SEC598: **Security Automation for Offense, Defense, and Cloud**

6	36	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Understand the security issues that most organizations are facing today
- Translate security issues into smaller problems, define automated solutions for those specific problems, and then fully chain features that can be used to tackle multiple issues in an automated manner
- Use tools like Terraform, Ansible, CHEF Puppet, and many more to locally automate secure configurations, set a desired-state configuration, deploy infrastructure as code in different environments, and detect and respond to security incidents in an automated manner
- Evaluate real-world scenarios within a combination of on-premise and cloud environments using a reference framework that can be immediately used and implemented in your organization

Author Statement

I started my career as a security engineer and was always interested in learning more about offensive security and how to implement certain defense mechanisms in response, especially from the perspective of the technology used. I quickly became aware that a structured solution was required to reduce the overall security risk exposure for the organizations I was working with.

Over the past years I have seen that automation and orchestration can maximize the value of current security operations centers. Many of these organizations have the same challenges: hunting for talent, supporting an ever-increasing technology landscape, and how to reduce the time to handle and respond to incidents.

I am very excited to release SEC598, which is purely focused on automation, and I am convinced that SEC598 gives you an in-depth understanding of automation concepts, technologies and how to apply them for offense and defense. This course was created together with SANS ISC handlers, providing a unique mix of offensive and defensive skills.

—Jeroen Vandeleur

Our virtual organization, GLOBEX, is struggling with typical cybersecurity challenges. The organization is growing, moving towards multiple cloud environments, and supporting continuous deployment. You just got hired as a security expert and your manager tells you that our environment is increasingly complex and we are facing more and more cyber threats. We need you to focus on and improve our core security services with a limited security team.

SEC598: Security Automation for Offense, Defense, and Cloud will equip you with the expertise to apply automated solutions to prevent, detect, and respond to security incidents. The cybersecurity skill gap continues to push organizations to adopt automation to deal with security operations, so most automation training focuses exclusively on DevSecOps and automation tools/scripting. SEC598 takes another approach: students first train to understand the concept of automation, then learn how existing technologies can be best leveraged to build automation stories that translate repeatable problems to automated scripts.

SEC598 gives students real-world examples of how to automate tasks within complex environments. The course features more than 15 labs plus a capstone exercise where students develop automation stories to attack and defend a simulated organization. The six-part course starts with an introduction to security automation, describing concepts such as infrastructure as code, configuration management tooling, emulations, and playbook development. Students will then apply these concepts starting with the engineering process within hybrid environments. You will learn how to use different technologies to assess, deploy, and monitor environments, combining configuration management tools, infrastructure as code, security orchestration, automation and response (SOAR) engines, and cloud native services for automation. You will then learn how to use this automation specifically for offense and defensive by looking at certain techniques being used to emulate adversaries and automate security testing.

You will see how infrastructure as code enables red teamers to become more efficient and stealthier before we turn to a discussion of how certain defense techniques can be automated. There is no other training that offers such a comprehensive understanding and application of security automation to the spectrum of cyber security teams.

You Will Learn

- Prevention, detection, and response for specific attack techniques used by real-world adversaries and penetration testers
- Offensive and defensive perspectives of these attack techniques through hands-on exercises
- How to translate repeatable activities into automated tasks
- How to improve the efficiency and effectiveness of a security operations team
- Cloud security automation in AWS and Azure
- Where to apply security automation and how to properly engineer your environment for automation
- The power of leveraging automation in purple team exercises

Section Descriptions

SECTION 1: Security Automation Concepts

Section 1 lays the foundation for the remainder of the course by explaining overall security automation concepts and how they can be used within different environments and technology stacks. Concepts to be discussed include automation triggers, desired state configuration and security automation, and SOAR.

TOPICS: Course Outline and Lab Setup; Security Architecture and Configuration; Security Automation Fundamentals

SECTION 2: Security Automation Engineering

Section 2 focuses on security task automation in your infrastructure and explains how security automation can be engineered with built-in scripting and configuration management tooling. We will analyze how PowerShell can be used for desired state configuration to detect and respond to system misconfigurations. We will also look at what you can achieve with infrastructure as code tooling and a variety of SOAR tools. Finally, we will discuss playbook design and development for automated incident handling and mitigation techniques.

TOPICS: Automating Security Hardening; PowerShell Basics; Configuration Management Tooling; Security Orchestration and Automation; Security Automation with Python; Security Orchestration Tools; SOAR Playbooks; Automated Security Controls; Automating Security Compliance; Automating Security Hardening; Introduction to Cloud Environments; Cloud 101

SECTION 3: Security Automation in the Cloud

Sections 1 and 2 covered security automation based largely on on-premise technology stacks, so in Section 3 we will move towards cloud native automation tooling. Attendees will gain an in-depth understanding of cloud native technologies used for security automation. We will zoom into blueprinting, compliance validation, and automated remediation by using real-world examples of cloud misconfigurations.

TOPICS: Introduction to the Cloud; Microsoft Azure Automation; AWS Automation; Bringing It All Together

SECTION 3: Offensive Security Automation

In Section 4, we will use the automation techniques we learned in previous sections for offensive security automation activities. This section presents examples on how to automate offensive techniques used by real-world adversaries and goes on to explain how chaining attack techniques can be used to emulate these adversaries.

TOPICS: Introduction; Automating Offensive Security Testing; Emulating Real-World Cyber Attacks; Chaining Techniques and Automating Adversaries; Organizing Chaos; Offensive Security in the Cloud

SECTION 5: Defensive Security Automation

Section 5 focuses on defensive security controls and how we use automation to prevent, detect, and respond to security incidents. Students will gain an in-depth understanding of how attacks can be detected and how to enrich incidents to minimize false positives and automatically trigger responses.

SECTION 6: Security Automation Capstone

The final course section is a capstone event where students can apply and reinforce all the skills they've learned in a friendly, competitive environment. The capstone is a full day of challenging hands-on work applying the principles taught throughout the course. Your team will progress through multiple levels and missions designed to ensure the presence of detection and defensive capabilities.

TOPICS: Applying Previously Covered Security Controls In-Depth; Applying and Fine-Tuning Detection Capabilities and Using Automation to Reduce the False Positive Ratio; Configuration Management Tools; Infrastructure as Code Templates; XSOAR Playbook Development; AWS Configuration Rules and ARM Templates

Who Should Attend

This course will be helpful to anyone in the cybersecurity and information security industry looking at how to automate certain security tasks and identify those that cannot be automated. Basically, this involves any industry including retail, finance, medical, healthcare, and government affected by nation-state attackers, APT, ransomware, or other threats. Job roles that can benefit from SEC598 include:

- Security Architects
- Security Engineers
- Incident Responders
- Enterprise Risk Analysts
- Ethical Hackers
- Penetration Testers
- Red Team Members
- Blue Team Members
- Purple Team Members
- Security Operations Center Analysts
- Cloud Engineers