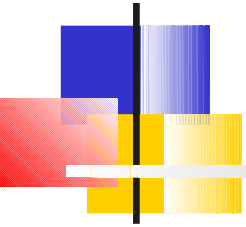


Top 20 critical security controls



What it is



- These Top 20 Controls were agreed upon by a powerful consortium under the auspices of the Center for Strategic and International Studies.
- Members of the Consortium include NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities.



Guiding Principles

- Defenses should focus on addressing the most common and damaging attack activities occurring today, and those anticipated in the near future.
- Enterprise environments must ensure consistent controls across an enterprise to negate attacks.
- Defenses should be automated where possible, and periodically or continuously measured using automated measurement techniques where feasible.
- To address current attacks occurring on a frequent basis against numerous organizations, a variety of specific technical activities should be undertaken to produce a more consistent defense.

Why to use them



- The automation of these Top 20 Controls will radically lower the cost of security while improving its effectiveness.
- The US State Department has already demonstrated more than 80% reduction in "measured" security risk through the rigorous automation and measurement of the Top 20 Controls.

Guidelines Version 2.3



- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation

Guidelines



- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches



Guidelines

- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know



Guidelines

- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises



Nel seguito

In generale per ogni controllo avremo 3 info

- a) cosa può succedere se non esiste (S)
- b) come implementarlo (ci concentriamo su strumenti per implementarlo in automatico) (T)
- c) metrica per misurare se è implementato efficacemente (M)



CC 1: Inventory of Authorized and Unauthorized Devices (S)

- Attackers deploy systems that continuously scan address spaces of target waiting for new, unprotected systems to be attached to the network.
- Additionally, attackers frequently look for experimental or test systems that are briefly connected to the network but not included in the standard asset inventory of an organization.



CC 1: Inventory of Authorized and Unauthorized Devices (T)

- Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s). Active tools scan address ranges, passive tools identify hosts by analyzing their traffic
- Deploy dynamic host configuration protocol (DHCP) server logging, and improve the asset inventory and detect unknown systems through this DHCP information.
- Ensure that equipment acquisitions automatically update the inventory system as new devices are connected to the network. Use robust change control process to validate and approve new devices.



CC 1: Inventory of Authorized and Unauthorized Devices (M)

- The system should
 - Identify any new unauthorized devices connected to the network within 24 hours,
 - Alert administrative personnel
 - Automatically isolate the unauthorized system from the network within one hour of the initial alert
- In the future alert sent within 2 minutes and isolation achieved within 5 .

CC 2: Inventory of Authorized and Unauthorized Software (S)



- Attackers continuously scan address spaces of target organizations looking for vulnerable versions of software that can be remotely exploited.
- Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites.
- Without the ability to inventory and control which programs are installed and allowed to run on their machines, enterprises make their systems more vulnerable.

CC2: Inventory of Authorized and Unauthorized Software Tools (T)



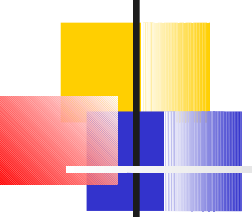
- Deploy application white listing technology that allows systems to run software only on the white list and prevents execution of all other software.
- Only a general purpose system may result in a long list
- Devise a list of authorized software for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.
- Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system



CC 2: Inventory of Authorized and Unauthorized Software (M)

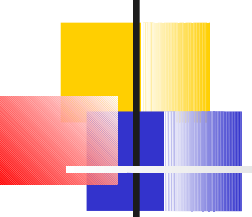
- The system should
 - detect and identify any attempt to install or execute unauthorized software
 - alert personnel within 24 hours
 - block installation, prevent execution, or quarantine unauthorized software within one additional hour, alerting when this has occurred.
- Organizations should strive for even more rapid alerting and isolation.

CC3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers (S)



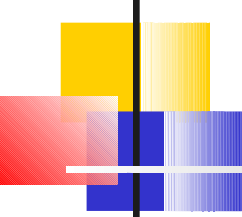
- Automated scanners constantly search target networks looking for systems that were configured with vulnerable software installed the way it was delivered from manufacturers and resellers, thereby making it immediately vulnerable to exploitation.
- Default configurations are not geared to security, leaving extraneous services that are exploitable in their default state. In addition, patches are not always applied in a timely manner
- Attackers attempt to exploit both network-accessible services and browsing client software using such techniques.
- Defenses against these automated exploits include procuring computer and network components with the secure configurations already implemented, deploying such pre-configured hardened systems, updating these configurations on a regular basis, and tracking them in a configuration management system.

CC3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers (T)



- Organizations can implement this control by developing a series of images and secure storage servers for hosting these standard images.
- Commercial and/or free configuration management tools can then be employed to measure the settings operating system and applications of managed machines to look for deviations from the standard image configurations used by the organization.
- Some configuration management tools require that an agent be installed on each managed system, while others remotely log in to each managed machine using administrator credentials. Either approach or a combination of the two approaches can provide the information needed for this control.

CC3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers (M)

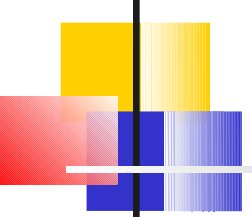


- The system must be capable of identifying any changes to an official hardened image ie. modifications to key files, services, ports, configuration files, or any software installed on the system.
- The configuration of each system must be checked against the official master image database to verify any changes to secure configurations that would impact security.
- Any of these changes to a computer system must be detected within 24 hours and notification performed by alerting administrative personnel.
- Systems must block installation, prevent execution, or quarantine unauthorized software within one additional hour, alerting or sending e-mail when this action has occurred.
- In the future organizations should strive for even more rapid alerting and isolation.

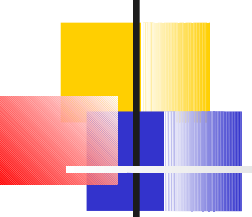
CC4: Continuous Vulnerability Assessment and Remediation (S)

- Soon after new vulnerabilities are discovered and reported, attackers engineer exploit code and then launch that code against targets of interest.
- Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain.
- Organizations that do not scan for vulnerabilities face a significant likelihood of having their computer systems compromised. Vulnerabilities must also be tied to threat intelligence and be properly prioritized.
- As vulnerability scans become more common, attackers are utilizing them as a point of exploitation. It is important to carefully control authenticated vulnerability scans and the associated administrator account.

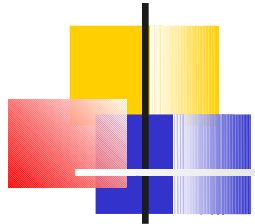
CC4: Continuous Vulnerability Assessment and Remediation (T)

- 
-
- A large number of vulnerability scanning tools are available to evaluate the security configuration of systems. Some enterprises use services based upon remotely managed scanning appliances.
 - To help standardize the definitions of vulnerabilities in multiple departments or across organizations, tools should measure security flaws and map them to vulnerabilities using some industry-recognized vulnerability, configuration, and platform classification schemes and languages: CVE, CCE, OVAL, CPE, CVSS, and/or XCCDF.
 - Advanced vulnerability scanning tools can be configured with user credentials to log in to scanned systems and perform more comprehensive scans than without credentials.
 - The frequency of scanning activities should increase as the diversity of an organization's systems increases to account for the varying patch cycles of each vendor.

CC4: Continuous Vulnerability Assessment and Remediation (T)

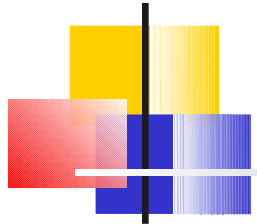
- 
-
- CVE = common vulnerability enumeration
 - assigns identifiers to publicly known system vulnerabilities
 - CCE = common configuration enumeration
 - assigns unique entries (CCEs) to configuration guidance statements and configuration controls to improve workflow by facilitating fast and accurate correlation of configuration issues present in disparate domains
 - OVAL = open vulnerability assessment language
 - a language that standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment

CC4: Continuous Vulnerability Assessment and Remediation (T)



- CPE common product enumeration
 - A standard machine-readable format for encoding names of IT products and platforms.
 - A set of procedures for comparing names.
 - A language to build "applicability statements" = CPE names with simple logical operators.
 - A standard notion of a CPE Dictionary.
- CVSS Common vulnerability scoring system
 - maps each vulnerability into a risk for the whole system
- XCCDF Extensible Configuration Checklist Description Format
 - specification language for writing security checklists, benchmarks. An XCCDF document represents a structured collection of security configuration rules for some target systems.

CC4: Continuous Vulnerability Assessment and Remediation (T)



The CVSS standard includes three groups of metrics of a vulnerability:

- base metrics= intrinsic and fundamental characteristics that are constant over time and user environments;
- temporal metrics = characteristics that change over time but not among user environments
- environmental metrics = characteristics that are relevant and unique to a particular user's environment

CC4: Continuous Vulnerability Assessment and Remediation (T)



Base Score Metrics

Exploitability Metrics

Access Vector (AV)*

- Local (AV:L) Adjacent Network (AV:A) Network (AV:N)

Access Complexity (AC)*

- High (AC:H) Medium (AC:M) Low (AC:L)

Authentication (Au)*

- Multiple (Au:M) Single (Au:S) None (Au:N)

* - All base metrics are required to generate a base score.

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Partial (C:P) Complete (C:C)

Integrity Impact (I)*

None (I:N) Partial (I:P) Complete (I:C)

Availability Impact (A)*

None (A:N) Partial (A:P) Complete (A:C)

CC4: Continuous Vulnerability Assessment and Remediation (T)

Temporal Score metrics

Exploitability (E)

Not Defined (E:ND) Unproven that exploit exists (E:U) Proof of concept code (E:POC) Functional exploit exists (E:F) High (E:H)

Remediation Level (RL)

Not Defined (RL:ND) Official fix (RL:OF) Temporary fix (RL:T)
Workaround (RL:W) Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:ND) Unconfirmed (RC:UC) Uncorroborated (RC:UR)
Confirmed (RC:C)

CC4: Continuous Vulnerability Assessment and Remediation (T)



Environmental Score metrics

General Modifiers

Collateral Damage Potential (CDP)

- Not Defined (CDP:ND)
- None (CDP:N)
- Low (light loss) (CDP:L)
- Low-Medium (CDP:LM)
- Medium-High (CDP:MH)
- High (catastrophic loss) (CDP:H)

Target Distribution (TD)

- Not Defined (TD:ND)
- None [0%] (TD:N)
- Low [0-25%] (TD:L)
- Medium [26-75%] (TD:M)
- High [76-100%] (TD:H)

Impact Subscore Modifiers

Confidentiality Requirement (CR)

- Not Defined (CR:ND)
- Low (CR:L)
- Medium (CR:M)
- High (CR:H)

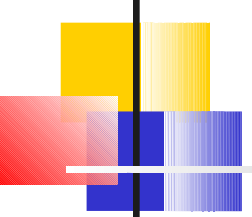
Integrity Requirement (IR)

- Not Defined (IR:ND)
- Low (IR:L)
- Medium (IR:M)
- High (IR:H)

Availability Requirement (AR)

- Not Defined (AR:ND)
- Low (AR:L)
- Medium (AR:M)
- High (AR:H)

CC4: Continuous Vulnerability Assessment and Remediation (M)

- 
-
- All machines identified by the asset inventory system associated with Critical Control 1 must be scanned for vulnerabilities.
 - Additionally, if the vulnerability scanner identifies any devices not included in the asset inventory, it must alert or send e-mail to enterprise administrative personnel within 24 hours.
 - The system must be able to alert or e-mail enterprise administrative personnel within one hour of weekly or daily automated vulnerability scans being completed.
 - If a scan cannot be completed successfully, the system must alert or send e-mail to administrative personnel within one hour indicating that the scan has not completed successfully.
 - Every 24 hours after that point, the system must alert or send e-mail about the status of uncompleted scans, until normal scanning resumes..



Critical Control 5: Malware Defenses (S)

- Malicious software is an integral and dangerous aspect of Internet threats, targeting end-users and organizations via web browsing, e-mail attachments, mobile devices, the cloud, and other vectors.
- Malicious code may tamper with the system's contents, capture sensitive data, and spread to other systems.
- Modern malware aims to avoid signature-based and behavioral detection, and may disable anti-virus tools running on the targeted system.
- Anti-virus and anti-spyware software, collectively referred to as anti-malware tools, help defend against these threats by attempting to detect malware and block its execution.



Critical Control 5: Malware Defenses (T)

- Organizations use automation to ensure anti-virus signatures are up to date and the built-in administrative features of security suites to verify that anti-virus, anti-spyware, and host-based IDS features are active on every managed system.
- Organization run automated assessments daily to find and mitigate systems that have deactivated such protections or do not have the latest malware definitions.
- Some enterprises deploy honeypot and tarpit tools to identify attackers in their environment.
- Security personnel should continuously monitor honeypots and tarpits to determine whether traffic is directed to them and account logins are attempted.



Critical Control 5: Malware Defenses (M)

- Systems must identify any malicious software that is installed, attempted to be installed, executed, or attempted to be executed on a computer system within one hour, alerting personnel via their centralized anti-malware console or event log system.
- Systems must block installation, prevent execution, or quarantine malicious software within one hour, alerting or sending e-mail when this action has occurred.
- Every 24 hours after that point, the system must alert or send e-mail about the status of the malicious code until such time as the threat has been completely mitigated on that system.



Critical Control 6: Application Software Security (S)

- Application software could be vulnerable to remote compromise by attackers that can inject specific exploits, including buffer overflows, SQL injection attacks, cross-site scripting, cross-site request forgery, and click-jacking of code to gain control over vulnerable machines.
- To avoid such attacks, both internally developed and third-party application software must be carefully tested.
- For third-party application software, enterprises should verify that vendors have conducted detailed security testing of their products.
- For in-house developed applications, enterprises must conduct such testing themselves or engage an expert.



Critical Control 6: Application Software Security (T)

- Source code testing tools, web application security scanning tools, and object code testing tools have proven useful in securing application software, along with manual application security penetration testing.
- The Common Weakness Enumeration (CWE) is used by many tools to identify the weaknesses that they find.
- Organizations can also use CWE to determine which types of weaknesses they are most interested in addressing and removing.
- MITRE's Common Attack Pattern Enumeration and Classification can be used to organize and record the breadth of the testing for the CWEs.



Critical Control 6: Application Software Security (M)

- The system must be capable of detecting and blocking an application-level software attack, and must generate an alert within 24 hours of detection and blocking.
- All Internet-accessible web applications must be scanned on a weekly or daily basis, alerting or sending e-mail to administrative personnel within 24 hours of completing a scan.
- Additionally, all high-risk vulnerabilities in Internet-accessible web applications identified by vulnerability scanners, static analysis tools, and automated database configuration review tools must be mitigated (by fixing the flaw or implementing a compensating control) within 15 days of discovery



Critical Control 7: Wireless Device Control (S)

- Major thefts of data have been initiated by attackers who have gained wireless access from outside the physical building, bypassing organizations' security perimeters by connecting wirelessly to access points inside.
- Wireless clients accompanying traveling officials are infected on a regular basis through remote exploitation during air travel or in cyber cafes.
- Such exploited systems are then used as back doors when they are reconnected to the network of a target organization.
- Because they do not require direct physical connections, wireless devices are a convenient vector for attackers to maintain long-term access into a target environment.



Critical Control 7: Wireless Device Control (T)

- Effective organizations run wireless scanning, detection and discovery tools and wireless intrusion detection systems.
- Wireless traffic should be captured within the borders of a facility to determine whether it was transmitted using weaker protocols or encryption than the organization mandates.
- When devices relying on weak wireless security settings are identified, they should be found within the organization's asset inventory and either reconfigured more securely or denied access to the organization network.
- Additionally, remote management tools on the wired network should be used to pull information about the wireless capabilities and devices connected to managed systems.



Critical Control 7: Wireless Device Control (M)

- The system must be capable of identifying unauthorized wireless devices or configurations within range of the organization systems or connected to their networks.
- The system must be capable of identifying any new unauthorized wireless devices that associate or join the network within one hour.
- The system must automatically isolate an attached wireless access point from the network within one hour and alert or send e-mail notification when isolation is achieved.
- The asset inventory database and alerting system must be able to identify the location, department where authorized and unauthorized wireless devices are plugged.



Critical Control 8: Data Recovery Capability (S)

- When attackers compromise machines, they often make significant changes to configurations and software.
- Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information.
- When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine.



Critical Control 8: Data Recovery Capability (M)

- Once per quarter (or whenever new backup equipment is purchased), a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment.
- The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.



Critical Control 9: Security Skills

Assessment and Appropriate Training to Fill Gaps (S)

- Most adversaries will be stopped by effective implementation of the other Critical Controls, but some will slip through fissures in the program.
- Skilled employees in the following jobs are essential for implementing and monitoring those Controls, for finding attackers that get through the defenses, and for developing systems that are much harder to exploit:
 - system, network, application penetration testers,
 - security monitoring and event analysts,
 - incident responders in-depth,
 - threat analysts/counter intelligence analysts,
 - risk assessment engineers,
 - advanced forensics analysts,
 - secure coders and code reviewers,
 - security engineers - operations, and
 - security engineers/architects



Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches (S)

- Attackers take advantage of the fact that network devices may become less securely configured over time as users demand exceptions for specific and temporary needs.
- Some exceptions are not undone they are no longer applicable.
- Attackers search for electronic holes in firewalls, routers, and switches and use those to penetrate defenses.
- Attackers have exploited flaws in these network devices to gain access to target networks, redirect traffic on a network (to a malicious system masquerading as a trusted system), and intercept and alter information while in transmission.



Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches (T)

- Some organizations use commercial tools that evaluate the rule set of network filtering devices to determine whether they are consistent or in conflict, providing an automated sanity check of network filters and search for errors in rule sets or access controls lists (ACLs) that may allow unintended services through the device.
- Such tools should be run each time significant changes are made to firewall rule sets, router ACLs, or other filtering technologies.



Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches (M)

- The system must be capable of identifying any changes to network devices, including routers, switches, firewalls, and IDS and IPS systems.
- The configuration of each system must be checked against the official master image database to verify any changes to secure configurations that would impact security.
- Any of these changes to a device must be detected within 24 hours and notification performed by alerting or sending e-mail notification to a list of enterprise personnel. If possible, devices must prevent changes to the system and send an alert indicating the change was not successful.



Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services (S)

- Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and domain name system (DNS) servers installed by default on a variety of different device types,.
- Many software packages automatically install services and turn them on as part of the installation of the main software package without informing a user or administrator that the services have been enabled.
- Attackers scan for such issues and attempt to exploit these services, often attempting default user IDs and passwords or widely available exploitation code.



Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services (T)

- Port scanning tools are used to determine which services are listening on the network for a range of target systems. In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service listening on each discovered open port.
- Services and their versions are compared against an inventory of services required by the organization for each server and workstation in an asset management system.
- Added features in these port scanners are being used to determine the changes in services offered by scanned machines on the network since the previous scan, helping security personnel identify differences over time.



Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services (M)

- The system must be capable of identifying any new unauthorized listening network ports that are connected to the network within 24 hours, alerting or sending e-mail notification to a list of enterprise personnel.
- Every 24 hours, the system must alert about the status of the system until the listening network port has been disabled or has been authorized by change management.
- The system service baseline database and alerting system must be able to identify the location, department, and other details about the system where authorized and unauthorized network ports are running.



Critical Control 12: Controlled Use of Administrative Privileges (S)

- The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise.
- A first common attack fools a user, running as a privileged user into opening a malicious e-mail attachment or a file from a malicious website. If the victim account has administrative privileges, the attacker controls the machine and install keystroke loggers, sniffers, and remote control software to find passwords and other data.
- The second common attack is elevation of privileges by guessing or cracking an administration password. If administrative privileges are loosely and widely distributed, the attacker has a much easier time gaining full control of systems.



Critical Control 12: Controlled Use of Administrative Privileges (T)

- Built-in operating system features can extract lists of accounts with super-user privileges. To verify that users with high-privileged accounts do not use such accounts for day-to-day web surfing and e-mail reading, security personnel should periodically gather running processes to determine browsers or e-mail readers running with high privileges.
- Some legitimate system administration activity may require the execution of such programs over the short term, but long-term use could indicate that an administrator is not adhering to this control.
- To enforce the requirement for strong passwords, built-in operating system features for minimum password length can be configured to prevent users from choosing short passwords.



Critical Control 12: Controlled Use of Administrative Privileges (M)

- The system must be configured to comply with password policies at least as stringent as those described in the controls above.
- Security personnel must be notified via an alert or e-mail within 24 hours of the addition of an account to a super-user group, such as a domain administrator.
- While the 24-hour timeframes represent the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting.



Critical Control 13: Boundary Defense (S1)

- Attackers use configuration and architectural weaknesses found on perimeter systems, network devices, and Internet-accessing client machines to gain initial access into an organization.
- Then, with a base of operations on these machines, attackers often pivot to get deeper inside the boundary to steal or change information or to set up a persistent presence for later attacks against internal hosts.
- To control the flow of traffic through network borders and police content boundary defenses should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks, and network-based IPS and IDS. It is also critical to filter both inbound and outbound traffic.



Critical Control 13: Boundary Defense (S2)

- It should be noted that boundary lines between internal and external networks are diminishing as a result of increased interconnectivity within and between organizations as well as the rapid rise in deployment of wireless technologies.
- These blurring lines sometimes allow attackers to gain access inside networks while bypassing boundary systems.
- However, even with this blurring of boundaries, effective security deployments still rely on carefully configured boundary defenses that separate networks with different threat levels, sets of users, and levels of control.
- Effective multi-layered defenses of perimeter networks help lower the number of successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary



Critical Control 13: Boundary Defense (T1)

- The boundary defenses included in this control build on Critical Control 10 (Secure Configurations for Network Devices).
- The additional recommendations focus on improving the overall architecture and implementation of both Internet and internal network boundary points.
- Internal network segmentation is central to this control because once inside a network, many intruders attempt to target the most sensitive machines.
- Setting up even a basic level of security segmentation across the network and protecting each segment with a proxy and a firewall will greatly reduce an intruder's access to the other parts of the network.



Critical Control 13: Boundary Defense (T2)

- One element of this control can be implemented using free or commercial IDS and sniffers to look for attacks from external sources directed at DMZ and internal systems, as well as attacks originating from internal systems against the DMZ or Internet.
- Security personnel should regularly test these sensors by launching vulnerability-scanning tools against them to verify that the scanner traffic triggers an appropriate alert.
- The captured packets of the IDS sensors should be reviewed using an automated script each day to ensure that log volumes are within expected parameters and that the logs are formatted properly and have not been corrupted



Critical Control 13: Boundary Defense (M)

- The system must be capable of identifying any unauthorized packets sent into or out of a trusted zone and ensure that the packets are properly blocked and/or trigger alerts.
- Any unauthorized packets must be detected within 24 hours, with the system generating an alert or e-mail for enterprise administrative personnel.
- While the 24-hour timeframe represents the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting.



Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs (S)

- Deficiencies in security logging and analysis allow attackers to hide their location, malicious software used for remote control, and activities on victim machines.
- Even if the victim knows that its system has been compromised, without protected and complete logging records it is blind to the details of the attack and to subsequent actions taken by the attackers.
- Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible.
- Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, so they do not know that their systems have been compromised.



Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs (T)

- Operating systems, network services, and firewall technologies offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers.
- Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required.
- Actual correlation tools can make audit logs far more useful for subsequent manual inspection. Such tools can be quite helpful in identifying subtle attacks.
- Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks.



Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs (M)

- The system must be capable of logging all events across the network. The logging must be validated across both network-based and host-based systems.
- Any event must generate a log entry that includes a date, timestamp, source address, destination address, and other details about the packet.
- Any activity performed on the network must be logged immediately to all devices along the critical path.
- When a device detects that it is not capable of generating logs (due to a log server crash or other issue), it must generate an alert or e-mail for enterprise administrative personnel within 24 hours.



Critical Control 15: Controlled Access Based on the Need to Know (S)

- Some organizations do not carefully identify and separate their most sensitive data from less sensitive, publicly available information on their internal networks.
- In many environments, internal users have access to all or most of the information on the network.
- Once attackers have penetrated such a network, they can easily find and exfiltrate (exportate) important information with little resistance.
- In several high-profile breaches over the past two years, attackers were able to gain access to sensitive data stored on the same servers with the same level of access as far less important data.



Critical Control 15: Controlled Access Based on the Need to Know (T1)

- It is important that an organization understand what its sensitive information is, where it resides, and who needs access to it.
- To derive sensitivity levels, organizations need to put together a list of the key types of data and the overall importance to the organization.
- At a base level, a data classification scheme is broken down into two levels: public (unclassified) and private (classified). Once the private information has been identified, it can then be further subdivided based on the impact it would have to the organization if it were compromised.



Critical Control 15: Controlled Access Based on the Need to Know (T2)

- After determining data sensitivity, the data should be traced back to business applications and the physical servers that house them.
- The network is segmented so that systems of the same sensitivity level are on the same network and segmented from systems with different trust levels.
- If possible, firewalls should control access to each segment. Only encrypted data should flow in a network with a lower trust level.
- For each user group it should be determined the information the group needs to perform its jobs. Based on the requirements, access should only be given to the segments or servers needed for each job. Detailed logging should be turned on for all servers in order to track access and examine situations where someone is accessing data that they should not be accessing



Critical Control 15: Controlled Access Based on the Need to Know (M)

- The system must be capable of detecting all attempts by users to access files on local systems or network-accessible file shares without the appropriate privileges, and it must generate an alert or e-mail for administrative personnel within 24 hours.
- While the 24-hour timeframe represents the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting.



Critical Control 16: Account Monitoring and Control (S)

- Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network watchers. Accounts of contractors and employees who have been terminated have often been misused in this way.
- Some malicious insiders or former employees have accessed accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes



Critical Control 16: Account Monitoring and Control (T)

- Most operating systems can log information about account usage, but these features are sometimes disabled by default or do not provide fine-grained detail about access to the system by default.
- Security personnel can configure systems to record more detailed information about account access, and use home-grown scripts or third-party log analysis tools to analyze this information.
- Accounts must also be tracked very closely. Any account that is dormant must be disabled and eventually removed from the system. All active accounts must be traced back to authorized users of the system. Their passwords should be robust and changed on a regular basis.
- Users must also be logged out after a period of no activity to minimize the probability that an attacker use their system.



Critical Control 16: Account Monitoring and Control (M)

- The system must be capable of identifying unauthorized user accounts when they exist on the system.
- An automated list of user accounts on the system must be created every 24 hours and an alert or e-mail must be sent to administrative personnel within one hour of completion of a list being created.



Critical Control 17: Data Loss Prevention (S)

- Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework.
- Over the last several years, there has been a noticeable shift in attention and investment from securing the network to securing systems within the network, and to securing the data itself.
- DLP controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance.



Critical Control 17: Data Loss Prevention (T)

- Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.
- Deploy an automated tool on network perimeters that monitors for certain sensitive information, keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.
- Conduct periodic scans of server machines using automated tools to determine whether sensitive data is present on the system in clear text. These tools search for patterns that indicate the presence of sensitive information and can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.



Critical Control 17: Data Loss Prevention (M)

- The system must be capable of identifying unauthorized data leaving the organization, whether via network file transfers or removable media.
- Within one hour of a data exfiltration event or attempt, enterprise administrative personnel must be alerted by the appropriate monitoring system.
- Once the alert has been generated it must also note the system and location where the event or attempt occurred. If the system is in the organization's asset management database, the system owner must also be included in the generated alerts.



Critical Control 18: Incident Response and Management (S)

- Considerable damage has been done to organizational reputations and a great deal of information has been lost in organizations that do not have fully effective incident response plans in place.
- Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow proper procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion.
- Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and possibly exfiltrating more sensitive data than would otherwise be possible were an effective incident response plan in place.



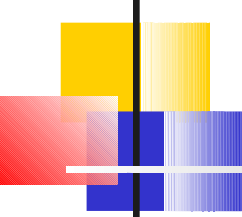
Critical Control 18: Incident Response and Management (T)

- After defining detailed incident response procedures, the incident response team should engage in periodic scenario-based training, working through a series of attack scenarios fine-tuned to the threats and vulnerabilities the organization faces.
- These scenarios help ensure that team members understand their role on the incident response team and also help prepare them to handle incidents.



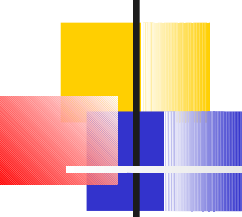
Critical Control 19: Secure Network Engineering (S)

- Many controls in this document are effective but can be circumvented in networks that are poorly designed.
- Without a carefully planned and properly implemented network architecture, attackers can bypass security controls on certain systems, pivoting through the network to gain access to target machines.
- Attackers frequently map networks looking for unneeded connections between systems, weak filtering, and a lack of network separation.
- A robust, secure network engineering process must be employed to complement the other detailed controls being measured.



Critical Control 19: Secure Network Engineering (T1)

- Design the network using a minimum of a three-tier architecture (DMZ, middleware, and private network).
- Any system accessible from the Internet should be on the DMZ, but DMZ systems should never contain sensitive data.
- Any system with sensitive data should reside on the private network and never be directly accessible from the Internet.
- DMZ systems should communicate with private network systems through an application proxy residing on the middleware tier.
- To support rapid response and shunning of detected attacks, engineer the network architecture and its corresponding systems for rapid deployment of new access control lists, rules, signatures, blocks, blackholes, and other defensive measures.



Critical Control 19: Secure Network Engineering (T2)

- Deploy domain name systems (DNS) in a hierarchical, structured fashion, with all internal network client machines configured to send requests to intranet DNS servers, not to DNS servers located on the Internet.
- These internal DNS servers should be configured to forward requests they cannot resolve to DNS servers located on a protected DMZ. These DMZ servers, in turn, should be the only DNS servers allowed to send requests to the Internet.
- Segment the enterprise network into multiple, separate trust zones to provide more granular control of system access and additional intranet boundary defenses.



Critical Control 20: Penetration Tests and Red Team Exercises (S)

- Penetration testing involves mimicking the actions of computer attackers to identify vulnerabilities in a target organization, and exploiting them to determine what kind of access an attacker can gain.
- Penetration tests typically provide a deeper analysis of security flaws than a vulnerability assessment by showing whether and how an attacker can compromise machines, pivot to other systems inside a target organization, and access sensitive information.
- The goals of red team exercises are to improve organizational readiness, improve training for defensive practitioners, and inspect current performance levels. Independent red teams can provide valuable and objective insights about vulnerabilities and the efficacy of defenses and mitigating controls already in place.



Critical Control 20: Penetration Tests and Red Team Exercises (T)

- Each organization should define a clear scope and rules of engagement for penetration testing and red team analyses.
- The scope of such projects should include, at a minimum, systems with the organization's highest value information and production processing functionality. Other lower-value systems may also be tested to see if they can be used as pivot points to compromise higher-value targets.
- The rules of engagement for penetration tests and red team analysis should describe, at a minimum, times of day for testing, duration of tests, and the overall test approach.