SEC564: **Red Team Exercises and Adversary Emulation**

2 Day Course	12 CPEs	Laptop Required

You Will Be Able To

- Build a Red Team program
- Leverage Red Team exercises and adversary emulations to obtain a holistic view of an organization's security posture
- Measure, train, and improve people, processes, and technology for the organization

"Real-world red teaming is so much different from what people assume, and SEC564 delivers reality. Amazing course!"

— Shyaam Sundhar Rajamadam Srinivasan, **Digitonto LLC**

"SEC564 provides a way to 'measure' red team maturity."

— Robert Lee Smith, **Intel Corporation**

In SEC564, you will learn how to plan and execute an end-to-end adversary emulation, including how to plan and build a red team program, leverage threat intelligence to map against adversary tactic, techniques, and procedures (TTPs), emulate those TTPs, report and analyze the results of red team exercises, and ultimately improve the overall security posture of the organization.

You will do all of this in a course-long exercise, in which we perform an adversary emulation against a target organization modeled on an enterprise environment. This environment includes Active Directory, email, web, and file servers, as well as endpoints running the latest operating systems. We will start by consuming cyber threat intelligence to identify and document an adversary that has the intent, opportunity, and capability to attack the target organization. You will discover the TTPs used by the adversary while creating an adversary emulation plan leveraging MITRE ATT&CK (Adversary Tactics, Techniques, and Common Knowledge).

We'll cover the planning phase of these exercises, showcasing various industry frameworks and methodologies for red teaming and adversary emulation. These frameworks are industry standards used by various regulatory bodies to ensure consistent and repeatable red team exercises.

Using strong planning and threat intelligence, students will follow the same unified kill chain as the adversaries to reach the same objective, from setting up attack infrastructure with command and control to emulating multiple TTPs mapped to MITRE ATT&CK.

The course concludes with exercise closure activities such as analyzing the response of the blue team (people and process), reporting, and remediation planning and retesting. Finally, you will learn how to show the value that red team exercises and adversary emulations bring to an organization. The main job of a red team is to make a blue team better. Offense informs defense and defense informs offense.

Author Statement

"Organizations are maturing their security testing programs to include Red Team exercises and adversary emulations. These exercises provide a holistic view of an organization's security posture by emulating a realistic adversary to test security assumptions, measure the effectiveness of people, processes, and technology, and improve detection and prevention controls. This course will teach you to plan Red Team exercises, leverage threat intelligence to map against adversary tactics, techniques, and procedures, build a Red Team program and plan, execute a Red Team exercise and report and analyze the results, and improve the overall security posture of the organization."

— Jorge Orchilles

Section Descriptions

SECTION 1: Introduction and Planning of Red Team Exercises

Section 1 begins by introducing Red Team exercises and adversary emulations, showing how they differ from other security testing types such as vulnerability assessments, penetration tests, and purple teaming. Following the hybrid approach of the course, you will be introduced to a number of industry frameworks (including the Cyber Kill Chain, Unified Kill Chain, and MITRE ATT&CK) for Red Team exercises and adversary emulations. Threat Intelligence is critical to performing Red Team exercises and will be covered early in the course. A red teamer needs to know how to obtain and consume threat intelligence in order to successfully emulate an adversary. Red Team exercises require substantial planning, and you will learn what triggers an exercise and how to define objectives and scope, set up attack infrastructure, understand roles and responsibilities (including those of the Trusted Agents, be they White Team or Cell), and establish the rules of engagement. With a strong plan in place, the exercise execution phase begins. You will learn how to perform the steps to emulate an adversary and carry out a high-value Red Team exercise. We will cover reconnaissance, social engineering, weaponization, and delivery. Section 1 concludes with a lab testing your payload and attack infrastructure.

TOPICS: About the Course; Defining Terms; Motivation and Introduction; Frameworks and Methodologies; Threat Intelligence; Planning; Red Team Exercise Execution

SECTION 2: Red Team Exercise Execution and Closure

Section 2 continues with executing a Red Team exercise and wraps up with closure activities. The section is filled with exercises that walk students through the course-long Adversary Emulation Red Team Exercise. Multiple Red Team exercise phases are explored that use realistic TTPs to ultimately meet the emulated adversary objective. During the exercises, you gain initial access, perform discovery of the target network from patient zero, attempt privilege escalation, create advanced command-and-control channels, and establish persistence. These exercises reinforce the lecture portion of the course. You will learn various methods covering defensive evasion and execution, access to credentials, and lateral movement and pivoting techniques. You'll then use those skills in exercises to obtain the emulated adversary's objective. Lastly, you will complete the exercise by performing various closure activities.

TOPICS: Red Team Exercise Execution; Exercise Closure

Who Should Attend

- Security professionals interested in expanding their knowledge of Red Team exercises in order to understand how they are different from other types of security testing
- Penetration testers and Red Team members looking to better understand their craft
- Blue Team members, defenders, and forensic specialists looking to better understand how Red Team exercises can improve their ability to defend by better understanding offensive methodologies, tools, tactics, techniques, and procedures
- Auditors who need to build deeper technical skills and/or meet regulatory requirements
- Information security managers who need to incorporate or participate in high-value Red Team exercises

"SEC564 is perfect for penetration testers looking to move to red teams."

— Tim Maletic, **D & B**

"For a lot of companies, red teaming is a new approach, and therefore training in that field is really necessary."

— Andreas Hinosaar, **Estonian MOD**