THE RIGHT CONNECTION
CENIC 2026

CIS Workshop

Sunday, March 29, 2026
1:30 PM to 4:30 PM

**Please check in at the registration table before the workshop begins. Thank you.*

Workshop Summary

This two-part hands-on workshop will introduce attendees to the Center for Internet Security's CIS Critical Security Controls and CIS Benchmarks, a set of globally recognized best practices and tools for securing IT systems and data.

The first part of the workshop will introduce you to the CIS Critical Security Controls themselves as well as the CIS Controls Navigator and the CIS Controls Self Assessment Tool (CIS CSAT), which can help you map the Critical Security Controls to other security standards and automate the tracking and prioritization of your implementation of the CIS Controls, respectively.

The second part of the workshop will introduce you to the CIS Benchmarks, which consist of over 100 community-developed secure configuration recommendations for more than 25 vendor product families. These Benchmarks map directly to the CIS Critical Security Controls and are designed to harden organizations' technologies against cyberattacks.

Welcome & Introductions: 1:30 PM to 1:45 PM
Part 1: 1:45 PM to 2:45 PM

Framework Overload to Oversight: Regaining Control with the CIS Controls

Charity Otwell, Director of Critical Security Controls

Have you ever felt overwhelmed by the endless cycle of control implementation and audits? Whether you are working with one framework or juggling several, the process can quickly become a mountain of evidence requests, tight deadlines, and endless follow-ups. At the center of it all is one word: control.

In this session, we'll focus on a specific set of controls—the CIS Critical Security Controls, a prioritized, prescriptive, and simplified set of best practices designed to help organizations build a stronger cybersecurity foundation. By adopting the CIS Controls, organizations not only improve their security posture but also move closer to alignment with major compliance frameworks such as NIST 800-53, ISO 27001, PCI DSS, HIPAA, and others.

What you will learn

1. How to use the CIS Controls Navigator interactive tool that shows you how a single control fulfills requirements for over 25 different frameworks.
2. How to replace your spreadsheets with the CIS CSAT (Self Assessment Tool) and track progress, assign tasks, keep score, and generate reports.

Takeaway

Learn a methodology that lets you assess once and report to many in an automated, familiar way for assessors.

Break: 2:45 PM to 3:00 PM
Part 2: 3:00 PM to 4:30 PM

CIS Benchmarks: Building a Strong Foundation for Secure Configurations

Phil White, Director of Benchmarks

In today's evolving threat landscape, secure system configurations are critical to protecting infrastructure. The Center for Internet Security (CIS) Benchmarks provide prescriptive, consensus-driven guidance in both human-readable and machine-readable formats to help organizations harden a wide range of technologies.

Developed and maintained by a global community of cybersecurity experts, CIS Benchmarks are living standards that evolve in response to emerging threats and best practices. In this session, you'll discover what CIS Benchmarks are, how they are created, and why they are essential for any cybersecurity program. We'll explore the structure of a Benchmark, practical implementation strategies, and how these standards align with other security frameworks.

You'll also learn about the power of the CIS community and how you can contribute to shaping future guidance. To bring it all together, we'll demonstrate CIS-CAT Assessor Pro, a tool that automates compliance checks against multiple CIS Benchmarks. Whether you're new to CIS Benchmarks or a seasoned user, you'll leave with actionable insights to strengthen your security posture and engage with a global network of experts.

What you will learn

1. How to use CIS Benchmarks to harden systems to the appropriate profile level.
2. How to determine what profile is correct for you.
3. What products and technologies the CIS Benchmarks support.
4. How to execute the CIS benchmarks in your environment.
5. What kind of reporting and remediation guidance is provided.
6. What kind of artifacts will be produced for evidence.

Takeaway

CIS Benchmarks provides a well-supported, widely recognized solution for hardening operating systems, cloud environments, and network devices.

Please reach out with any questions to:

Charity Otwell, Director of Critical Security Controls, CIS: controlsinfo@cisecurity.org
Phil White, Director of Benchmarks, CIS: phil.white@cisecurity.org

David Han, Cybersecurity Engineer, CENIC: dhan@cenic.org
Philip Romero, Manager, Information Security Office, CENIC: promer@cenic.org

Sign up in advance using this form: https://forms.gle/UqETiauSmTNLQrQh8