NIST - Protect

Protect (PR)

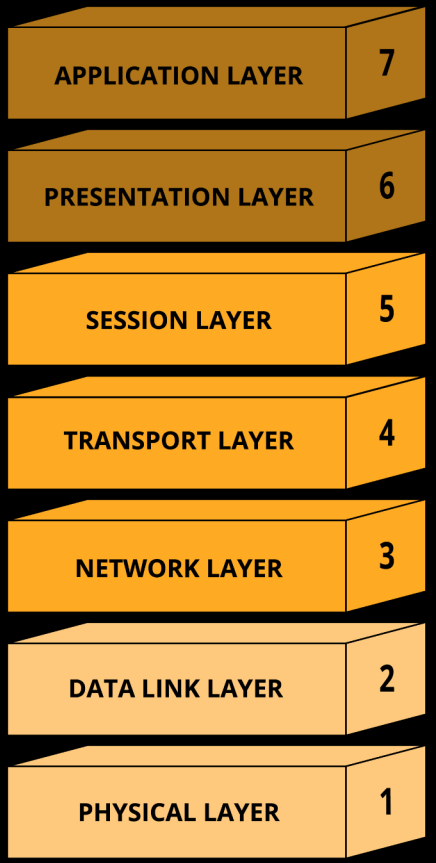
- NIST Definition: Safeguards to manage the organization’s cybersecurity risks are used. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities.
- Safeguarding an organization’s assets against threats
- Implementation of security measures designed to mitigate unauthorized access, disclosure, alteration, distribution, and destruction of data.
- Ensuring Confidentiality, Integrity, and availability (CIA-Triad)
- What are some tools and actions we may implement to protect our assets?

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

CIA Triad

https://www.energy.gov/femp/operational-technology-cybersecurity-energy-systems

OSI Model



— Human-computer interaction layer, where applications can access the network services

— Ensures that data is in a usable format and is where data encryption occurs

— Maintains connections and is responsible for controlling ports and sessions

— Transmits data using transmission protocols including TCP and UDP

— Decides which physical path the data will take

— Defines the format of data on the network

— Transmits raw bit stream over the physical medium

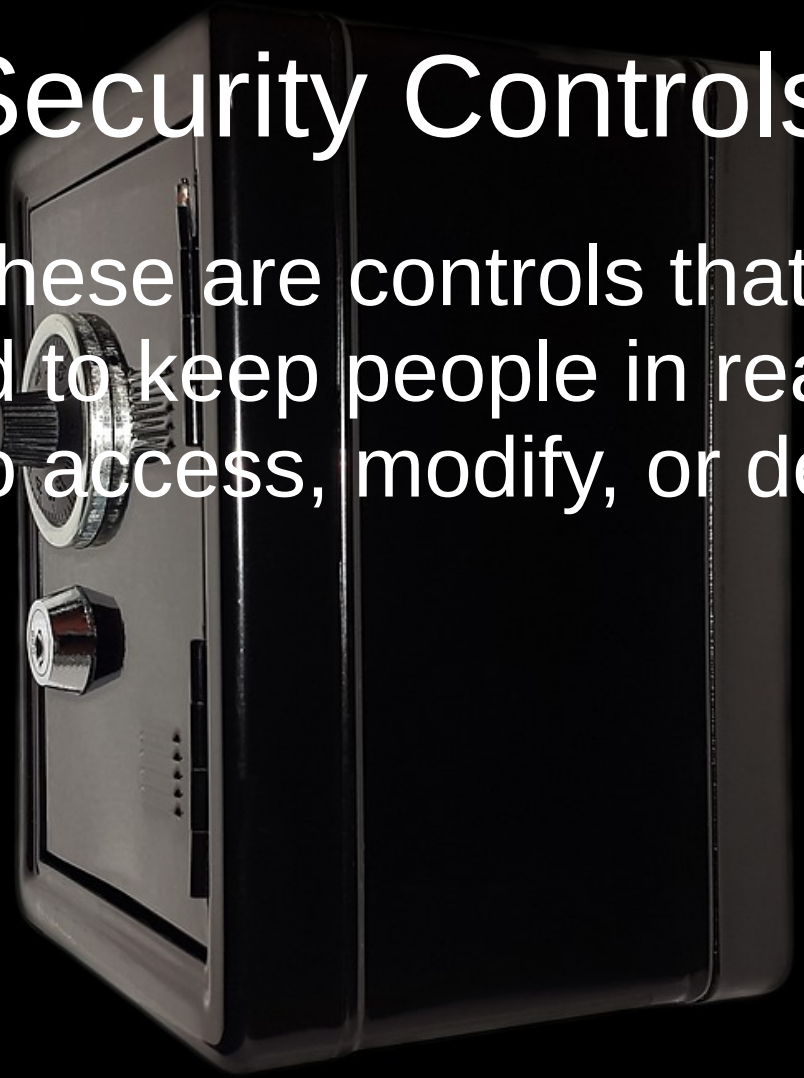
https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

Security Controls

- Technical – Probably the first type of control we tend to think of working in IT. These are controls we enforce through the use of technology; our hardware and software systems we have implemented on our network.

Security Controls

- Physical – These are controls that are implemented to keep people in real space from being able to access, modify, or destroy our assets.



Security Controls

- Administrative – These are controls that are put in place and enforced via policies and procedures… No you can’t take that $20,000 server home to work on it… That violates company policy 42 section IV subsection B

Security Controls

		CONTROL FUNCTIONS		
		Preventative	**Detective**	**Corrective**
CONTROL TYPES	**Physical**	Fences, gates, locks	CCTV and surveillance camera logs	Repair physical damage, re-issue access cards
	Technical	Firewall, IPS, MFA solution, antivirus software	Intrusion detection systems, honeypots	Patch a system, terminate a process, reboot a system, quarantine a virus
	Administrative	Hiring and termination policies, separation of duties, data classification	Review access rights, audit logs, and unauthorized changes	Implement a business continuity plan or incident response plan

https://www.f5.com/labs/learning-center/what-are-security-controls

Protecting Data at Rest and in Flight

- Questions to consider:
  - Where is data stored both physically and logically?
  - How is data transmitted?
  - How is our data being handled internally and by 3rd parties?
  - Who should have access to what data?
    - Principle of least privilege – only access necessary to complete a job
  - Are access logs in place and working ?
- What is a use case for encryption and hashing?

What to do in Protection

- Cybersecurity awareness training
- Penetration testing/threat hunting
- Resilience (Incident Response plans, playbooks, workshops)
- Patching and Upgrading systems
- Improving workflows
- Reviewing rule-sets on systems like email
- And much much more!

Patches and Updates

- Patch Tuesday!
  - This is an unofficial day, usually the second Tuesday of the month, when companies release patches and updates for their software
- Any idea what the following Wednesday is called?
- In a Windows environment what tool on the domain controller may I use to control how updates are handled?


Windows Update
Patches and Updates
You're up to date
Last checked: Today, 9:59 AM
Check for updates
More options
Get the latest updates as soon as they're available
Be among the first to get the latest non-security updates, fixes, and improvements as they roll out. Learn more
On
Pause updates
Pause for 1 week
DEMO
Update history
Advanced options
Delivery optimization, optional updates, active hours, other update settings
Windows Insider Program
Get preview builds of Windows to share feedback on new features and updates
Windows Update is committed to helping reduce carbon emissions. Learn more
Get help
Give feedback

Detect

- NIST Definition: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- We need to know when a security event, incident, or anomaly has occurred.

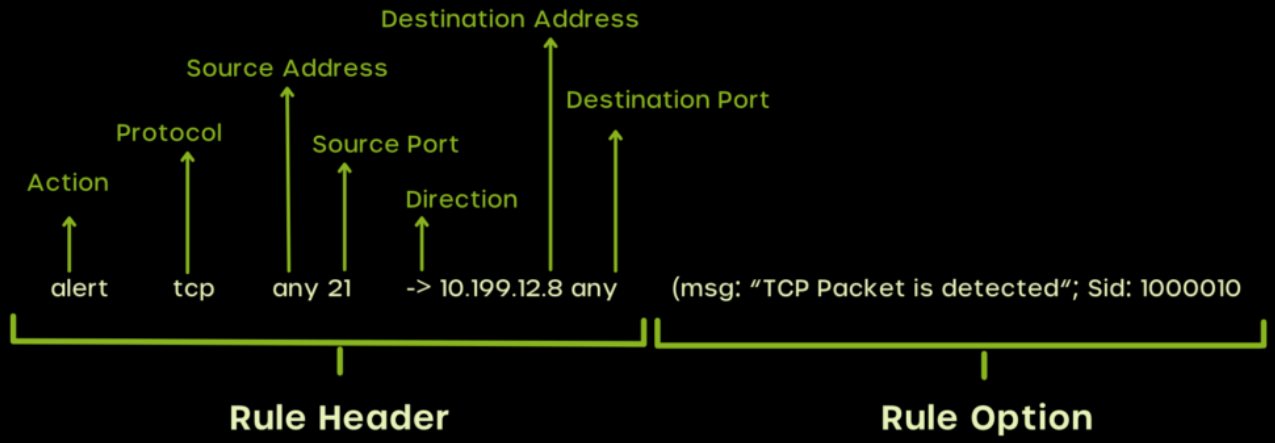
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Detection Methods

- What are some indicators of compromise?
- What activities or events may tip us off that we have been compromised?
- What sources can we lean on to learn about a breach?

SNORT

- Widely used, open-source Intrusion Detection/Prevention System



https://cyvatar.ai/write-configure-snort-rules/

https://www.snort.org/

Snort Cheat Sheet

Sniffer Mode

Sniff packets and send to standard output as a dump file

-v (verbose)	Display output on the screen
-e	Display link layer headers
-d	Display packet data payload
-x	Display full packet with headers in HEX format

Packet Logger Mode

Input output to a log file

-r	Use to read back the log file content using snort
-l (directory name)	log to a directory as a tcpdump file format
-k (ASCII)	Display output as ASCII format

Snort Rules Format

Rule Header + (Rule Options)

Action - Protocol - Source/Destination IP's - Source/Destination Ports - Direction of the flow

Alert Example	alert udp !10.1.1.0/24 any -> 10.2.0.0/24 any
Actions	alert, log, pass, activate, dynamic, drop, reject, sdrop
Protocols	TCP, UDP, ICMP, IP

Snort Rules Example

log tcp !10.1.1.0/24 any -> 10.1.1.100 (msg: "ftp access";)

NIDS Mode

Use the specified file as config file and apply rules to process captured packets

-c	Define configuration file path
-T	Use to test the configuration file including rules

Logger Mode command line options

-l logdir	Log packets in tcp dump
-K ASCII	Log in ASCII format

NIDS Mode Options

Define a configuration file	-c (Configuration file name)
Check the rule syntax and format for accuracy	-T -c (Configuration file name)
Alternate alert modes	-A (mode: Full, Fast, None, Console)
Alert to syslog	-s
Print alert info	-v
Send SMB alert to PC	-M (PC name or IP address)
ASCII log mode	-K
No logging	-N
Run in Background	-D
Listen to a specific network interface	-i

Output Default Directory

/var/snort/log

https://cyvatar.ai/write-configure-snort-rules/

- SNORT
- https://resources.infosecinstitute.com/topics/penetration-testing/snort-rules-workshop-part-one/
- rules stored:
- /etc/snort/rules/
- config add ruleset (section 7):
- nano /etc/snort/snort.conf
- Rule to create in sera.rules:
- alert icmp any any -> 8.8.8.8 any (msg:"GOOGLE PING DETECTED!"; SID: 500000001337;)
- validate config:
- sudo snort -T -i eth0 -c /etc/snort/snort.conf
- Run Snort:
- sudo snort -A console -q -c /etc/snort/snort.conf -i eth0