SEC566: Implementing and Auditing Security Frameworks and Controls

GCCC Critical Controls
giac.org/gccc

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organizations' important information and systems
- Understand the importance of each control and how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
- Identify and utilize tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of security controls
- Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- Audit each of the Critical Security Controls, with specific, proven templates, checklists, and scripts provided to facilitate the audit process

Notice to Students

The CIS released version 8 of the Controls in May 2021. This course content is updated to reflect the changes in the CIS Controls, as well as the most recent versions of the NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC).

Building and Auditing Critical Security Controls

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches?

In addition to defending their information systems, many organizations have to comply with a number of cybersecurity standards and requirements as a prerequisite for doing business. Dozens of cybersecurity standards exist throughout the world and most organizations must comply with more than one such standard. Is your organization prepared to comply and remain in compliance?

In February of 2016, then California Attorney General, Vice President Kamala Harris stated that "the 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

The Center for Internet Security (CIS) Critical Controls are specific security controls that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

As threats and attack surfaces change and evolve, an organization's security should as well. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the CIS Critical Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the CIS Critical Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by international governments, the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

SEC566 will enable you to master the specific and proven techniques and tools needed to implement and audit Version 8 of the CIS Controls as documented by the Center for Internet Security (CIS), as well as those defined by NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC). Students will learn how to merge these various standards into a cohesive strategy to defend their organization and comply with industry standards.

SANS' in-depth, hands-on training will teach security practitioners to understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats. SEC566 shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, this course is the best way to understand how you will measure whether the Controls and other standards are effectively implemented.

"Loved this course. It provides a method of measuring your security posture and applying the concept to any organization."

—John M., **U.S. Military**

Section Descriptions

SECTION 1: Introduction and Overview of the CIS Critical Controls

Students will learn the background and context for the CIS Controls v8 as well as the NIST SP 800-171 and Cybersecurity Maturity Model Certification (CMMC). These standards, or control frameworks organize and influence cybersecurity practices. These controls or safeguards are organized into defensive domains. To understand how these defensive domains interact, students need to first understand building blocks of a cyber security program including the importance of a governance foundation and how to streamline control implementation across multiple frameworks. We will establish a baseline knowledge of key terms used in the defensive domains.

TOPICS: Understanding the CIS Critical Controls; Understanding NIST SP 800-171 and CMMC; Understanding the Collective Control Catalog; Establishing the Governance Foundation of a Security Program; CIS Control #1: Inventory and Control of Enterprise Assets

SECTION 2: Data Protection, Identity and Authentication, Access Control Management, Audit Log Management

During Section 2, the course will begin to cover the defensive domains of data protection, identification and authentication, and access control management., and audit and accountability. Students will learn how identity and access control promote data protection and they will also learn the importance of audit log management.

TOPICS: CIS Control #3: Data Protection; CIS Control #5: Account Management; CIS Control #6: Access Control Management; CIS Control #8: Audit Log Management

SECTION 3: Server, Workstation, and Network Device Protections – Part 1

During Section 3 , the course will cover the defensive domains of configuration management, system and software integrity, vulnerability management, and physical protection.

TOPICS: CIS Control #2: Inventory and Control of Software Assets; CIS Control #7: Continuous Vulnerability Management; CIS Control #4: Secure Configuration of Enterprise Assets and Software; Physical Security Controls (800-171 & CMMC)

SECTION 4: Server, Workstation, and Network Device Protections – Part 2

During Section 4, the course will cover the defensive domains of system integrity, system and communications protection, configuration management, and media protection.

TOPICS: CIS Control #9: Email and Web Browser Protections; CIS Control #10: Malware Defenses; CIS Control #11: Data Recovery; CIS Control #12: Network Infrastructure Management; CIS Control #13: Network Monitoring and Defense

SECTION 5: Governance and Operational Security

During Section 5 of the course, we will cover the defensive domains of security awareness , service provider management, application development security, incident management, and penetration testing.

TOPICS: CIS Control #14: Security Awareness and Skills Training; CIS Control #15: Service Provider Management; CIS Control #16: Application Software Security; CIS Control #17: Incident Response Management; CIS Control #18: Penetration Testing

"This course is providing me with the necessary context to understand the Critical Security Controls in depth, and further helping me understand how to present recommendations to our business owners."

— Chris Harper, **Centrus Energy**

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel and contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC440, MGT516, MGT551, MGT512, SEC401, and SEC501

GCCC
Critical Controls
giac.org/gccc

GIAC Critical Controls Certification

The GIAC Critical Controls Certification is the only certification based on the Critical Security Controls, a prioritized, risk-based approach to security. This certification ensures that candidates have the knowledge and skills to implement and execute the Critical Security Controls recommended by the Council on Cybersecurity, and perform audits based on the standard.

- Background, purpose, and implementation of the CIS Critical Controls
- Account monitoring, application software security, boundary defense, and controlled use of administrative privileges and need-to-know access
- Data protection and data recovery capability; email and web browser protections; inventory and control of hardware and software assets; and limitation and control of network ports
- Maintenance, monitoring, and analysis of audit logs; secure configurations for hardware, software, and network devices; and wireless access control