EXCITE® 2.0

Experiential Cyber Immersion Training & Exercises®

OUR APPROACH

In a world of constantly evolving threats, the Leidos AI-driven defense solutions are designed to move beyond mere response; they anticipate, adapt and act preemptively. These solutions embody the essence of advanced intelligence, transforming traditional cyber defense into a proactive, resilient and adaptive strategy. As part of our approach, Leidos offers immersive training and real world exercises that are necessary to prepare the cybersecurity workforce. Leidos created and delivers Experiential Cyber Immersion Training and Exercises (EXCITE) to help prepare information security professionals to proactively remediate and mitigate advanced threats. EXCITE 2.0 combines instructor-led training with realistic, hands-on exercises that immerse cyber analysts in the reconstruction and mitigation of full-stack cyberattack scenarios within a lab environment. The EXCITE 2.0 course has been updated for 2025 with more advanced and complex cyberattack scenarios, mimicking today's advanced persistent threat actors (APTs).

Through successful completion of the five-day, in-person EXCITE 2.0 course, the cyber analyst will understand core security intelligence center concepts, enterprise security architecture and how each component contributes to security intelligence, tools and techniques necessary to identify trends and extract indicators from large data sets, key networking concepts relevant to the security intelligence process, and key forensics and incident response concepts critical to the security intelligence process.

Strengthening cyber intelligence and defense through immersive training

EMPOWERING YOUR MISSION

EXCITE 2.0 primes incident responders and cybersecurity professionals to leverage a consistent, repeatable analysis framework for effective cyber defense, supporting our customer organizations in the development of an adaptive defense strategy. EXCITE 2.0 is designed to help our customers meet cyberattacks head-on. It is also a key component in the Leidos PACKITTM (Proven Analytic-Centric Kill-Chain Implementation and Transformation) approach to cybersecurity and defense.

EXCITE 2.0 COURSE MODULES

1. **Security intelligence core concepts:** Understand fundamental differences between traditional IT security operations and security intelligence as well as learn about how advanced persistent threats operate.
2. **Advanced command-line analysis:** Utilize advanced command-line techniques to extract indicators from large datasets.
3. **Host-based incident response and forensics concepts:** Focus on host-based incident response domains specific to APT incidents and dynamic malware analysis techniques.
4. **Network forensics concepts:** Concentrate on key network protocols (DNS, SMTP, encoded/encrypted C2) and analysis of large packet capture.
5. **Defensible enterprise architectures:** Reinforce learning by providing students with hands-on experience and focusing on understanding the implications and impacts of adversary attacks and the potential mitigations upon the enterprise network architecture, with a review of the mitigation matrix.

Our instructors are seasoned cybersecurity practitioners who lead Leidos cybersecurity teams. When they are assigned to lead an EXCITE 2.0 course, they lead teams of eight to 16 through in-person modules and they coach the teams through the technical depth and complexity of the material. The course is taught at a Leidos facility near the customer's student population. It can be taught at a customer site if the network meets the requirements.

Networks and systems will continue to be targeted for attacks from evolving threats. EXCITE 2.0 can help prepare your information security professionals. Contact Leidos EXCITE 2.0 experts to discuss how EXCITE 2.0 can help your organization develop an intelligence-based cyber defense for your cybersecurity journey.

FOR MORE INFORMATION

defensivecyber@leidos.com | leidos.com/cyber