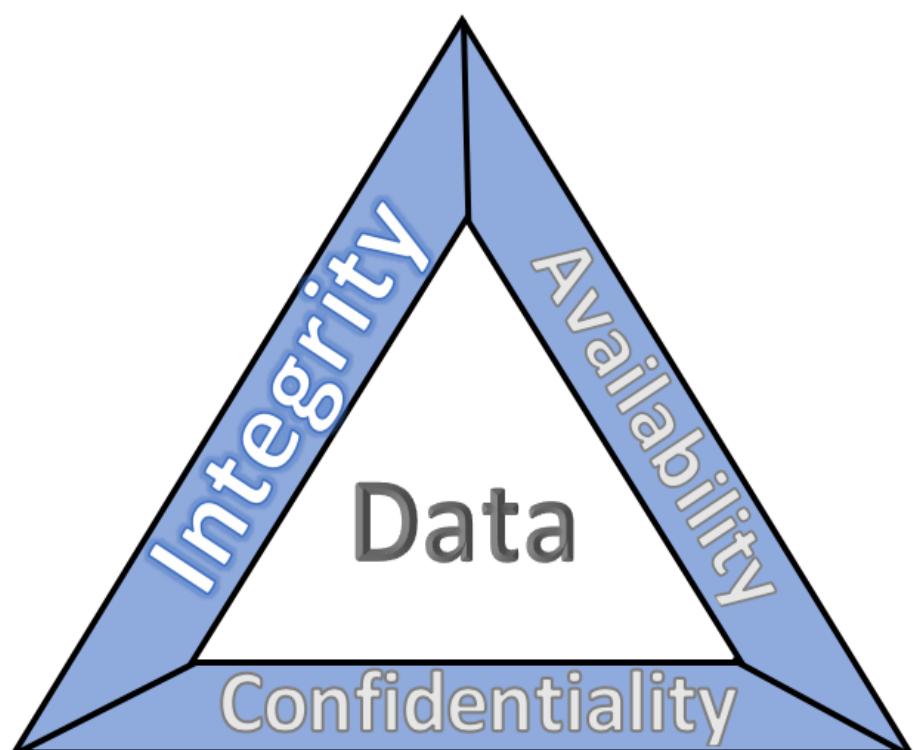


# Threats, Vulnerabilities, and Risks... Oh my!



**SECTIGO WEB**  
SECURITY PLATFORM

What is the difference between  
a threat, a vulnerability, and a risk?



**Threat:**  
Something  
that can damage  
or destroy an  
asset



**Vulnerability:**  
A weakness  
or gap in  
your  
protection



**Risk:**  
Where assets,  
threats, and  
vulnerabilities  
intersect

# Agenda

- CIA – No, not the feds
- Threats
- Vulnerabilities
- Risks
  - Math – Not really so much



# CIA

- **Confidentiality** – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- **Integrity** — guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity
- **Availability** – ensuring timely and reliable access to and use of information

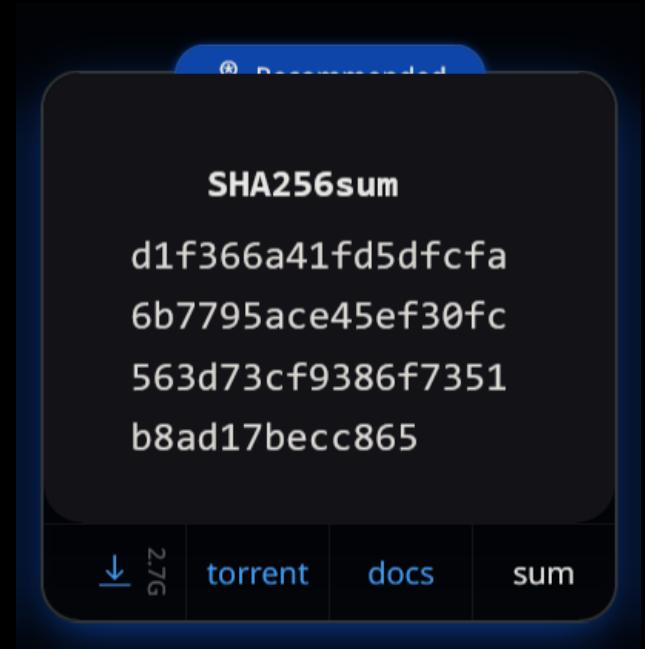
# Confidentiality

- Ensuring only authorized people can access data
- Encryption technology
- Credential Access
- NDAs, policies, etc.



# Integrity

- Guarantee the data you have is what was intended
- Hashing algorithms
- Non-repudiation - Authenticity



# Availability

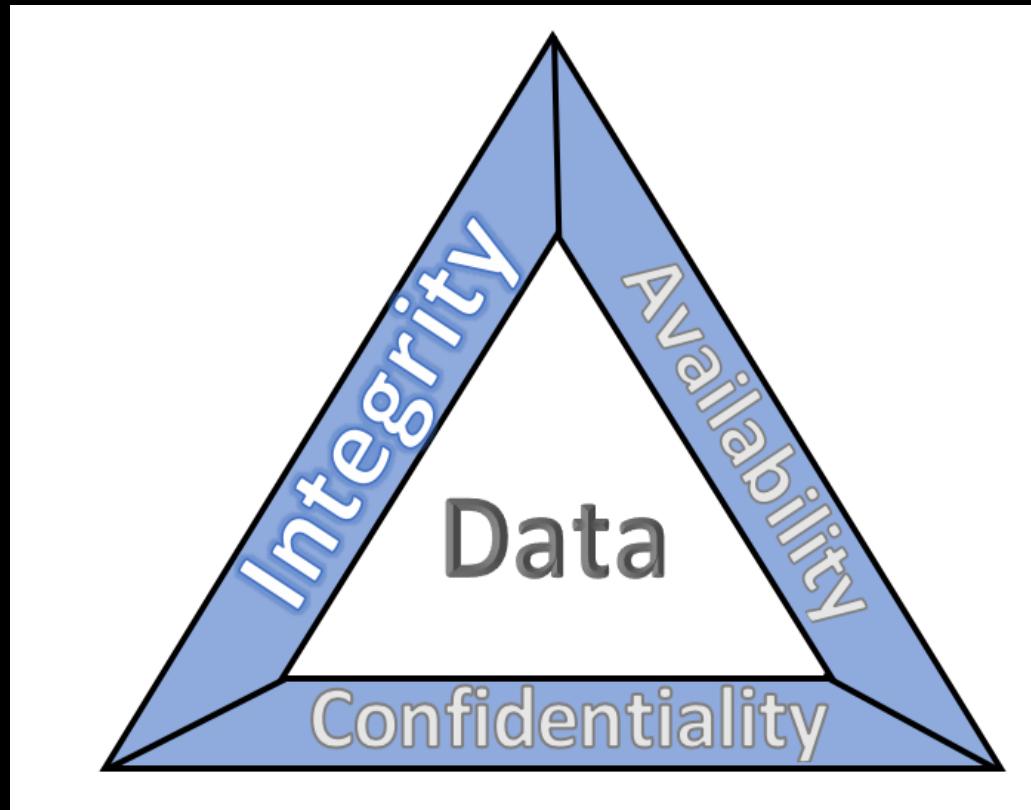
- Ensuring data is actually there for users to access
- Service up-time
- In a timely manner
- Backups and redundant systems
- TCP and other protocols



Wireshark capture window showing network traffic on \*vEthernet (WSL). The table lists network packets with columns for Source, Destination, Protocol, and Info.

Source	Destination	Protocol	Info
Microsof_71:39:ad	Broadcast	ARP	Who has 172.23.192.1? Tell 172.23.198.66
Microsof_92:b9:56	Microsof_71:39:ad	ARP	172.23.192.1 is at 00:15:5d:92:b9:56
172.23.198.66	172.23.192.1	DNS	Standard query 0x9b36 A google.com
172.23.198.66	172.23.192.1	DNS	Standard query 0x6648 AAAA google.com
172.23.192.1	172.23.198.66	DNS	Standard query response 0x9b36 A google.com A 142.251.214.142
172.23.192.1	172.23.198.66	DNS	Standard query response 0x6648 AAAA google.com AAAA 2607:f8b0:4000:1::1
172.23.198.66	142.251.214.142	TCP	51412 → 80 [SYN] Seq=0 Win=64446 Len=0 MSS=1401 SACK_PERM TSval=4023194659 T
142.251.214.142	172.23.198.66	TCP	80 → 51412 [SYN, ACK] Seq=0 Ack=1 Win=65353 Len=0 MSS=1286 SACK
172.23.198.66	142.251.214.142	TCP	51412 → 80 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=4023194659 T
172.23.198.66	142.251.214.142	HTTP	GET / HTTP/1.1
142.251.214.142	172.23.198.66	TCP	80 → 51412 [ACK] Seq=1 Ack=75 Win=65536 Len=0 TSval=2260854399 T
142.251.214.142	172.23.198.66	HTTP	HTTP/1.1 301 Moved Permanently (text/html)
172.23.198.66	142.251.214.142	TCP	51412 → 80 [ACK] Seq=75 Ack=774 Win=64256 Len=0 TSval=4023194779 T
172.23.198.66	142.251.214.142	TCP	51412 → 80 [FIN, ACK] Seq=75 Ack=774 Win=64256 Len=0 TSval=4023194779 T
142.251.214.142	172.23.198.66	TCP	80 → 51412 [FIN, ACK] Seq=774 Ack=76 Win=65536 Len=0 TSval=2260854399 T
172.23.198.66	142.251.214.142	TCP	51412 → 80 [ACK] Seq=76 Ack=775 Win=64256 Len=0 TSval=4023194892 T

# CIA is a Balancing Act



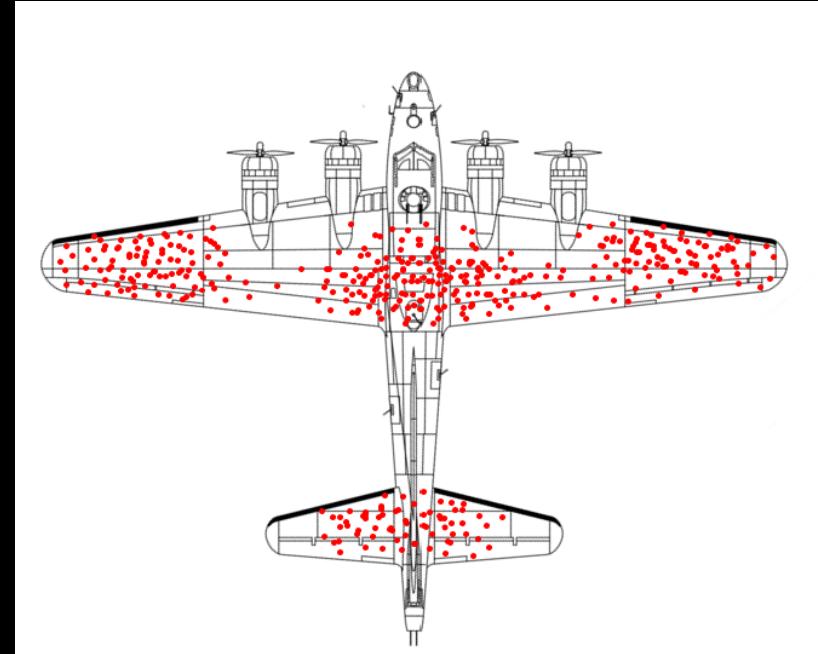
# Threats

- Anything that \*CAN\* cause harm to a system
- Natural
- Unintentional
- Malicious
- Who or what is threatening us?
- APTs, Employees, hacktivists, script kiddies



# Vulnerabilities

- Weak points in our attack surface
- Outdated systems, bad policy and procedures, poor user habits
- What are the vulnerable areas on this airplane?



# Risks

- Risk = (Threats \* Vulnerabilities \* Probability \* Impact)/Countermeasures
- How bad is it if we are compromised?
- Risk tolerance - The level of risk an entity is willing to assume in order to achieve a potential desired result.

<https://www.sans.org/blog/insider-threat-risk-formula-survivability-risk-and-threat/>

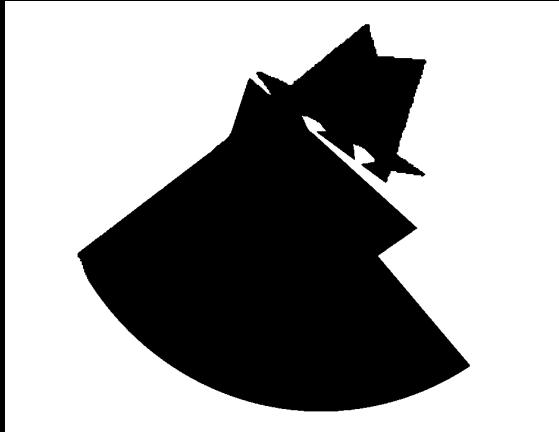
[https://csrc.nist.gov/glossary/term/risk\\_tolerance](https://csrc.nist.gov/glossary/term/risk_tolerance)

# All Together now

Vulnerability



Threat



Risk

