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

5 Day Program	30 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

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

Measure what matters, not what's easy.

Students learn how to measure and visualize security data using the same tools that developers and engineers are using, as well as how to extract, load, and visualize data from cloud services, on-premise systems, and security tools. The course includes PowerShell scripting, automation, time-series databases, dashboard software, and even spreadsheets to present management with the strategic information it needs and to facilitate the work of your operations staff with sound tactical data.

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.

Key Takeaways

- Measure and report on compliance across the enterprise
- Visualize data for rapid absorption and decision making
- Supply appropriate data at the tactical and strategic levels
- Turn management requirements into actionable data
- Use the tools you already own to report on compliance

Hands-on Training

SEC557 focuses very heavily on hands-on activities, with as much as 50% of your day being spent at the keyboard. Students gather compliance data from remote AWS and Azure lab environments and from common on-premise systems, including Windows, Linux and VMWare hosts. Tools used to extract data include PowerShell, Pester, Inspec, SOAP and REST APIs, FleetDM, OSQuery, PowerCLI and Bash commands. Measurement data is loaded into a Graphite time-series database (TSDB), and then visualized in multiple Grafana dashboards. Lab activities for the course include:

- **SECTION 1:** PowerShell fundamentals, Working with the .NET framework, Reading and writing JSON, XML, HTML, and CSV data, Using spreadsheets as data sources and as visualization tools, Configuring Graphite and loading data, Adding Grafana data sources and building dashboards
- **Section 2:** Consuming web APIs, Verifying Docker security, Using static analysis tools for security testing, Gathering inventory information using the AWS CLI, Assessing identity and access management (IAM) roles and user settings, Verifying AWS security settings, Validating the security of infrastructure as code deployments
- **Section 3:** Querying Windows settings, Extracting data from Active Directory, Compliance testing with Pester, VMware infrastructure testing, Querying Linux/Unix, Monitoring patch velocity on Windows and Unix systems
- **Section 4:** Gathering inventory information using the AWS CLI and PowerShell, Assessing IAM roles and user settings, Verifying logging settings, Checking for proper resource access control, Auditing network security settings, Validating security of infrastructure as code deployments
- **Section 5:** Azure benchmark compliance, Azure AD measurement, Verifying Docker security, Static analysis tools, Alternative visualization tools: ImportExcel XYZ

Section Descriptions

SECTION 1: PowerShell Fundamentals, Time-Series Databases 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 the need for automation in compliance measurement and how to "live off the land" by using ubiquitous tools which are managed by other teams. We discuss the various sources of compliance data in the modern enterprise and examine how to visualize data for use by management and operations staff. We introduce the SEC557 ELVis (Extract, Load, VISualize) technique and using PowerShell as a tool for gathering and examining compliance-related data. At the end of the section, we cover the care and feeding of time-series databases and dashboard tools, ending with importing our first data and visualizing it.

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: Advanced PowerShell Scripting and Automation, Gathering and Using Structured Data

Section 2 builds on the previous section, extending the student's PowerShell skill set by adding techniques for dealing with structured data. We use live REST and SOAP APIs to extract, load and visualize structured data formats which include JSON, XML, CSV and even spreadsheets and HTML. We explore options for password and secrets management in PowerShell. We introduce advanced PowerShell script and function development and how to reuse code across projects and systems. We also explore how to automate our scripts in Windows, Unix and continuous integration environments.

TOPICS: Handling structured data: JSON, XML, CSV, HTML, XLSX; Interacting with REST and SOAP APIs; Authenticated access to APIs; Retrieving and processing large datasets with PowerShell; Creating PowerShell scripts and functions; Secrets and credential handling in PowerShell

Who Should Attend

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

SECTION 3: System and Infrastructure Compliance Measurements

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 also explore the use of relational databases for storing compliance data and the use types of visualizations available for tabular data.

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; Using Relational Databases for Storing Compliance Data

SECTION 4: Cloud Compliance: AWS

Section 4 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 which can be automated to measure and report on the security of cloud-based systems, with a focus on AWS.

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

SECTION 5: Cloud Compliance: Azure/GCP, DevOps Compliance

Section 5 extends the cloud compliance discussion to include the Azure and Google Cloud platforms. We discuss the specifics of ensuring compliance with standards in each environment and explore the use of tools to measure compliance. We cover some technologies which are commonly used in DevOps environments and the benchmarking and static analysis tools which work with infrastructure as code and containers. We end the day by exploring other visualization techniques which can be helpful for tactical and operational measurements.

TOPICS: Compliance in Azure; Compliance in GCP; DevOps Concepts; Container Concepts; Securing the Container Ecosystem; Ensuring Security at Deploy Time

"The content in this course is helping me understand the importance of scripting, data acquisition, and data automation. I think this course is a must for anyone looking to understand the importance of these topics."

—Robert Hymus, **Here Corp**

"The timing of the industry and the needs / demands are major reasons why one should take this class, as it relates to compliance, cyber audits, and supports senior management initiatives."

—Diane D, **U.S. Government**