SEC557: **Continuous Automation for Enterprise and Cloud Compliance**

3 Day Course	18 CPEs	Laptop Required

You Will Be Able To

- Turn policies and management requirements into visually presented security metrics
- Reduce the time and effort required to gather and report on security and compliance data
- Measure security and compliance in cloud and traditional infrastructure
- Use PowerShell scripts and command-line tools to extract relevant data from cloud services
- Gather information from web APIs and security tools
- Extract information about virtualization infrastructure
- Query data from fleets of heterogenous systems
- Monitor servers and endpoints for proper configuration
- Work with data formats commonly used by security tools, DevOps pipelines, and cloud services
- Build tactical visual reports for use by operations staff and management
- Manage and load time-series databases for tracking metrics over time
- Build strategic dashboards for security and compliance

Using Cloud Security and DevOps Tools to Measure Security and Compliance

Agile development, DevOps, cloud technologies, and virtualization have enabled organizations to build and deploy systems at a terrifyingly fast rate. The old and cumbersome manual ways to test security and compliance can't keep up. You need to understand and use the same tools and techniques that your developers and engineers are using, and you need to be able to generate results quickly and often - without slowing down your organization.

SEC557 uses the ELVis (Extract, Load, and VISualize) technique to help you gather and present useful security and compliance information to your organization. Students will learn how to use PowerShell scripting and automated tools to gather measurements from cloud service providers, operating systems, Active Directory, security tools, web APIs, and datacenter infrastructure. For some data, you'll prepare tactical visualizations on the fly by building spreadsheets, pivot tables, and graphs using scripts. Then import your data into the Graphite time-series database for strategic analysis and reporting. You'll also build Grafana dashboards for use by management, security, compliance, and operations staff.

Author Statement

"When I started performing IT and security audits in the 1990s, it was reasonable to ask during an annual engagement 'What has changed since the last time I was here?' My clients could point out physical servers in the data center and tell me what functions were performed by each. We could work for weeks on a software audit without slowing down the development.

"Then came virtualization, agile development, microservices, the cloud, and DevOps. The old ways of measuring security and compliance aren't fast enough for the modern enterprise. SEC557 answers the question 'How can the manager/auditor/security/compliance professional possibly keep up?' It teaches you to leverage and integrate with the processes used by your developers and engineers so that you can enforce security and compliance requirements without becoming an obstacle."

— Clay Risenhoover

Section Descriptions

SECTION 1: Scripting, Data Acquisition, and Visualization Tools

Section 1 begins with a discussion of the special problems faced by audit, security, and compliance professionals in the age of Agile, Cloud, and DevOps. We explore some of the technologies that organizations are using to embrace higher-velocity IT delivery and how to work with those technologies to increase our own speed. We introduce the SEC557 ELVis (Extract, Load, VISualize) technique. Then, we get to work using PowerShell to gather and manipulate data. We move from basic commands to techniques to quickly process large data sets and then format the output to be used in other tools or easily consumed by the people tasked with securing our enterprise. At the end of the section, we load data into a time-series database and build our first dashboards.

TOPICS: Security, audit, and compliance in a fast-moving world; PowerShell ecosystem; PowerShell commands and scripting; Using .NET objects in PowerShell; Working with common data formats; Building tactical reports directly from acquired data using pivot tables and graphs; Working with time-series databases; Working with dashboard software

SECTION 2: Acquiring and Visualizing Cloud Service Data

Section 2 focuses on helping the organization safely use cloud services. We discuss shared responsibility models and how the enterprise should operate securely in the cloud. We then explore a combination of native and third-party tools that can be automated to measure and report on the security of cloud-based systems.

TOPICS: Shared responsibility models; Identity and access management (IAM); Multi-factor authentication; Logging in the cloud; Monitoring access and changes to cloud resources; Network configuration checks; Automated VM assessment tools; Ensuring security at deploy time

SECTION 3: Acquiring and Visualizing Data from OSes, Virtualization, and Containers

In Section 3, we cover how to extract and report on data from operating systems, datacenter infrastructure, and container technologies. We begin the course section looking at techniques to get data from individual Windows system and Active Directory domains and forests. Then we examine Linux/Unix systems to see how to gather measurements from them as well. Next, we explore how to use OSQuery to retrieve useful information from a wide variety of operating systems, and we add in fleet management software to allow us to query these systems at scale. We end the section with a discussion of how to measure security and compliance of container systems like Docker.

TOPICS: Gathering configuration and security information from Windows systems with PowerShell; Querying Active Directory with PowerShell; Querying Linux and Unix systems with PowerShell and native tools; Using OSQuery to monitor systems; Using Fleet to manage large numbers of heterogenous systems; Securing the Docker ecosystem

Lab Information

SEC557 focuses very heavily on hands-on activities, with as much as 50% of your day being spent at the keyboard. Lab activities for the course include:

- Introduction to PowerShell
- Using .NET objects in PowerShell
- PowerShell date/time handling
- Working with common data input/output formats: JSON, XML, CSV, HTML, spreadsheets
- Data acquisition from Web APIs: REST and SOAP
- Building Excel spreadsheets, pivot tables, and graphs with code
- Configuring the Graphite time-series database (TSDB)
- Importing data into Graphite
- Managing data sources and building dashboards with Grafana
- Extracting data from the Amazon Web Services (AWS) Command Line Interface (CLI)
- Acquiring data from AWS security tools
- Acquiring data from OSQuery/Fleet
- Acquiring data from VMWare infrastructure

Who Should Attend

- IT operations managers
- Security managers
- Risk and compliance auditors
- Security auditors
- Security engineers
- Security analysts
- System administrators