Final Day to Choose Your Favorite Special Offer with OnDemand Training (https://www.sans.org/ondemand/specials?msc=OAB)

CIS Critical Security Controls

The CIS Critical Security Controls for Effective Cyber Defense

The CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principal benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results. The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners. They were created by the people who know how attacks work - NSA Red and Blue teams, the US Department of Energy nuclear energy labs, law enforcement organizations and some of the nation's top forensics and incident response organizations - to answer the question, "what do we need to do to stop known attacks." That group of experts reached consensus and today we have the most current Controls. The key to the continued value is that the Controls are updated based on new attacks that are identified and analyzed by groups from Verizon to Symantec so the Controls can stop or mitigate those attacks.

The Controls take the best-in-class threat data and transform it into actionable guidance to improve individual and collective security in cyberspace. Too often in cybersecurity, it seems the "bad guys" are better organized and collaborate more closely than the "good guys." The Controls provide a means to turn that around.

SANS Supports the CIS Critical Security Controls with Training, Research and What Works

To support information security practitioners and managers implement the CIS Critical Security Controls, SANS provide a number of resources and information security courses.

Critical Security Controls Courses

- SEC440: Critical Security Controls: Planning, Implementing and Auditing (https://www.sans.org/course/critical-security-controls-planning-implementing-auditing?msc=cishp)
- SEC566: Implementing and Auditing the Critical Security Controls - In-Depth (https://www.sans.org/course/implementing-auditing-critical-security-controls?msc=cishp)

Security Operations Center Courses

- SEC511: Continuous Monitoring and Security Operations (https://www.sans.org/course/continuous-monitoring-security-operations?msc=cishp)
- SEC555: SIEM with Tactical Analysis (https://www.sans.org/course/siem-with-tactical-analytics?msc=cishp) (NEW!)

Information Security Resources

- NewsBites: Bi-weekly email of top news stories with commentary from SANS Editors. View recent editions & Subscribe (https://www.sans.org/newsletters/newsbites/?msc=cishp)

- Whitepapers: Research from SANS instructors and masters students. Download the latest papers related to the Critical Controls (https://www.sans.org/reading-room/whitepapers/critical?msc=cishp)
- Webcasts: Topical content presented by SANS Instructors, vendors, and leaders in infosec security. View upcoming webcasts (https://www.sans.org/webcasts/?msc=cishp)

CIS Critical Security Controls – Version 7.1

To learn more about the CIS Critical Security Controls and download a free detailed version please visit: **http://www.cisecurity.org/critical-controls/ (http://www.cisecurity.org/critical-controls/)**

For Small and Medium Enterprises (SMEs): Download a specifically selected **sub-set of the CIS Controls (http://www.cisecurity.org/white-papers/cis-controls-sme-guide)** to help protect your business.

The SANS "What Works" program highlights success stories in cybersecurity - real examples of how real security teams have made measurable improvements in the effectiveness and efficiency of their security controls. While most of the press coverage focuses on breaches and other security failures, there are thousands of cybersecurity leaders quietly working hard and make advances against threats while enabling business and mission needs.

SANS expert John Pescatore interviews the end user and decision maker and produces a Q&A formatted case study and a live webcast that allows security practitioners to take advantage of lessons learned and accelerate their own cybersecurity improvements.

Check out recent SANS WhatWorks case studies:

Case Studies

Title	Vendor	Date
A Credit Union Increased Network Security With Network Access Control Based on Great Bay Software Beacon (/media/critical-security-controls/case-studies/GreatBay-Software-WhatWorks-Case-Study.pdf)	Great Bay Software	August 4, 2016
What Works in Threat Prevention: Detecting and Stopping Attacks More Accurately and Quickly with ThreatSTOP (/media/critical-security-controls/case-studies/ThreatSTOP-WhatWorks-Case-Study.pdf)	ThreatSTOP	May 16, 2016
Inspecting Encrypted Traffic with the Blue Coat SSL Visibility Appliance (/media/critical-security-controls/case-studies/Blue-Coat-WhatWorks-Case-Study.pdf)	Blue Coat	Mar. 23, 2016

What Works in Supply Chain and Partner Security: Using BitSight to Assess and Monitor Third-Party Cybersecurity (/media/critical-security-controls/case-studies/BitSight-WhatWorks-Case-Study.pdf)	BitSight	Nov. 7, 2015
Using WhiteHat Sentinel Dynamic and Static Solutions to Increase Application Security Before and After Production Deployment (/media/critical-security-controls/case-studies/WhatWorks-Case-Study-WhiteHat.pdf)	WhiteHat Security	Oct. 9, 2015
Lifecycle Vulnerability Management and Continuous Monitoring with Rapid7 Nexpose (/media/critical-security-controls/case-studies/case-study-rapid7.pdf)	Rapid7	Sept. 15, 2015
Using Palo Alto Networks Next Generation Firewalls to Increase Visibility into Threats and Reduce Threat Risks (/media/critical-security-controls/case-studies/case-study-palo-alto-networks.pdf)	Palo Alto Networks	May 19, 2015
Blocking Complex Malware Threats at Boston Financial (/media/critical-security-controls/case-studies/Invincea-BostonFinancial-WhatWorks-Whitepaper.pdf)	Invincea	Mar. 27, 2015
Increasing Security and Reducing Costs by Managing Administrator Rights with Process-based Privilege Management (/media/critical-security-controls/case-studies/WhatWorks-Viewfinity.pdf)	Viewfinity	Mar. 27, 2015
Reaping the Benefits of Continuous Monitoring and Mitigation at Pioneer Investments (/media/critical-security-controls/case-studies/WhatWorks-ForeScout.pdf)	ForeScout	Mar. 27, 2015
How VCU uses FireEye for Advanced Threat Detection and Prevention (/media/critical-security-controls/case-studies/FireEye_VCU_Case_Study_F.pdf)	FireEye	Mar. 10, 2015
Increasing Vulnerability Management Effectiveness While Reducing Cost (/media/critical-security-controls/case-studies/WhatWorks-Case Study-TENABLE-Network-Security.pdf)	Tenable	Feb. 19, 2015

Home (/critical-security-controls)

Guidelines (/critical-security-controls/guidelines)

History (/critical-security-controls/history)

Vendor Perspective (/critical-security-controls/vendor-perspective)

Best of Awards (/critical-security-controls/best-of-awards)

Downloads

- 2018 SANS Critical Security Controls Poster 🗎 (https://www.sans.org/media/critical-security-controls/Poster_CIS-Security-Controls_2018.pdf)
- 2016 SANS Continuous Monitoring Poster 🗎 (https://www.sans.org/media/critical-security-controls/SANS_CSC_Poster.pdf)
- 2014 SANS Critical Security Controls Poster (https://www.sans.org/media/critical-security-controls/Poster_Fall_2014_CSCs_WEB.PDF)

Feedback

Send Comments and Feedback to CCA@sans.org (mailto:CCA@sans.org)

Latest Whitepapers

Using Zero Trust to Enable Secure Remote Access (/reading_room/whitepapers/analyst/zero-trust-enable-secure-remote-access_39665)
By Dave Shackleford

Natural Language Processing for the Security Analyst (/reading_room/whitepapers/securityanalytics/natural-language-processing-security-analyst_39645)
By Daniel Severance

Real-Time Honeypot Forensic Investigation on a German Organized Crime Network (/reading_room/whitepapers/threathunting/real-time-honeypot-forensic-investigation-german-organized-crime-network_39640)
By Karim Lalji

Last 25 Papers » (/reading_room/)

Latest Tweets @SANSInstitute

Did you know you can demo roughly an hour of content for 50+ [...] (https://twitter.com/sansinstitute/statuses/1280677998790881281)
July 8, 2020 - 1:40 AM

Catch the latest episode of the #BlueprintPodcast, just out [...]
(https://twitter.com/sansinstitute/statuses/1280665415673360384)
July 8, 2020 - 12:50 AM

So much @sansforensics knowledge in one place! Download your [...]
(https://twitter.com/sansinstitute/statuses/1280653066119843841)
July 8, 2020 - 12:00 AM

Contact Us

Mon-Fri: 9am-8pm ET (phone/email)
Sat-Sun: 9am-5pm ET (email only)
301-654-SANS(7267)
info@sans.org (mailto:info@sans.org)

"The perfect balance of theory and hands-on experience."
- James D. Perry II, University of Tennessee

"SANS is a great place to enhance your technical and hands-on skills and tools. I thoroughly recommend it."
- Aaron Waugh, Datacom NZ Ltd

"SANS always provides you what you need to become a better security professional at the right price."
- Rasik Vekaria, BP

(https://twitter.com/sansinstitute) (https://www.linkedin.com/company/14104)
(https://www.facebook.com/pages/SANS-Institute/173623382673767)
(https://www.sans.org/rss.php)

Find Training (/find-training/) | Live Training (/security-training/) | Online Training (/online-security-training/) | Programs (/programs/) | Resources (/security-resources.php) | Vendor (/vendor/) | About (/about/)

Privacy Policy (/privacy/) | Trademark Usage Policy (/trademarkuse.pdf) | Credits (/site-credits) | © 2000-2020 SANS™ Institute