SYNERCOMM
SECURE • INTELLIGENT • NETWORKS

CIS Top 20 #5

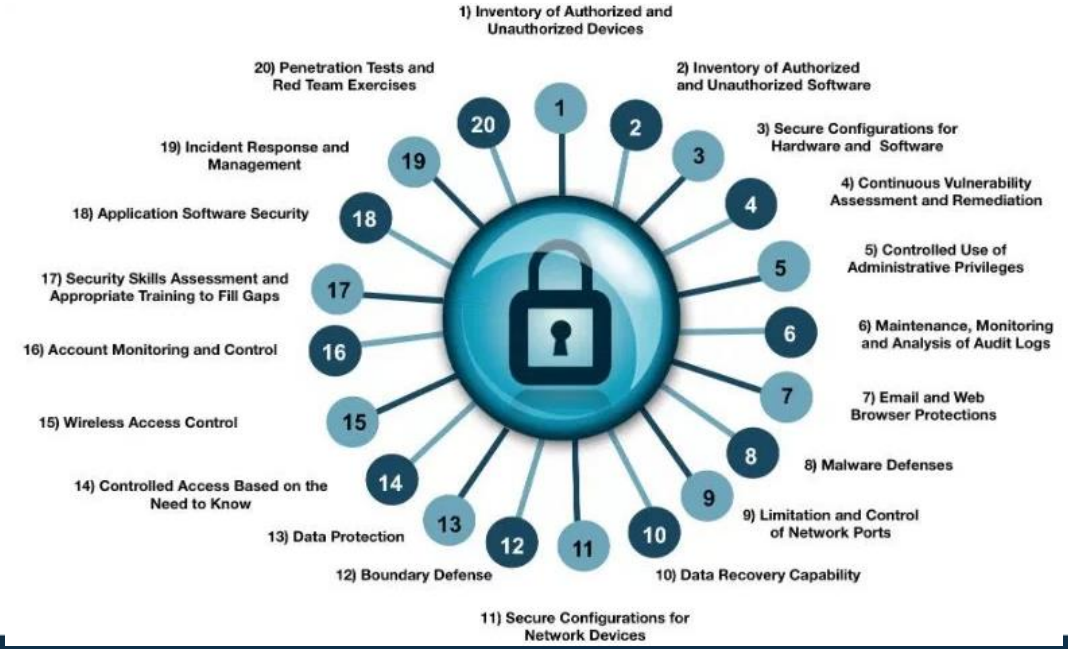
Controlled Use of Administrative Privileges

3265 GATEWAY ROAD, SUITE 650 BROOKFIELD, WI 53045 / P: 262.373.7100 / INFO@SYNERCOMM.COM / SYNERCOMM.COM

CIS Top 20 Critical Security Controls

CIS Top 20 Critical Security Controls

CIS CSC #5: Controlled use of administrative privileges



CIS Top 20 Critical Security Controls

CIS Top 20 Critical Security Controls

CIS Top 20 Critical Security Controls

75% of Hackers Say Privileged Accounts Are Still ... - Dark Reading
https://www.darkreading.com/.../75...hackers...privileged-accounts.../1321791?
Aug 18, 2015 - WASHINGTON, D.C. – August 17, 2015 – Thycotic, a provider of smart and effective **privileged account** management solutions for global organizations, today announced the results of a survey of 201 white hat and black hat **hackers** at Black Hat USA 2015. The survey, which was conducted live on August ...

Dissecting the Make-Up of a Privileged Account Hack - SecureWorld
https://www.secureworldexpo.com/.../dissecting-the-make-up-of-a-privileged-account...
Sep 5, 2017 - Industry analysts estimate that from 60 to 80 percent of all security breaches now involve the compromise of user and **privileged account** passwords. In fact, a **recent** survey of **hackers** attending the 2017 Black Hat conference in Las Vegas, revealed that compromising **privileged accounts** and email accounts ...

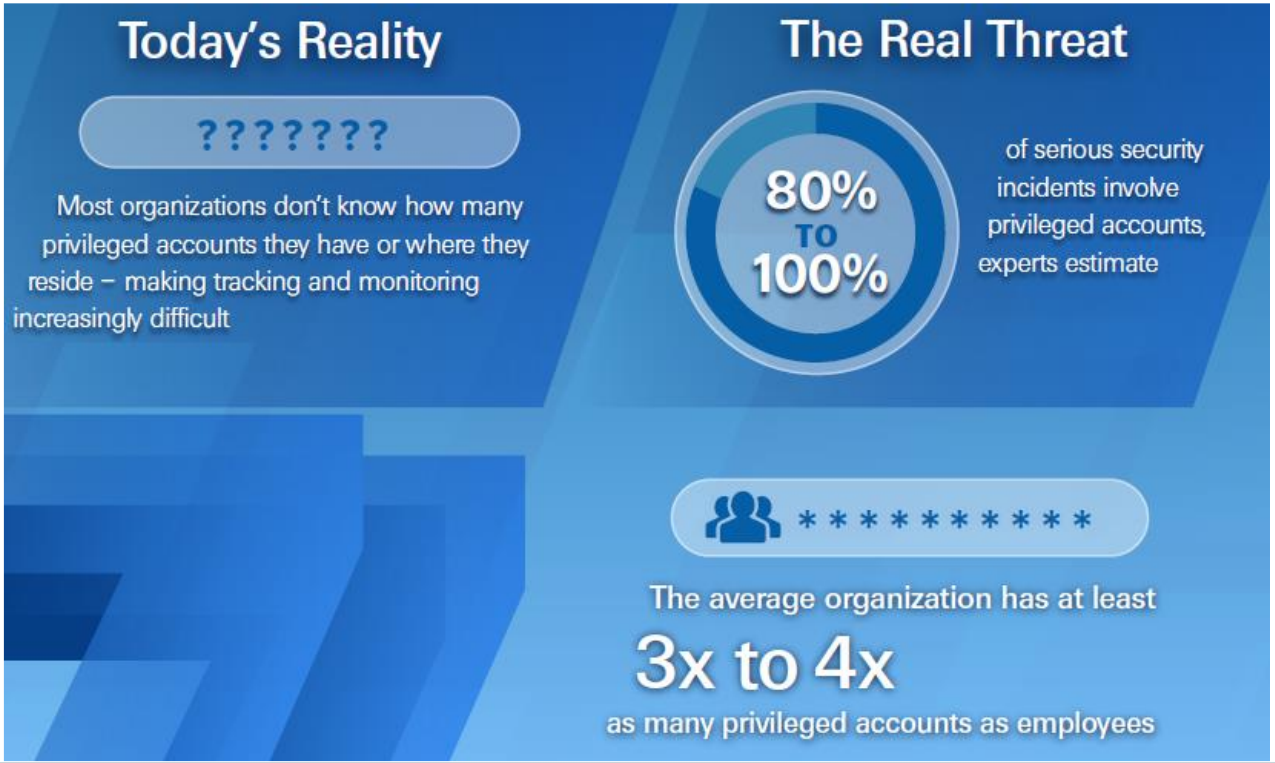
Privileged-account attacks are behind every major cyber crime - Data ...
https://blog.code42.com/privileged-account-attacks-are-behind-every-major-cyber-cri...
Jan 8, 2016 - In other cases, cyber criminals steal or **hack** all-access credentials, as was the case with the 2013 Target and the 2014 Home Depot breaches. Regardless of the cause, studies of major breaches find that 100 percent of cyber crime attacks exploit privileged credentials. Two factors make **privileged-account** ...

Hackers See Privileged Accounts as Best Route to Sensitive Data ...
https://www.infosecurity-magazine.com/news/hackers-see-privileged-accounts/
Aug 14, 2017 - When it comes to what works and doesn't work for protecting critical data, nearly one third (32%) of respondents at the **recent** Black Hat conference said that accessing **privileged accounts** was the number one choice for the easiest and fastest way to get access to critical data. The survey, carried out by ...

88 Percent of Networks Susceptible to Privileged Account Hacks ...
https://threatpost.com/88-percent-of-networks...privileged-account-hacks/115314/
Nov 10, 2015 - Researchers with the Massachusetts-**based** firm connected the dots between **privileged accounts** and their networks and determined that for some networks, if a ... By and large, the majority of networks CyberArk looked at, 88 percent, were susceptible to being **hacked** through privileged credentials. Only 12 ...

Privileged identities are at the core of today's cyber attacks

CIS Top 20 Critical Security Controls



CIS Top 20 Critical Security Controls

CIS Top 20 Critical Security Controls

CIS Top 20 Critical Security Controls

- What is a privileged Account?

CIS Top 20 Critical Security Controls

- Why are they Dangerous?

CIS Top 20 Critical Security Controls

- What can we do about it?

CIS Top 20 Critical Security Controls

How to Get Started

Step 1. Gap Assessment.

2. Implementation Roadmap
3. Implement the First Phase of Controls
4. Integrate Controls into Operations
5. Report and Manage Progress

CIS Top 20 Critical Security Controls

Develop Privileged User Access Management	Does your Agency grant privileged user access (e.g. access that allows the user to make mass changes such as system, network, database admins)following a formal approval process involving an information security officer / similar designated role?
	Is the approval granted to individuals based on documented business need and role requirements?
	Does the Agency control, monitor and report privileged accounts periodically?
Develop User Access Account Review Cycles	Does your Agency conduct reviews of user accounts periodically to ensure that: ➢ Access levels remain appropriate ➢ Terminated employees do not have active accounts ➢ Group accounts exist, if approved ➢ No duplicate user identifiers
	If the Agency conducts period reviews, is there a defined schedule?
	Does your Agency review information system accounts within every 180 days?
	In addition, does your Agency require information system accounts be to recertified annually?

CIS Top 20 Critical Security Controls

Implement Separation of Duties	Does your Agency enforce separation of duties for access controls through assigned access authorizations, some of which are noted below? ➢ Audit function and information system access administration; ➢ Management of critical business and information systems; ➢ System testing and production; ➢ Independent entity for information system security testing.
Develop the process of Least Privilege	Has your Agency implemented a process to: a) Disable file system access not explicitly required b) Provide minimal physical and system access to contractors c) Require contractors' access policy compliance d) Grant role-based-access e) Disable systems and removable media boot access unless authorized by the CIO If authorized, boot access must be password protected

CIS Top 20 Critical Security Controls

- Security Model Level - Basic

- Manual processes for managing privileged passwords, including spreadsheets, physical safes
- Local administrator access on their machines
- Individual vulnerability patching, management, and inconsistent policies by application
- Lack of auditing and control over root and privileged accounts
- No session monitoring or recording of privileged use
- No singular, clear picture of threats or what to do about them
- Disorganized and chaotic directory services infrastructure, with multiple logons required, and inconsistent policy
- No visibility over changes made to AD objects, configurations, or permissions;
- Always reacting

CIS Top 20 Critical Security Controls

- **Progressing**
- Some automation and some cycling of some privileged passwords
- 50% or fewer users with administrator credentials in the organization
- More automated scanning on vulnerable systems
- Common use of the root account, with some auditing of usage, perhaps sudo
- Some session monitoring for compliance purposes, snapshotting
- Threat analytics mostly from SIEMs
- Few (but not one) logins to heterogeneous systems
- Some change auditing, but lacking recovery of unwanted changes

CIS Top 20 Critical Security Controls

- **Advanced**
- Automated password and session management of all shared accounts
- Rules-based least privilege implemented organization-wide, on all systems
- Automated scanning, patching, and reporting of vulnerable systems
- Full control and accountability over privileged users on any system, eliminating root access or insufficient methods like sudo
- Automatic recording of keystrokes/video/over-the-shoulder activities
- Integrated threat analytics to improve decision-making
- Single sign on for heterogeneous systems leveraging familiar infrastructure
- Full auditing and recovery of changes across the environment; Ability to proactively know and deliver what auditors are looking for

CIS Top 20 Critical Security Controls

- However, before you can start protecting privileged user and application accounts, you must first be able to find them, which can be incredibly difficult.

CIS Top 20 Critical Security Controls

- CSC 5.1 Run automated Privileged Account scanning tools against all systems on the network on a monthly basis
- CSC 5.1 Procedure: Scan entire network monthly for Privileged and shared accounts
- The organization:
  - IT department to run scan monthly
  - IT department will review scan logs for completeness
  - Metrics:
  - IT department will report in new administrator level accounts
  - The IT department will audit SIEM logs daily for authentication successes and failures of administrative accounts

CIS Top 20 Critical Security Controls

- Step 1: Improve Accountability and Control Over Privileged Passwords

CIS Top 20 Critical Security Controls

- Step 2: Implement Least Privilege, Application Control for Windows & Mac Desktops

CIS Top 20 Critical Security Controls

- Step 3: Leverage Application-Level Risk to Make Better Privilege Decisions

CIS Top 20 Critical Security Controls

- Step 4: Implement Least Privilege in Unix & Linux Environments

CIS Top 20 Critical Security Controls

- Step 5: Unify Management, Policy, Reporting, and Threat Analytics

CIS Top 20 Critical Security Controls

- Step 6: Integrate Unix, Linux, and Mac into Windows

CIS Top 20 Critical Security Controls

- Step 7: Real-Time Change Auditing and Recovery for Windows Environments

CIS Top 20 Critical Security Controls

5.1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.
5.2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.
5.3	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.
5.4	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.
5.5	Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.
5.6	Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards,-certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.
5.7	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).
5.8	Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.
5.9	Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

CIS Top 20 Critical Security Controls

- AUTHOR NOTE! With the recent vulnerability disclosures of Kerberos Golden & Silver tickets, this section is particularly important!
- *5-1 - Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.*
- This is pretty standard in Linux. You crazy Windows users need to stop setting everyone as local admin. At the VERY least, create a second account for them to use when needing to perform admin tasks, and disable login from those account through group policy.
- RunAsSPC - While not an application whitelist, it can allow users to run applications which require elevation
- Use your SIEM to monitor
- Commercial Tools
- PowerBroker - Powerful tool to escalate privileges and take care of pesky UNC. Solution for Windows and Linux.
- PolicyPak - Integrates with Group Policy
- Centrify Server Suite - Windows and Linux application and Privilege control.

CIS Top 20 Critical Security Controls

- *5 -2 - Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.*
- Windows security event log can be monitored to detect real-time changes to the administrators group on workstations, servers, and privileged domain security groups.
- SCCM
- Viewfinity by CyberArk
- PowerBroker by BeyondTrust
- Secret Server by Thycotic
- Centrify Privilege Account Suite

CIS Top 20 Critical Security Controls

- *5-3 - before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.*
- Rapid7 - Nexpose & IoT seeker
- Tenable –Nessus
- can scan for default accounts on many types of common systems

CIS Top 20 Critical Security Controls

- *5-4 - Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.*
- **Free Tools**
- Netwrix - AD Change Reporter Free, One of the most simple setups I have ever performed. But, you MUST read the user guide that comes with the download file. There are some pre-requisites that must be met.
- Scripted - Alternative to using 3rd party software. Easy to follow guide.
- GPO - Only enables logging, you still need to alert
- **Commercial Tools**
- ADAuditPlus - ManageEngines real time monitor and alerting tool
- Netwrix also offers commercial versions of their free tool above.

CIS Top 20 Critical Security Controls

- *5-5 - Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.*
- One consideration, you have more than just domain admin and local admin accounts you should worry about. You have Schema Admins, Enterprise Admins, SQL admins, Spiceworks admins, IIS Admins, Switch Admins... ANY admin account on any device/application should be monitored.
- Free Tools
- If you enable logging on your domain controllers, the logging is taken care of. You now need something that can report on these logs. SEIM comes to mind
- Splunk - There is a discussion on their community regarding this feature.
- Commercial Tools
  The above listed tool has a commercial versions too

CIS Top 20 Critical Security Controls

- *5-6 - Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.*
- **Free Tools**
- FreeRADIUS - This is the poor-man's RSA token. But, it works.
- Authy - 2 factor authentication
- **Commercial Tools**
- Centrify
- Okta
- BeyondTrust

CIS Top 20 Critical Security Controls

- *5-7 - Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.***Where MFA is not used*
- Tools
- While you're at it, mitigate pass-the-hash attacks with the following tool:
- LAPS - Randomize each local admin account's password and store is securely in Active Directory. Can be deployed through GPMC.

CIS Top 20 Critical Security Controls

- *5-8 - Block access to a machine (either remotely or locally) for administrator-level accounts. Instead, administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.*
- ****AUTHOR NOTE! You should also deny logons to your service accounts, but grant them the "log on as a service" right in Group Policy.
- Tools
- GPO - Deny logons to specific groups/users

CIS Top 20 Critical Security Controls

- *5-9* - Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.
- Tools
- Centrify Jumpbox

CIS Top 20 Critical Security Controls

- *Note - Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800-132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super-user privileges.*
- You can monitor these files, and access attempts with a good HIDS (CSC 5-2).

CIS Top 20 Critical Security Controls

Top privileged password management tool capabilities to look for:

1. Full network scanning, discovery, and profiling with auto-onboarding
2. Builds permission sets dynamically according to data from scans
3. Automatically rotates SSH keys and cycles passwords according to a defined schedule
4. Provides granular access control, workflow, and auditing
5. Workflow-based and break glass options for requesting access
6. Password and session management integrated within the same solution – no requirement for two different interfaces, or to be charged separately for each
7. Leverages an integrated data warehouse and threat analytics across the privilege landscape
8. Flexible deployment options: hardware appliances, virtual appliances, or software

CIS Top 20 Critical Security Controls

- A few general best practices to consider as well
  - Remove local admin accounts
  - Enforcing context-aware multifactor authentication
  - Consolidating identity stores into a single directory
  - Implementing single sign-on
  - Conducting periodic access review for administrative and privileged users
  - Limiting access for remote identities to just the applications or systems they immediately require
  - Governing access through time-bound and temporary privileged access
  - Automating role-based provisioning and deprovisioning to apps and infrastructure
  - Automating mobile app provisioning and deprovisioning
  - Automatically deprovisioning privileged users' access rights in high-risk environments when they terminate
  - Implementing least-privilege access for administrators
  - Centrally controlling access to shared and service accounts
  - Eliminating shared administrative accounts
  - Managing privileged access at the granular command or app level
  - Actively monitoring all privileged sessions and commands
  - Recording all privileged sessions and commands

CIS Top 20 Critical Security Controls

- Center for Internet Security (CIS): https://www.cisecurity.org/
- NIST Cyber Security Framework (CSF): http://www.nist.gov/cyberframework/
- CIS Critical Security Controls (CSC): https://www.cisecurity.org/critical-controls.cfm
- Auditscripts resources (provided by James Tarala, CSC Editor): https://www.auditscripts.com/free-resources/critical-security-controls/
- STIG https://iase.disa.mil/stigs/Pages/index.aspx

CIS Top 20 Critical Security Controls

- SynerComm's IT Summit
- April 9-10th
- Lambeau Field, Green Bay, WI
- Validate Your IT Strategy
- FREE!!
- Register: www.events.synercomm.com

CIS Top 20 Critical Security Controls

Thank you for Attending.

Hope you can join us for the Complete CIS Top 20 CSC

Tuesday April 3rd

CIC CSC #6
Maintenance, Monitoring, and Analysis of Audit Logs