Tanium Certified Professional Endpoint Risk and Security (TCPRS)

SKU: TAN-EXAM-TCPRS / Exam Code: TAN-5100

TCPRS serves to identify candidates who possess the ability to address common use cases in Security, Risk, and Compliance using Tanium. The exam consists of 60 total score points, including multiple choice items and practical application items, and has a seat time of 110 minutes.

Tanium Certified Professional Endpoint Risk and Security Workflow

- **PREVIOUSLY ACHIEVED TANIUM CERTIFIED OPERATOR (TCO) CERTIFICATION**
- **"WORKING WITH TANIUM WBTS" OR "WORKING WITH TANIUM: ENDPOINT RISK AND SECURITY" COURSE**
- **TANIUM CERTIFIED PROFESSIONAL ENDPOINT RISK AND SECURITY EXAM**

CANDIDATE PROFILE:

An experienced Tanium user with 2-3 years of IT experience, a working knowledge of risk, security, and compliance, and 6-12 months of hands-on experience using Tanium to complete a variety of tasks including:

- Manage compliance and vulnerability of enterprise assets
- Discover and monitor sensitive information
- Employ threat intelligence, collect forensics data, and triage suspicious events
- Manage native endpoint security policies and firewalls
- Curate and manage threat intel

PREREQUISITES REQUIRED:

TCO Certification

RECOMMENDED COURSES:

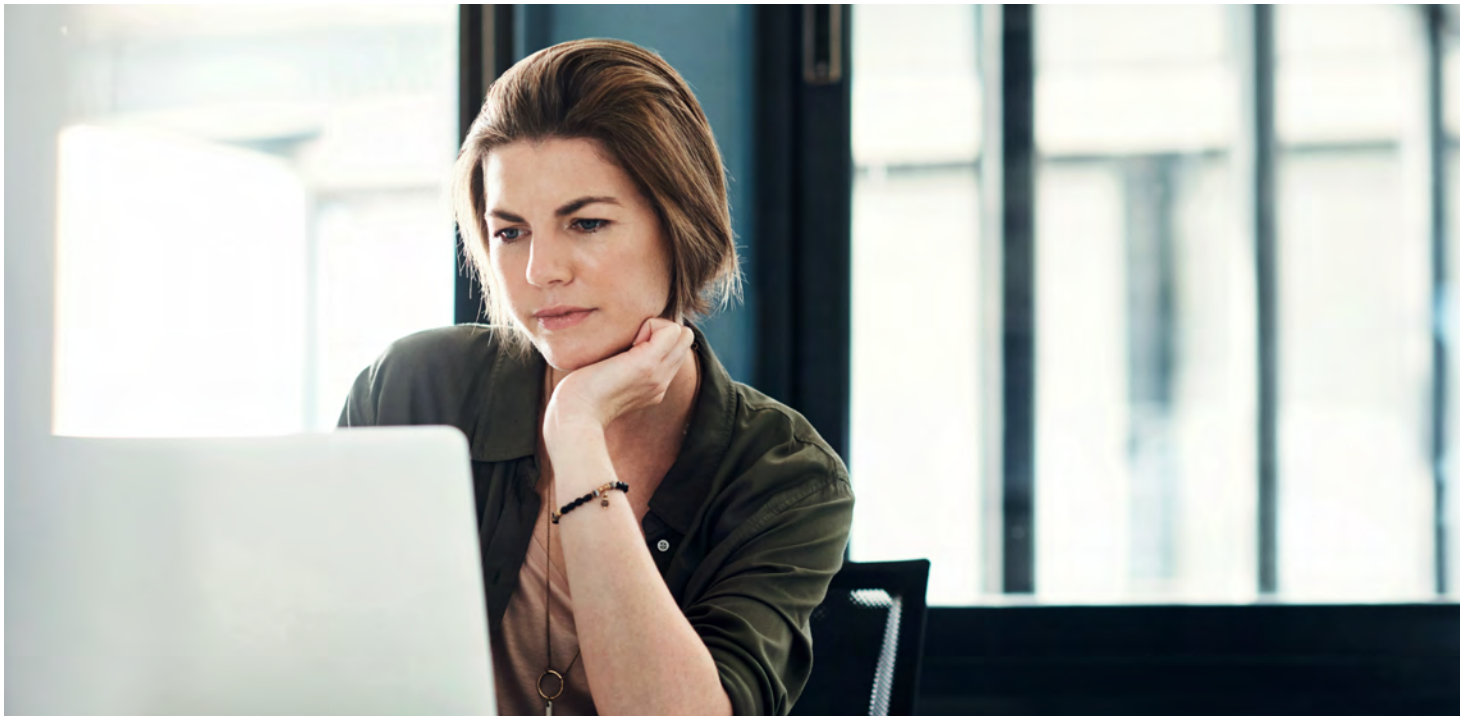
Working with Tanium WBTs:

- Comply
- Reveal
- Benchmark
- Enforce
- Integrity Monitor
- Threat Response

Or Working with Tanium: Endpoint Risk and Security

REQUIRED:

Passing score on the TCPRS exam



Exam blueprint

Please review the exam blueprint to learn what to expect and to help you prepare. The blueprint provides general guidelines for the content likely to be included on the exam. Related topics may also appear on any specific delivery of the exam. Blueprints may change at any time without notice.

COMPLY – 20%

- Manage vulnerability assessments
- Interpret and monitor vulnerability exposures
- Manage compliance assessments
- Analyze and evaluate security policies and configuration
- Analyze compliance findings
- Recognize when and how to exclude known and accepted compliance or vulnerability findings

THREAT RESPONSE – 33%

- Investigate and respond to suspicious endpoint activity
- Perform initial alert triage
- Perform threat hunting activities
- Collect forensic data
- Manage intel

ENFORCE – 13%

- Manage configuration policy and enforcements
- Manage remediation policy and apply enforcement

REVEAL – 14%

- Manage validations
- Manage rules/rulesets
- Perform quick searches
- Analyze and evaluate findings
- Manage profiles

BENCHMARK – 8%

- Analyze Benchmark data and identify areas of improvement
- Pivot to action for remediation
- Investigate Benchmark metrics

INTEGRITY MONITOR – 12%

- Analyze unexpected change events
- Manage monitors
- Manage labels/rules
- Manage watchlists for sensitive data monitoring

Tanium, the industry's only provider of Converged Endpoint Management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. Visit us at www.tanium.com.