ROLE-BASED

CyberVista®

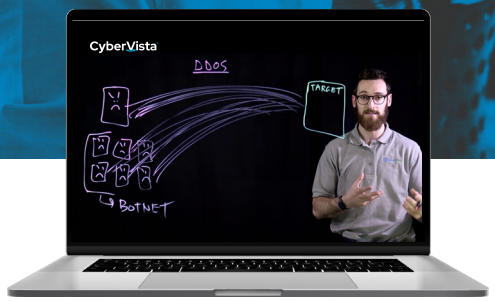
Critical Knowledge™

Overview

Organizations today still struggle to source, develop, and retain top cybersecurity talent. Moreover, without a clear method of identifying current competencies and skills gaps of employees, training falls short of effectively preparing individuals for these critical roles.

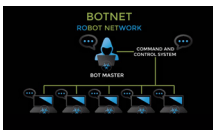
As leaders realize that they can't rely on or wait for traditional talent sources to improve, investing in growing talent internally through entry-level talent initiatives has become a necessity.

CyberVista created **Critical Knowledge,** a holistic cybersecurity training solution aligned to the NICE Framework, to help cybersecurity leaders enhance workforce development strategies.



Domain 2, DDOS

Domain 1, NTP



Domain 2, DDOS

What is the Critical Knowledge Course?

Critical Knowledge is designed to function as an industry-standard cybersecurity training program, directly aligned to the highly adopted NICE Framework. The purpose of Critical Knowledge is to provide leaders with a better way to identify and develop talent through fundamental cybersecurity skills training. Organizations who use Critical Knowledge benefit by filling persistent skills gaps, ensuring baseline knowledge across teams and individuals, while indirectly improve hiring and retention strategies for cybersecurity and cyber-enabled teams.

The curriculum spans seven units ranging from foundational to advanced cybersecurity topics, covering networking fundamentals, types of attacks, technical concepts, and operations. Units are modular in design, each comprising four to nine hours of dedicated training material, so participants can digest all or specific topics that are most relevant to their current or aspirational position.

CyberVista uses a diagnostics-first approach to training. Our diagnostic assessments can identify employee strengths and weaknesses at the onset of training to outline the most optimal learning path for employee success. In short, it allows your organization to train with purpose.

Who is this program for?

- **Entry-level cybersecurity talent** to help achieve the desired skills baseline
- **IT professionals transitioning to cybersecurity** who want to build on technical experience in a new field
- **Experienced cybersecurity professionals** who want to shift careers to another field within cybersecurity
- **Professionals with non-technical backgrounds entering cybersecurity**

Benefits of Training

- Mapped to the Workforce Framework for Cybersecurity (NICE Framework)
- Quickly identify and develop KSA strengths and weaknesses for multiple cyber roles
- Gain a more holistic view of the cybersecurity ecosystem and its unique subgroups
- Implement more effective hiring and career development strategies

Course Units

1

NETWORK FUNDAMENTALS

Review foundational concepts on networking and computing principles, network functions, and potential vulnerabilities

2

ATTACKS & VULNERABILITIES

Identify and define the different types of cyber attacks and vulnerabilities.

3

NETWORK SECURITY

Understand how to defend a network through various devices and techniques.

4

SECURITY ENGINEERING

Understand additional technical security defenses, security frameworks, and protocols.

5

RISK MANAGEMENT & GOVERNANCE

Review different risk management principles, laws and regulations, and business continuity planning.

6

SECURITY OPERATIONS

Gain perspective on the function of security operations that upholds organizationAl security posture.

7

OFFENSIVE & DEFENSIVE SCHEMA

Identify and define the different methods of basic offensive and defensive operations.

What's included?

- **Diagnostic Assessment:** Gain a snapshot of the current competencies by individual and team.
- **Video Library:** Engaging modular, on-demand video lessons including guided lab walk-throughs.
- **Labs:** Guided and problem-oriented labs to reinforce practical applications.
- **(Optional) Live Online Training Sessions**
- **Final Assessment:** A final assessment to measure improvement following the training engagement.
- **Final Insights Report:** An extensive workforce analysis providing key insights on results and recommendations for continuous improvement.

> We had excellent help from the account management to the instructors—a great experience all around. **Really great business and people.**

Director of SOC
Fortune 100 Retail Client

Gartner peerinsights

Let's talk.

See new opportunities for your cybersecurity workforce.

For more information contact us at **sales@cybervista.net** or call **844-558-4782.**

CyberVista