20 Critical Security Controls
for Effective Cyber Defense

The 20 Critical Controls enable cost-effective computer and network defense, making the process measurable, scalable, and reliable throughout the U.S. government, in the defense industrial base, and in other organizations that have important information and systems to protect. It is based on actual threats. The controls were selected by a consensus of the major U.S. government organizations that defend against cyber attacks as the controls that are most critical for stopping known attacks. Only one other security framework is based on threat – The Strategies to Mitigate Targeted Cyber Intrusions published by the Australian Defence Signals Directorate – which are also presented here.

The 20 Critical Controls prioritize the less threat-related catalog of guidelines published by the U.S. National Institutes of Standards and Technology (NIST) in Special Publication 800-53.

This poster offers a snapshot of the purpose and main features of each of the 20 Critical Controls, shows the NSA ratings of each control based on how well it accomplishes attack mitigation, where it fits in the overall hierarchy of required controls, and the level of technical maturity that has been reach in implementing the control. The poster also maps the 20 Critical Controls to the Australian Defence Signals Directorate's Strategies to Mitigate Targeted Cyber Intrusions and the NIST Special Publication 800-53, Revision 3, Priority 1 Controls.

You'll find the up-to-date 20 Critical Controls, Version 3 document posted at:
www.sans.org/critical-security-controls

And the Strategies to Mitigate Targeted Cyber Intrusions posted at:
www.dsd.gov.au/infosec/top35mitigationstrategies.htm

UK Centre for the Protection of National Infrastructure (CPNI) is developing advice to support the 20 Critical Controls: www.cpni.gov.uk/advice/infosec

NSA's Attack Mitigation View Of The 20 Critical Controls

The National Security Agency categorized the 20 Critical Controls both by their attack mitigation impact and by their importance.

Categories of Attack Mitigation

ADVERSARY ACTIONS TO ATTACK A NETWORK

Reconnaissance	Get In	Stay In	Exploit
Hardware Inventory (CAG 1)	Secure Configuration (CAG 3)	Audit Monitoring (CAG 14)	Security Skills & Training (CAG 9)
Software Inventory (CAG 2)	Secure Configuration (CAG 10)	Boundary Defense (CAG 13)	Data Recovery (CAG 8)
Continuous Vuln Access (CAG 4)	Application SW Security (CAG 6)	Admin Privileges (CAG 12)	Data Loss Prevention (CAG 17)
Networking Engineering (CAG 19)	Wireless (CAG 7) Malware Defense (CAG 5)	Controlled Access (CAG 15)	
Penetration Testing (CAG 20)	Limit Ports/P/S (CAG 11)	Penetration Testing (CAG 20)	Incident Response (CAG 18)

STOP ATTACKS EARLY — STOP MANY ATTACKS — MITIGATE IMPACT OF ATTACKS

Ranking in Importance: In order for a critical control to be a priority, it must provide a direct defense against attacks. Controls that mitigate: known attacks; a wide variety of attacks; attacks early in the compromise cycle; and the impact of a successful attack will have priority over other controls. Special consideration will be given to controls that help mitigate attacks that we haven't discovered yet.

VERY HIGH
These controls address operational conditions that are actively targeted and exploited by all threats.

HIGH
These controls address known initial entry points for targeted attacks.

MEDIUM
These controls reduce the attack surface, address known propagation techniques, and/or mitigate impact.

LOW
These controls are about optimizing, validating, and/or effectively managing controls.

Proof Of Value In Automating The 20 Critical Controls

Automating the critical controls provides daily, authoritative data on the readiness of computers to withstand attack as well as prioritized action lists for system administrators to maintain high levels of security. At the same time, it eliminates the massive financial waste associated with thick audit reports that are out-of-date long before they are published.

But such claims need proof.

At the US State Department, we see the first agency-wide implementation of automated security monitoring with unitary scoring giving system administrators unequivocal information on the most important security actions that need to be implemented every day. And the results are in:

In the first year the risk score for hundreds of thousands of computers across the State Department dropped by nearly 90% while those of other federal agencies hardly changed at all. (Chart 1) And the risk reduction continues to today. As importantly, when a major new threat arose, the State Department was able to get 90% of it systems patched in 10 days (Chart 2) while other agencies, without automation and scoring and sysadmin prioritization, got between 20% and 65% of their systems patched in several months.

Chart 1: 90% Risk Reduction In Less Than A Year

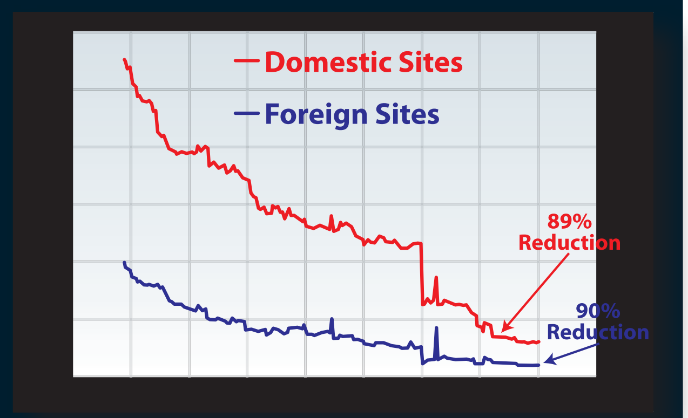
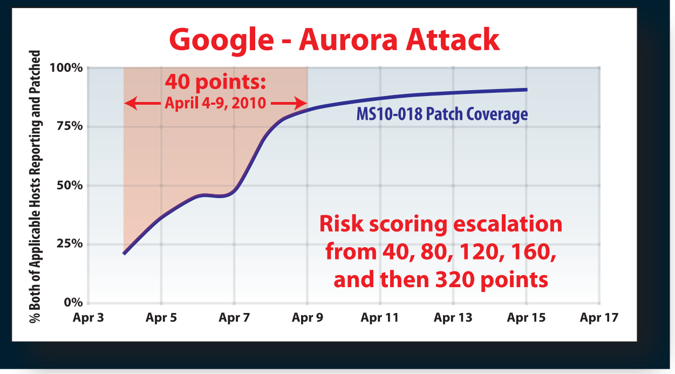


Chart 2: Threat-based mitigation: Giving the high priority fix a 40 point risk score gained rapid remediation to 80%; increasing it to 320 points pushed compliance to 90%.



The Australian Government's Strategies to Mitigate Targeted Cyber Intrusions

1 2 3 4 *Once organizations have implemented the top four mitigation strategies, firstly on computers used by employees most likely to be targeted by intrusions and then for all users, additional mitigation strategies can then be selected to address system security gaps to reach an acceptable level of residual risk*

20 Critical Security Controls			National Security Agency Assessment of the 20 Critical Controls				The Australian Government's Strategies to Mitigate Targeted Cyber Intrusions		Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls
Critical Security Control		Critical Security Control Description	Tier	Attack Mitigation	Dependencies	Technical Maturity	Ranking	Description	
1	Inventory of Authorized and Unauthorized Devices	**Reduce the ability of attackers to find and exploit unauthorized and unprotected systems:** Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.	1	Very High	Foundational	High			CM-8 (a, c, d, 2, 3, 4) PM-5 PM-6
2	Inventory of Authorized and Unauthorized Software	**Identify vulnerable or malicious software to mitigate or root out attacks:** Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.	1	Very High	Foundational	High	4.	Application whitelisting to help prevent malicious software and other unapproved programs from running e.g. by using Microsoft Software Restriction Policies or AppLocker.	CM-1 • CM-2 (2, 4, 5) • CM-3 CM-5 (2, 7) • CM-7 (1, 2) CM-8 (1, 2, 3, 4, 6) • CM-9 PM-6 • SA-6 • SA-7
3	Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers	**Prevent attackers from exploiting services and settings that allow easy access through networks and browsers:** Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.	1a	Very High	Capability	High	1. 2. 3. 13. 14. 20. 22. 25. 26. 27. 28. 31.	Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high risk vulnerabilities. Use the latest version of applications. Patch operating system vulnerabilities. Patch or mitigate within two days for high risk vulnerabilities. Use the latest operating system version. Minimise the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for e-mail and web browsing. Application-based workstation firewall, configured to deny traffic by default, to protect against malicious or otherwise unauthorized incoming network traffic. Application-based workstation firewall, configured to deny traffic by default, that whitelists which applications are allowed to generate outgoing network traffic. Data Execution Prevention using hardware and software mechanisms for all software applications that support DEP. Non-persistent virtualized trusted operating environment with limited access to network file shares, for risky activities such as reading e-mail and web browsing. Standard Operating Environment with unrequired operating system functionality disabled e.g. IPv6, autorun and Remote Desktop. Harden file and registry permissions. Workstation application security configuration hardening e.g. disable unrequired features in PDF viewers, Microsoft Office applications, and web browsers. Restrict access to NetBIOS services running on workstations and on servers where possible. Server application security configuration hardening e.g. databases, web applications, customer relationship management and other data storage systems. Disable LanMan password support and cached credentials on workstations and servers, to make it harder for adversaries to crack password hashes.	CM-1 • CM-2 (1, 2) CM-3 (b, c, d, e, 2, 3) CM-5 (2) • CM-6 (1, 2, 4) CM-7 (1) • SA-1 (a) SA-4 (5) • SI-7 (3) PM-6
4	Continuous Vulnerability Assessment and Remediation	**Proactively identify and repair software vulnerabilities reported by security researchers or vendors:** Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.	1a	Very High	Capability	High	1. 2.	Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high risk vulnerabilities. Use the latest version of applications. Patch operating system vulnerabilities. Patch or mitigate within two days for high risk vulnerabilities. Use the latest operating system version.	RA-3 (a, b, c, d) RA-5 (a, b, 1, 2, 5, 6)
5	Malware Defenses	**Block malicious code from tampering with system settings or contents, capturing sensitive data, or spreading:** Use automated anti-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.	1a	High/ Medium	Capability	High/ Medium	4. 5. 12. 14. 21.	Application whitelisting to help prevent malicious software and other unapproved programs from running e.g. by using Microsoft Software Restriction Policies or AppLocker. Host-based Intrusion Detection/Prevention System to identify anomalous behavior such as process injection, keystroke logging, driver loading and call hooking. Workstation inspection of Microsoft Office files for abnormalities e.g. using the Microsoft Office File Validation feature. Application-based workstation firewall, configured to deny traffic by default, that whitelists which applications are allowed to generate outgoing network traffic. Antivirus software with up to date signatures, reputation ratings and other heuristic detection capabilities. Use gateway and desktop antivirus software from different vendors.	SC-18 SC-26 SI-3 (a, b, 1, 2, 5, 6)
6	Application Software Security	**Neutralize vulnerabilities in web-based and other application software:** Carefully test internally developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic, and explicitly check for errors in all user input (including by size and data type).	2	High	Capability	Medium	28.	Server application security configuration hardening e.g. databases, web applications, customer relationship management and other data storage systems.	CM-7 • RA-5 (a, 1) SA-3 • SA-4 (3) • SA-8 SI-3 • SI-10
7	Wireless Device Control	**Protect the security perimeter against unauthorized wireless access:** Allow wireless devices to connect to the network only if it matches an authorized configuration and security profile and has a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.	2	High	Capability	Medium			AC-17 AC-18 (1, 2, 3, 4) SC-9 (1) • SC-24 SI-4 (14, 15)
8	Data Recovery Capability	**Minimize the damage from an attack:** Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.	2	Medium	Capability	Medium			CP-9 (a, b, d, 1, 3) CP-10 (6)
9	Security Skills Assessment and Appropriate Training to Fill Gaps	**Find knowledge gaps, and fill them with exercises and training:** Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.	2	Medium	Capability	Medium	8.	User education e.g. Internet threats and spear phishing socially engineered e-mails. Avoid: weak passphrases, passphrase reuse, exposing e-mail addresses, unapproved USB devices.	AT-1 • AT-2 (1) AT-3 (1)
10	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	**Preclude electronic holes from forming at connection points with the Internet, other organizations, and internal network segments:** Compare firewall, router, and switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates.	3	High/ Medium	Capability/ Dependent	Medium/ Low	15. 19.	Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication and user directory information. Border gateway using an IPv6-capable firewall to prevent computers directly accessing the Internet except via a split DNS server, an e-mail server, or an authenticated web proxy.	AC-4 (7, 10, 11, 16) • CM-1CM-2 (1) CM-3 (2) • CM-5 (1, 2, 5) CM-6 (4) • CM-7 (1, 3) • RA-5 IA-2 (1, 6) • IA-5 • IA-8 • SC-9 SC-7 (2, 4, 5, 6, 8, 11, 13, 14, 18)
11	Limitation and Control of Network Ports, Protocols, and Services	**Allow remote access only to legitimate users and services:** Apply host-based firewalls and port-filtering and -scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.	3	High/ Medium	Capability/ Dependent	Medium/ Low	13. 19.	Application-based workstation firewall, configured to deny traffic by default, to protect against malicious or otherwise unauthorized incoming network traffic. Border gateway using an IPv6-capable firewall to prevent computers directly accessing the Internet except via a split DNS server, an e-mail server, or an authenticated web proxy.	CM-6 (a, b, d, 2, 3) CM-7 (1) SC-7 (4, 5, 11, 12)
12	Controlled Use of Administrative Privileges	**Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack:** (1) enticing users to open a malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuation (FDCC) standards.	4	High/ Medium	Dependent	Medium	3. 16. 17. 18. 31.	Minimise the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for e-mail and web browsing. Multi-factor authentication especially implemented for when the user is about to perform a privileged action, or access a database or other sensitive information repository. Randomised local administrator passphrases that are unique and complex for all computers. Use domain group privileges instead of local administrator accounts. Enforce a strong passphrase policy covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words. Disable LanMan password support and cached credentials on workstations and servers, to make it harder for adversaries to crack password hashes.	AC-6 (2, 5) AC-17 (3) AC-19 AU-2 (4)
13	Boundary Defense	**Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines:** Establish multilayered boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks ("extranets").	4	High/ Medium	Dependent	Medium/ Low	6. 7. 9. 10. 11. 19. 21. 32. 33. 34.	Whitelisted e-mail content filtering allowing only attachment types required for business functionality. Preferably convert/sanitise PDF and Microsoft Office attachments. Block spoofed e-mails using Sender Policy Framework checking of incoming e-mails, and a "hard fail" SPF record to help prevent spoofing of your organisation's domain. Web content filtering of incoming and outgoing traffic, using signatures, reputation ratings and other heuristics, and whitelisting allowed types of web content. Web domain whitelisting for all domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains. Web domain whitelisting for HTTPS/SSL domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains. Border gateway using an IPv6-capable firewall to prevent computers directly accessing the Internet except via a split DNS server, an e-mail server, or an authenticated web proxy. Antivirus software with up to date signatures, reputation ratings and other heuristic detection capabilities. Use gateway and desktop antivirus software from different vendors. Block attempts to access web sites by their IP address instead of by their domain name. Network-based Intrusion Detection/Prevention System using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries. Gateway blacklisting to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.	AC-17 (1) • AC-20 CA-3 • IA-2 (1, 2) IA-8 • RA-5 SC-7 (1, 2, 3, 8, 10, 11, 14) • SC-18 SI-4 (c, 1, 4, 5, 11) • PM-7
14	Maintenance, Monitoring, and Analysis of Security Audit Logs	**Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines:** Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run biweekly reports to identify and document anomalies.	4	Medium	Dependent	Medium	23. 24. 35.	Centralised and time-synchronised logging of allowed and blocked network activity, with regular log analysis, storing logs for at least 18 months. Centralised and time-synchronised logging of successful and failed computer events, with regular log analysis, storing logs for at least 18 months. Full network traffic capture to perform post-incident analysis of successful intrusions, storing network traffic for at least the previous seven days.	AC-17 (1) • AC-19 • AU-2 (4) AU-3 (1,2) • AU-4 • AU-5 AU-6 (a, 1, 5) • AU-8 AU-9 (1, 2) • AU-12 (2) • SI-4 (8)
15	Controlled Access Based on the Need to Know	Prevent attackers from gaining access to highly sensitive data: Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.	4	Medium	Dependent	Medium/ Low	15. 30.	Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication and user directory information. TLS encryption between e-mail servers to help prevent legitimate e-mails being intercepted and used for social engineering. Perform content scanning after e-mail traffic is decrypted.	AC-1 • AC-2 (b, c) AC-3 (4) AC-4 • AC-6 MP-3 • RA-2 (a)
16	Account Monitoring and Control	**Keep attackers from impersonating legitimate users:** Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.	4	Medium	Dependent	Medium/ Low	18.	Enforce a strong passphrase policy covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words.	AC-2 (e, f, g, h, j, 2, 3, 4, 5) AC-3
17	Data Loss Prevention	**Stop unauthorized transfer of sensitive data through network attacks and physical theft:** Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.	5	Medium/ Low	Dependent	Low	29.	Removable and portable media control as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.	AC-4 • MP-2 (2) • MP-4 (1) SC-7 (6, 10) • SC-9 • SC-13 SC-28 (1) • SI-4 (4, 11) • PM-7
18	Incident Response Capability	**Protect the organization's reputation, as well as its information:** Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.	5	Medium	Dependent	Low			IR-1 • IR-2 (1) IR-4 • IR-5 IR-6 (a) • IR-8
19	Secure Network Engineering	**Keep poor network design from enabling attackers:** Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers: DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.	6	Low	Indirect	Low	15. 19.	Network segmentation and segregation into security zones to protect sensitive information and critical services such as user authentication and user directory information. Border gateway using an IPv6-capable firewall to prevent computers directly accessing the Internet except via a split DNS server, an e-mail server, or an authenticated web proxy.	IR-4 (2) • SA-8 SC-7 (1, 13) • SC-20 • SC-21 SC-22 • PM-7
20	Penetration Tests and Red Team Exercises	**Use simulated attacks to improve organizational readiness:** Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises—all-out attempts to gain access to critical data and systems— to test existing defenses and response capabilities.	6	Low	Indirect	Medium/ Low			CA-2 (1, 2) • CA-7 (1, 2) RA-3 • RA-5 (4, 9) SA-12 (7)

🟨 *NSA identifies these 3 controls as having special value for immediate implementation in organizations that have not yet implemented more complete defenses.*

AUSTRALIA — Australian Government Department of Defence
UNITED KINGDOM — CPNI Centre for the Protection of National Infrastructure
UNITED STATES — Homeland Security

SANS
Winter 2012

Building Successful Careers in Cyber Security

The U.S. National Initiative for Cybersecurity Education (NICE) Framework and the SANS Institute Training, Education, and Certification Programs

NICE FRAMEWORK CATEGORY		NICE FRAMEWORK SPECIALTY AREA	NICE FRAMEWORK JOB TITLES	GIAC CERTS	SANS COURSES
Securely Provision	Specialty areas concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development.	**Enterprise Architecture** Develops the systems concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.	• IA Architect • Information Security Architect • Network Security Analyst • Information Systems Security Engineer • R&D Engineer • Security Architect • Security Engineer • Security Solutions Architect • Systems Engineer • Systems Security Analyst	GCED GCFW	SEC501: Advanced Security Essentials - Enterprise Defender SEC502: Perimeter Protection In-Depth SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth SEC577: Virtualization Security Fundamentals
		Information Assurance Compliance Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's IA requirements. Ensure compliance from internal and external perspectives.	• Accreditor • Auditor • Authorizing Official Designated Representative • Certification Agent • Certifying Official • Compliance Manager • Designated Accrediting Authority • IA Compliance Analyst/Manager • IA Officer • IA Manager • Portfolio Manager • Risk/Vulnerability Analyst • Security Control Assessor • Validator	GSNA	AUD407: Foundations of Auditing Information Systems AUD507: Auditing Networks, Perimeters & Systems SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth
		Software Engineering Develops, creates, and writes/codes, new (or modifies existing) computer applications, software, or specialized utility programs.	• Analyst Programmer • Computer Programmer • Configuration Manager • IA Engineer • IA Software Developer • IA Software Engineer • R&D Engineer • Secure Software Engineer • Security Engineer • Software Developer • Systems Analyst • Web Application Developer	GWEB GSSP-JAVA GSSP-NET GSSP-C	DEV522: Defending Web Applications Security Essentials DEV530: Essential Secure Coding in Java/JEE DEV532: Essential Secure Coding in ASP.NET DEV536: Secure Coding for PCI Compliance DEV541: Secure Coding in Java/JEE: Developing Defensible Applications DEV543: Secure Coding in C & C++ DEV544: Secure Coding in .NET: Developing Defensible Applications DEV551: Secure Mobile Applications Development: iOS App Security DEV568: Secure Mobile Applications Development: Android App Security
		Systems Development Works on the development phases of the systems development lifecycle.	• IA Developer • IA Engineer • Program Developer • Security Engineer • Information Systems Security Engineer • Systems Engineer	GWEB GSSP-JAVA GSSP-NET GSSP-C	DEV522: Defending Web Applications Security Essentials DEV530: Essential Secure Coding in Java/JEE DEV532: Essential Secure Coding in ASP.NET DEV536: Secure Coding for PCI Compliance DEV541: Secure Coding in Java/JEE: Developing Defensible Applications DEV543: Secure Coding in C & C++ DEV544: Secure Coding in .NET: Developing Defensible Applications DEV551: Secure Mobile Applications Development: iOS App Security DEV568: Secure Mobile Applications Development: Android App Security
Operate & Maintain	Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.	**Information Systems Security Management** Oversees the information assurance program of an information system in or outside the network environment; may include procurement duties (e.g., ISSO).	• Information Assurance Manager • Information Assurance Program Manager • Information Assurance Security Officer • Information Security Program Manager • Information Systems Security Manager • Information Systems Security Officer (ISSO)	GSNA GSLC GCPM	AUD507: Auditing Networks, Perimeters & Systems MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™ MGT525: IT Project Management, Effective Communication, and PMP Exam Prep SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth
		Network Services Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.	• Cabling Technician • Converged Network Engineer • Network Administrator • Network Analyst • Network Designer • Network Engineer • Network Systems And Data Communications Analyst • Telecommunications Engineer/Personnel/Specialist	GCED GCFW GCIA	SEC501: Advanced Security Essentials - Enterprise Defender SEC502: Perimeter Protection In-Depth SEC503: Intrusion Detection In-Depth SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth
		System Administration Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control/passwords/ account creation and administration.	• LAN Administrator • Platform Specialist • Security Administrator • Server Administrator • System Operations Personnel • Systems Administrator • Website Administrator	GSEC GCFW GCWN GCUX	SEC401: SANS Security Essentials Bootcamp Style SEC464: Hacker Detection for Systems Administrators with Continuing Education Program SEC502: Perimeter Protection In-Depth SEC505: Securing Windows SEC506: Securing Linux/Unix
		Systems Security Analysis Conducts the integration/testing, operations, and maintenance of systems security.	• IA Operational Engineer • Information Assurance Security Officer • Information Security Analyst/Administrator • Information System Security Manager • Information Systems Security Engineer • Platform Specialist • Security Administrator • Security Analyst • Security Control Assessor • Security Engineer	GSEC GCED GCFW GCWN GCUX	SEC401: SANS Security Essentials Bootcamp Style SEC464: Hacker Detection for Systems Administrators with Continuing Education Program SEC501: Advanced Security Essentials - Enterprise Defender SEC502: Perimeter Protection In-Depth SEC505: Securing Windows SEC506: Securing Linux/Unix SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth
Protect & Defend	Specialty areas responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks.	**Computer Network Defense** Use defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.	• LAN Administrator • Platform Specialist • Security Administrator • Server Administrator • System Operations Personnel • Systems Administrator • Website Administrator	GCFE GCFA GREM GSEC GCIA GCIH	FOR408: Computer Forensic Investigations - Windows In-Depth FOR508: Advanced Computer Forensic Analysis and Incident Response FOR558: Network Forensics FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques SEC401: SANS Security Essentials Bootcamp Style SEC464: Hacker Detection for Systems Administrators with Continuing Education Program SEC503: Intrusion Detection In-Depth SEC504: Hacker Techniques, Exploits and Incident Handling
		Computer Network Defense Infrastructure Support Tests, implements, deploys, maintains, and administers the infrastructure hardware and software, which are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.	• IDS Administrator • IDS Engineer • IDS Technician • Network Administrator • Information Systems Security Engineer • Network Analyst • Network Security Engineer • Network Security Specialist • Security Analyst • Security Engineer • Security Specialist • Systems Security Engineer	GCED GCFW GCIA GCWN GCUX	AUD407: Foundations of Auditing Information Systems SEC501: Advanced Security Essentials - Enterprise Defender SEC502: Perimeter Protection In-Depth SEC503: Intrusion Detection In-Depth SEC505: Securing Windows SEC506: Securing Linux/Unix SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth
		Incident Response Respond to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.	• Computer Crime Investigator • Incident Handler • Incident Responder • Intrusion Analyst	GCFA GCFE GREM GCIA GCIH	FOR408: Computer Forensic Investigations - Windows In-Depth FOR508: Advanced Computer Forensic Analysis and Incident Response FOR558: Network Forensics FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques SEC503: Intrusion Detection In-Depth SEC504: Hacker Techniques, Exploits and Incident Handling
		Security Program Management Manages relevant security (e.g., information security) implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources (e.g., CISO).	• Chief Information Security Officer (CISO) • Common Control Provider • Cybersecurity Officer • Enterprise Security Officer • Facility Security Officer • IT Director • Principal Security Architect • Risk Executive • Security Domain Specialist • Senior Agency Information Security Officer (SAIS)	GSLC GCPM	MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™ MGT514: IT Security Strategic Planning, Policy and Leadership MGT525: IT Project Management, Effective Communication, and PMP Exam Prep SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth
		Vulnerability Assessment and Management Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.	• Blue Team Technician • Close Access Technician • CND Auditor • Compliance Manager • Ethical Hacker • Governance Manager • Internal Enterprise Auditor • Penetration Tester • Red Team Technician • Reverse Engineer • Risk/Vulnerability Analyst • Vulnerability Manager	GSNA GWAPT GPEN GXPN	AUD407: Foundations of Auditing Information Systems SEC542: Web App Penetration Testing and Ethical Hacking SEC560: Network Penetration Testing and Ethical Hacking SEC580: Metasploit Kung Fu for Enterprise Pen Testing SEC642: Advanced Web App Penetration Testing and Ethical Hacking SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking SEC710: Advanced Exploit Development
Investigate	Specialty areas responsible for the investigation of cyber events/crimes of IT systems, networks, and/or digital evidence.	**Digital Forensics** Collects, processes, preserves, analyses, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, and counterintelligence or law enforcement investigations.	• Computer Network Defense Forensic Analyst • Digital Forensic Examiner • Digital Media Collector • Forensic Analyst • Forensic Analyst (Cryptologic) • Network Forensic Examiner	GCFE GCFA GREM	FOR408: Computer Forensic Investigations - Windows In-Depth FOR508: Advanced Computer Forensic Analysis and Incident Response FOR558: Network Forensics FOR563: Mobile Device Forensics FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
		Investigation Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection and appropriately balances the benefits of prosecution versus intelligence gathering.	• Computer Crime Investigator • Special Agent	GCFE GCFA GREM	FOR408: Computer Forensic Investigations - Windows In-Depth FOR508: Advanced Computer Forensic Analysis and Incident Response FOR558: Network Forensics FOR563: Mobile Device Forensics FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Operate & Collect	Specialty areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.	**Collection Operations** Executes collection using appropriate collection strategies and within the priorities established through the collection management process.	• CIC Case Officer • CIC Operations Officer • CIC Targeting Officer • Field Collection Officer • Special Agent	GCFE GCFA GREM	FOR408: Computer Forensic Investigations - Windows In-Depth FOR508: Advanced Computer Forensic Analysis and Incident Response FOR558: Network Forensics FOR563: Mobile Device Forensics FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
		Cyber Operations Uses automated tools to manage, monitor, and/or execute large-scale cyber operations in response to national and tactical requirements.	• Close Access Network Operator • Interactive Operator • Production Operator		MGT405: Critical Infrastructure Protection
		Cyber Operations Planning Gathers information and develops detailed operational plans and orders supporting requirements. Conducts strategic and operational level planning across the full range of operations for integrated information and cyberspace operations.	• Cryptologic Cyber Planner • Network Warfare Cyber Planner		NetWars
Analyze	Specialty areas responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.	**All Source Intelligence** Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesize and place intelligence information into context; draw insights about the possible implications.	• Battle Damage Assessment Analyst • General Military Intelligence Analyst • Indications and Warning Analyst • Operational Target Development		
		Cyber Threat Analysis Using cyber means, identify and assess the capabilities and activities of cyber criminals or foreign intelligence entities; produce findings to help initialize or support law enforcement and counterintelligence investigations or activities.	• CIC International Specialist • Criminal Research Specialist • Digital Network Exploitation Analyst • Endpoint Exploitation Analyst • Strategic Analyst • Tactical Analyst	GCFE GCFA GREM	FOR408: Computer Forensic Investigations - Windows In-Depth FOR508: Advanced Computer Forensic Analysis and Incident Response FOR558: Network Forensics FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
		Exploitation Analysis Analyzes collected information to identify vulnerabilities and potential for exploitation.	• Digital Network Exploitation Analyst • Endpoint Exploitation Analyst • Intel Analyst	GCIH GWAPT GPEN GAWN GXPN	SEC504: Hacker Techniques, Exploits and Incident Handling SEC542: Web App Penetration Testing and Ethical Hacking SEC560: Network Penetration Testing and Ethical Hacking SEC580: Metasploit Kung Fu for Enterprise Pen Testing SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses SEC642: Advanced Web App Penetration Testing and Ethical Hacking SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking SEC710: Advanced Exploit Development
		Targets Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.	• Effects Analyst • Target Analyst Reporter • Target Digital Network Analyst		

SANS

The Most Trusted Name for Information and Software Security

Security Roadmap

WINTER 2012 – 21ST EDITION

Building Successful Careers in Cyber Security

AND

20 Critical Security Controls for Effective Cyber Defense