NICE Challenge PROJECT

The Workforce Experience Before the Workforce

100+ Unique Challenges

400+ Colleges
750+ Educators

Our Mission

The NICE Challenge Project develops real world cybersecurity challenges within virtualized business environments that bring students the workforce experience before the workforce. Our goal is to bring the most realistic experiences to students, at scale year round, while also generating useful assessment data about their knowledge, skills, and abilities for educators.

How We Do It

Platform

We manage the hardware, hypervisors, & software at no cost to U.S. EDU

Powerful cross platform web application, no downloads required

Deploy challenges, access VM consoles, manage user accounts, & review results

Challenges

Competency based assessments focused on real world problems & context

Maps to NICE Framework Tasks, Work Roles, KSAs, & CAE KUs

Designed to capture useful data for actionable metrics & analytics

Environments

Full scale context rich business environments tailored around NICE Framework Categories

Fictional organizations & employees

Virtualized networks, servers, desktops, & specialized equipment

Challenge Mappings & Highlights

Protect & Defend

Specialty Areas
Cyber Defense Analysis
Cyber Defense Infrastructure Support
Incident Response

Work Roles
Cyber Defense Analyst
Cyber Defense Incident Responder
Cyber Defense Infrastructure Support Specialist

Challenge Highlight: Malware Aftermath Cleanup

Being a small retailer and having limited funding for technical staff, Pretty Safe Electronics (PSE) contracts with a managed service provider (MSP) to do some systems management and upkeep. Unfortunately, this expands the pool of people who have administrative access to business-critical systems. In this challenge, the MSP's access is misused by a rogue employee to implant some custom-made malware for purposes unknown. The player is told to review some suspicious looking traffic on the main firewall and from there they must identify the compromised system, quarantine the malware, and oust the rogue former MSP employee from the system.

Operate & Maintain

Specialty Areas
Customer Service & Technical Support
Data Administration
Knowledge Management
Network Services
Systems Administration
Systems Analysis

Work Roles
Data Analyst
Knowledge Manager
Network Operations Specialist
System Administrator
Systems Security Analyst
Technical Support Specialist

Challenge Highlight: STIG Solutions

DasWebs recently ordered an external security audit of its on-site systems and servers. The after-audit report yielded a fair number of security improvements that could be made to the company's internal systems. In this challenge, the company's security lead has tasked the player with implementing CAT I STIG baselines on the Windows-based employee workstations.

Investigate

Specialty Area
Digital Forensics

Work Role
Law Enforcement/Counterintelligence Forensics Analyst

Challenge Highlight: Digital Duplicates

A mysterious thumb drive has been found attached to an employee's workstation. Only one employee has access to the workstation and is unaware of the thumb drive's origin. The thumb drive was turned over to the company's security analyst and hooked up to a sheep dip system. In this challenge, the player has been tasked with creating a forensically sound duplicate of the thumb drive without modifying the original.