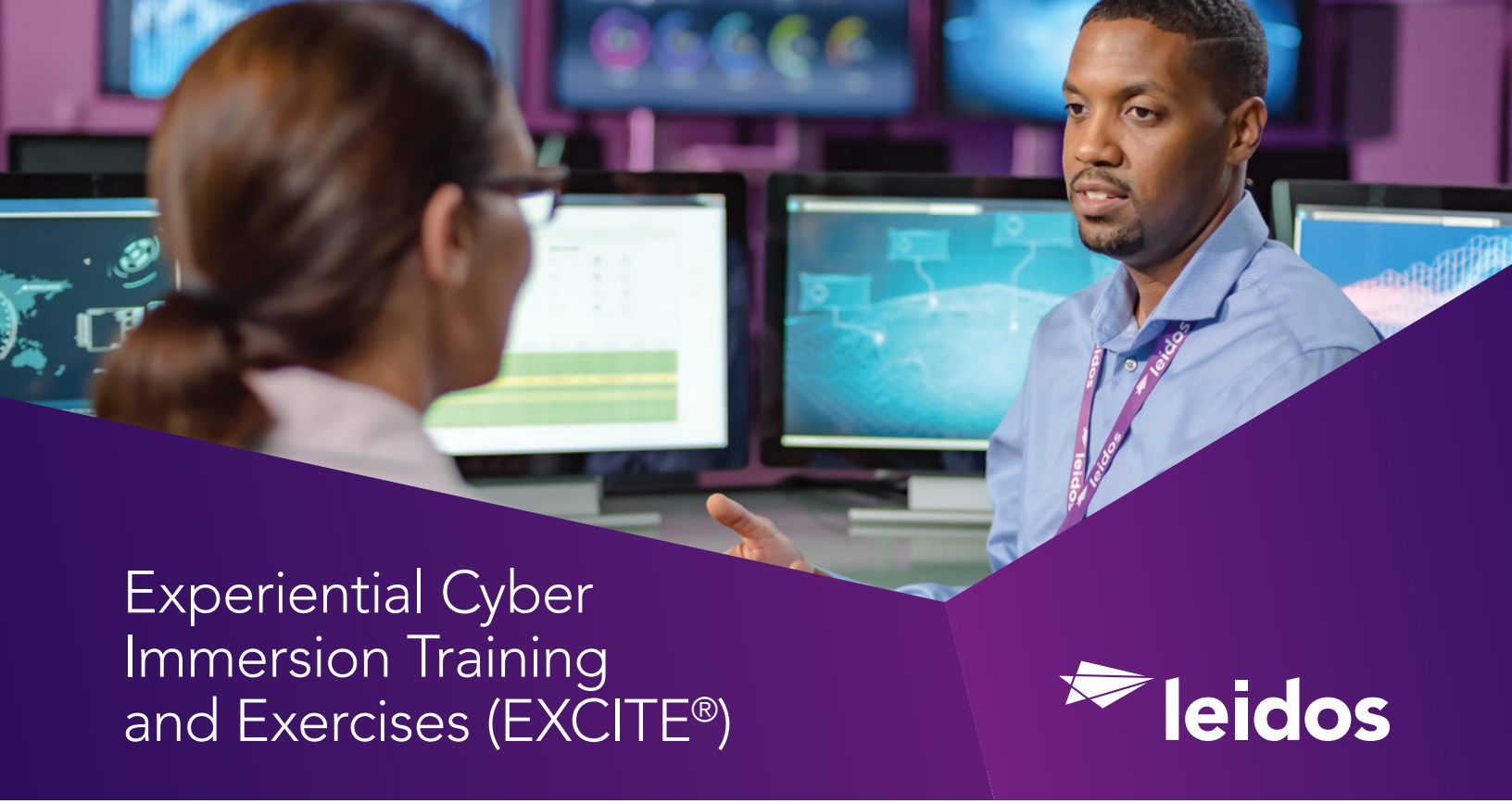

Experiential Cyber Immersion Training and Exercises (EXCITE®)

leidos

Our customers' crucial systems and networks are constantly under cyber-attack. As a global, leading cybersecurity practitioner, every day Leidos helps to safeguard some of the most sensitive information and mission-critical systems in the world.

To help information security professionals proactively remediate and mitigate advanced threats, Leidos developed Experiential Cyber Immersion Training and Exercises — EXCITE. EXCITE is a set of realistic, hands-on exercises that immerse students in the reconstruction and mitigation of a full attack scenario in a lab environment.

- Exercises and simulations based on real-world threats to build familiarity with attacks and mitigations
- Concepts such as defensible architectures, incident response, and forensic analysis
- Encouraging teamwork and collaboration within a challenging and fast-paced environment
- General security concepts to ensure a solid understanding of how to translate skills to their environment

OUR APPROACH

The training consists of a five-day foundational course, which accelerates the development of cybersecurity professionals, and a five-day advanced course, which builds on key technical domains introduced in the foundational course.

The foundational EXCITE course focuses on the skills needed to handle real-world events and threat activities, based on events encountered by the Leidos Cyber Incident Response Team (CIRT). Advanced EXCITE is designed for experienced cyber security analysts and builds on the key technical domains introduced in the foundational course, including Linux commands, networking, and forensics. The course merges sophisticated technical analysis concepts with the kill chain framework to create actionable information on advanced attacker tactics, techniques, and procedures (TTPs).

EXCITE COURSE CURRICULUM

Introduction to Intelligence-Based Cyber Defense (IBCD)

- IBCD & Threat-based DCO Core Concepts
- Linux CLI Data Analysis
- Host-based IR and Forensics
- Network Forensics
- Defensible Enterprise Architectures

Advanced Intelligence-Based Cyber Defense

- IBCD and Threat-based DCO Core Concepts
- Advanced Linux CLI Data Analysis
- Incident Response for APT
- Advanced Network Forensics
- Defensible Enterprise Architectures

Both the foundational and advanced EXCITE courses consist of approximately 50% lecture-based training and 50% hands-on lab exercise, plus additional time for coursework reviews.

In addition, we offer EXCITE Training for Leaders, a two-day course that gives information security leaders an understanding of the advanced persistent threat (APT), the risks it poses, and the unique approach recommended to mitigate it.

WHY PARTNER WITH LEIDOS?

EXCITE trains incident responders and cybersecurity professionals to leverage a consistent, repeatable analysis framework for effective cyber defense, giving our customer organizations an adaptive defense strategy, sustainable threat protection, and mature security posture. EXCITE empowers our customers to meet cyber-attacks head-on with a proactive, intelligence-based cyber defense. It is also a key component of our overall **PACKIT™** (Proven Analytic-Centric Kill-chain Implementation and Transformation) approach to Cyber Security and Defense.

NEXT STEP

Networks and systems will continue to be targeted for attacks from evolving threats. EXCITE can help ensure your information security professionals are prepared. Contact our Leidos EXCITE experts to discuss how we can help you develop an intelligence-based cyber defense for your cybersecurity journey.

FEATURES AND BENEFITS

Through our Leidos-developed and industry-recognized EXCITE training, Tier 1 analysts develop advanced capabilities to comprehensively perform analysis of events and capture the necessary information for deeper level analysis, if required, which is performed by Tier 2 and 3 personnel. This ensures that Tier 2 and 3 analysts focus on more complex events that may pose a greater enterprise risk.

Upon successfully completing the EXCITE course, the student will understand:

- Core Security Intelligence Center (SIC) concepts: Traditional security operations vs. security intelligence, threat-based defensive methodologies, and APTs
- Enterprise security architecture and how each component contributes to security intelligence
- Tools and techniques necessary to efficiently identify trends and extract indicators from large data sources
- Key networking concepts relevant to the security intelligence process
- Key forensics and incident response concepts critical to the security intelligence process

FOR MORE INFORMATION

leidos.com/cyber | leidos.com/contact

Export eTrace record 20510 | 19-0089 | Leidos Creative