other participants to collect points through investigation and by answering questions
- Conducting analyses using knowledge of networking protocols, endpoint operating systems, and common cyber-attack vectors

NETWITNESS SPECIALIST ANALYST CERTIFICATION EXAM

NETWITNESS
XDR
SPECIALIST
ANALYST

This certification reflects the fundamental knowledge required of security analysts performing incident response and analysis with the NetWitness Platform. The prerequisite for this certification is the NetWitness Certified Associate certification.

NETWITNESS
EDUCATION