Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. In addition to defending their information systems, many organizations find themselves responsible for being compliant with a number of cybersecurity standards and requirements as a prerequisite for doing business. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches?

In February of 2016, then California Attorney General, Vice President Kamala Harris recommended 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 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.

This course helps you master specific, proven techniques and tools needed to implement and audit the CIS Controls v8 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 for defending their organization and being compliant 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.

“SEC566 provides great tools, explanation, and insight!”

— Ryan LeVan, Trex Company, Inc.
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