TANIUM LEARNING CENTER

TANIUM THREAT RESPONSE ANALYST

COURSE DESCRIPTION

Tanium Threat Response Analyst is an immersive training that teaches learners how to manage and neutralize cyber threats through strategic incident response and analysis techniques.

Participants will learn how to use Tanium's powerful abilities to gain valuable network visibility, assess potential risks, plan for threat remediation, and empower IT teams to continuously secure, control, and manage every endpoint at speed and scale.

*Interactive lab access will be provided for hands-on activities.

DELIVERY OPTIONS

Instructor-Led Training (ILT)

Virtual Instructor-Led Training (VILT)

Web-Based Training (WBT)

ADDITIONAL RESOURCES

- Tanium Community Discussions and Groups
- Tanium Resource Center

Delivery options and duration

ILT/vILT: 8 hours | WBT: 4-6 hours

Prerequisites

Getting Started With Tanium

Target audience

This course is intended for Tanium operators who are ready to expand their knowledge of the Tanium Threat Response platform, and desire to become more proficient in the operation and primary use cases of Tanium Modules.

Registration information

For a list of scheduled courses and registration access, please log in to your Tanium Learning Center account.

If you do not have access to the Tanium Learning Center, please contact training@tanium.com.

COURSE OBJECTIVES

TANIUM THREAT RESPONSE ANALYST

- Identify key components and functionalities of Tanium for proactive threat hunting
- Analyze detection engineering techniques and manage intel effectively using Tanium
- Evaluate and prioritize alerts within SOC operations using Tanium's alerting capabilities
- Investigate incidents and perform incident response using Tanium's investigative tools
- Implement remediation strategies to address security gaps and improve security posture using Tanium

COURSE OUTLINE

INTRODUCTION

- Tanium for security
- Scenario introduction
- Learning objectives

THREAT HUNTING

- Understanding threat hunting
- Tanium and threat hunting
- Using Tanium Questions
- Enterprise Hunting dashboard
- Sending data to the SIEM
- Proactive hunting with Tanium
- Scenario

DETECTION ENGINEERING

- Understanding detection engineering
- Understanding intel options
- Testing & deploying intel
- From intel to alert
- Intel testing & tuning

SOC OPERATIONS

- Alert overview
- Alert details: finding context
- Triaging alerts
- Scenario

INCIDENT RESPONSE

- Knowing your data sources
- Investigating an alert
- Containment & response
- Scenario

REMEDIATION

- Remediation with Tanium