SEC366: **CIS Implementation Group 1**

1 Day Course	6 CPEs	Laptop Required

You Will Be Able To

- Apply initial security controls based on actual threats that are measurable, scalable, and reliable in stopping known attacks and protecting your organization's important information and systems
- Understand the importance of each CIS IG1 control and how it is compromised if ignored
- Explain the defensive goals that result in quick wins and increased visibility of network and systems
- Identify and use tools that implement controls through automation

Who Should Attend

- CIS Implementation Group 1 is geared towards small to medium-sized organizations which have limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. Examples of such customers are State, Local, and Tribal Governments, U.S. School Districts, U.S. Federal Circuit Courts, Managed Service Provider Consortiums, and non-profits.
- Technical non-security employees who have been tasked with managing security for their SMB

Business Takeaways

- Efficiently reduce the most important cyber-related risks
- Align compliance requirements with security and business goals and solutions
- Report the status of cybersecurity defense efforts to senior leadership in clear, business terms

The prioritization of CIS IG1 is particularly useful to small and mid-size organizations who lack full blown cybersecurity teams yet need basic protections in place. IG1 is the on-ramp to the CIS Controls and consists of a foundational set of 56 cyber defense Safeguards. The Safeguards included in IG1 are what every enterprise should apply to defend against the most common attacks.

IG1 is designed to protect low level sensitive data that principally surrounds employee and financial information. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

This targeted, hands-on training on CIS Controls Implementation Group 1 (IG1) teaches security practitioners not only how to defend against threats but also the reasoning behind these measures and how to future-proof defenses against emerging threats. SEC366 demonstrates how to implement the CIS Controls through cost-effective automation, making it an essential course for to measure and improve the effectiveness of cybersecurity controls in all organizations.

What is CIS Implementation Group 1?

CIS Implementation Group 1 is the most basic set of essential cyber hygiene controls that represent a minimum standard of information security necessary for every organization.

Author Statement

"The modern threat landscape is increasingly complex, and deciding which steps to take next in defending against these threats can be overwhelming, especially with the vast range of technologies and tools available. Adding to the challenge, organizations must also comply with various regulatory frameworks. This raises critical questions: Are we taking the right actions to protect our organization? What should be prioritized next?

"In SEC366: CIS Critical Security Controls IG1, we focus on answering these questions by guiding you through the implementation of Implementation Group 1 (IG1) controls. IG1 is designed specifically for organizations with limited cybersecurity resources, offering a targeted set of foundational safeguards that address the most common and impactful attacks occurring today, as well as anticipated future threats. This course will help you establish a strong security foundation by implementing these essential controls, which are both practical and effective.

"Students will not only learn how to align and map the CIS Controls to their organization's compliance and framework requirements but also how to measure control implementation and effectiveness. With the knowledge gained, you'll be able to communicate progress and risk reduction to leadership, ensuring your cybersecurity efforts are both strategic and measurable. This hands-on course equips you with the tools needed to confidently start your security program and continually assess and improve it over time."

—Brian Ventura

Section Description

SECTION 1: CIS Implementation Group 1

CIS Implementation Group 1 addresses the core functional areas of Govern, Identify, Protect, Detect, Respond and Recover. SEC366 supports the knowledge and skills to effectively understand, implement, and report on the CIS Controls Implementation Group 1, the highest priority controls for organizations of all size to implement.

TOPICS: CIS Resources; Govern; Identify; Protect/Detect; Measurement and Reporting