Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

IT Security: "Safeguards" to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.

Cybersecurity: The ability to protect or defend the use of cyberspace from cyberattacks

Cyber Attack: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information

Cyberspace: A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers

CISSP: Certified Information Systems Security Professional

Security professional: A strategic thinker able to interpret the changing threat landscape, understand the implications of changing technology, and enable the business to achieve it's goals.

Top certifications in-demand
- CISSP
- CISM
- CISA

Penetration testing focused
- CEH
- LPT
- GPEN
- OSCP

If a beginner
- CompTia Security+
- ISACA CSX
- SSCP

Certifications

CSX:F	Cybersecurity Fundamentals Certificate
CISSP	**Certified Information Security Professional**
CISA	**Certified Information Systems Auditor**
CISM	**Certified Information Security Manager**
PCI QSA	PCI Qualified Security Assessor
CCSP	Certified Cloud Security Professional
GSEC	GIAC Security Essentials
Security+	CompTIA Security+
C|EH	Certified Ethical Hacker
LPT	Licensed Penetration Tester

University of Victoria also GPEN, OSCP

Highest profile breaches could have been prevented with one or more of the following:

1) Security Awareness
2) Patching
3) Offline Backups
4) Password Management
5) Supply Chain Security

Key points
- Incidents are increasing in frequency, more sophisticated, and more targeted than ever
- No organization is immune to attack
- Organizations will be judged not only on their ability to prevent but detect and respond
- Doing the basics well will stop 80% of the problems
- Security is not just an IT problems

Cyber attacks are more
- Frequent
- Effective
- Targeted
- Sophisticated
- Profitable
- Elusive

Why organizations are targeted
- Gain economic advantage
- Access to financial or personal data, for fraud/identity theft
- Take over systems as launch point against others
- Retribution or make a statement
- Cause damage or distraction
- Surveillance

Business impacts
- Direct impact to clients
- Disruption of operations
- Financial
- Litigation
- Data breach and loss
- Brand and reputation
- Lost/stolen intellectual property

Attack vectors/methods

- phishing, smishing, vishing, social engineering, spearphishing, whaling
- malware, cryptoware, ransomware, scareware, malvertising, waterholing, pharming
- weak/no passwords/brute force
- supply chain/vendors/partners
- distributed denial of service (DDoS)
- poor coding hygiene (SQL inject, buffer overflow)
- exploiting other vulnerabilities

CIA Triad *

- **confidentiality**
  the property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- **integrity**
  maintaining and assuring the accuracy and completeness of data over its entire life-cycle
- **availability**
  preventing service disruptions due to power outages, hardware failures, and system upgrades; also preventing denial-of-service attacks

Triple A

- Authentication: Grants access
- Authorization: Determines permissions
- Accounting: Ensures logging

Five tenets

- **strong authentication**: more than one type of authentication (two-factor)
- **least privilege**: individual, program, or system is not granted any more information than necessary to perform the task
- **non-repudiation**: one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction
- **separation of duties**: ensures that an individual can not complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check.
- **defense in depth**: layering on and overlapping of security measures is called defense in depth - the strength of any system is no greater than its weakest link - the failure of any one defensive measure should not cause failure of the system

Challenges

- more connected and dependent on networks, systems, and data than ever
- despite awareness efforts, devices released with little to no security
- not getting through to users effectively
- broad misunderstanding of the impacts of not taking security seriously
- belief that security is an IT problem
- significant shortage of talent

Security Technology

- firewalls, VPN
- intrusion detection/prevention
- web content filtering
- email content filtering
- DDoS prevention
- Security Information and Event Management (SIEM)
- … and more

Types of Security Controls

- **administrative**: written policies, procedures, standards and guidelines
- **logical**: (technical controls) use data, software, and hardware to control access to information and computing systems
- **physical**: monitor and control the environment of the work place and computing facilities

Ransomware

- common type of cyber attack is ransomware
- data is encrypted by malware contained in websites and email attachments
- attacker demands payment to provide keys to decrypt data
- organizations with backups can restore files and avoid paying

Extortionware

- attackers realized if organizations have backups they are unlikely to pay
- new malware encrypts the data but sends a copy of the data to the attacker first (breach)
- attacker threatens to post data online if organization doesn't pay
- backups are insufficient and organization may need to pay

Best Practices

- Remember different kinds of controls
  - administrative, procedural — eg. policies, standards
  - technical, logical — eg. firewalls
  - physical — eg. fences
- COBIT (good practice framework)
- ITIL (IT Service Management)
- NIST (cybersecurity framework)
- ISO/IEC 27001 (information security standard)
- ISO/IEC 27002 (information security standard)

Hygiene Controls (procedural)

Security Controls	
Information Security Policy	Identify what employees may and may not do that will impact risk to systems and data
Risk Register	Conscious identification and treatment of physical and logical risks to systems and data
Risk Assessments	Review risk each time a new system is introduced or upon material change to an existing system
Incident Response Plan	Respond to inevitable security incidents in a consistent and scalable way
Incident Response Team	Team that is dedicated, virtual, or on retainer with third party provider to respond to security incidents
Security Education and Awareness	Humans represent the easiest method for attackers to gain unauthorized access to systems and data

109

Hygiene Controls (technical)

Security Controls	
Firewall	Modern version designed to prevent illegitimate network traffic
Intrusion Prevention	Sensors to prevent unauthorized access to networks and data
Website Content Filtering	System to detect employee access to inappropriate and infected websites
Email Content Filtering	System to detect infected email and spam messages
Anti-virus/ Malware	Software to detect malware and viruses on workstations and servers

110

Best Practices

- CIS (Center for Internet Security; best practices)
- SOX (Sarbanes Oxley)
- SAS70/SSAE16 (Statement on Standards for Attestation)
- PCI DSS (payment card industry data security standard; set of controls)
- FOIPPA (freedom of information and protection of privacy act)
  - previously required personal information be stored, accessed, and disclosed only in Canada
  - there were exceptions (eg. temporarily while travelling)
  - later amendments allow processing, routing
  - later amendments allow storage outside of Canada

University

Privileged account management

- Provide sparingly; only giving these permisions to users who need it
- Only use privileged accounts when necessary
- Monitor/check on these accounts and the use of them

Job rotation

- Reduce the length of time a person is in a job
- If you manage access properly this prevents people from having too much access
- Reduces chance for fraud

Information lifecycle management

- Creation
- Maintenance
- Distribution
- Disposition
- Use

Service level agreements (SLA)

- Agreement between organization and vendor that a service will perform to a certain level
- Availability/uptime, throughput, capacity, accuracy, response time, resolution time, mean time to resolution (MTTR), mean time between failures (MTBF)

TCP: Transmission Control Protocol

IP: Internet Protocol

- TCP/IP is the most widely implemented protocol in networks today
- IP adress identifies a system on a network, 4 numbers from 0-255 separated by periods

Subnetting

- Subnet masks take the same form as IP addresses but are used to determine which portions of the IP are for network and which are host addresses

IPv4 address

- 4 groups of decimals
- 4 groups of 8 bits (1 octet) = 32 bits

IPv6 address

- 8 groups of 4 hexadecimal digits
- 8 groups of 16 bits (2 octets) = 128 bits

DHCP: Dynamic Host Configuration Protocol

DHCP servers assign

- IP address
- Subnet mask
- Default gateway
- DNS servers

Media Access Control (MAC)

- Hardware address
- Intended to be unique but can be the same or changed/Spoofed
- 6 byte hexadecimal address that allows the network interface card (NIC) to be identified on the network
- 3 bytes identify the manufactuer
- 3 bytes are the serial number assigned to device

Domain Name System (DNS)

- Servers translate hostname to IP and IP to hostname

Address Resolution Protocol (ARP)

- Translates IP to MAC address

Classless Inter-Domain Routing (CIDR)

- Allows more flexible allocation of IP addresses
- Notation refers to the network bits

Routing

- different devices transmit traffic different ways

Device	Traffic	Note
hub	repeats traffic to all ports	inefficient
switch	sends traffic by MAC address	fast
router	send traffic by IP address	smart

- systems determine if host is on a local or remote network
- if remote then system looks in the routing table to determine whether it has an entry for the network
- if it does it uses that route, if not then uses default gateway
- if no known route static or learned then uses default route

Hub

- device that can be used for networking
- "dumb" device that sends all signals to all ports

Example:
If a device on port 1 wants to send to port 5 a copy of the traffic is sent to ports 2, 3, and 4 as well

hub icon 

Switch

- smarter device that can be used for networking
- understands physical addresses and sends traffic only to the port with the correct physical address

Example:
If a device on port 1 wants to send to port 5 it only sends to 5 based on MAC address. A MAC address looks like 76-E5-F9-DD-6B-07 and identifies the network card.

switch icon 

Router

- "smartest" device of the three that is used for networking
- understands IP addresses and networks and sends traffic only to the port with correct IP or network

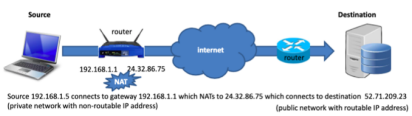
Example:
If a device on port 1 wants to send to port 5 it only sends to 5 based on IP address. An IP address looks like 24.14.82.67.

router icon 

NAT

NAT (Network Address Translation)

- how private and public networks communicate



Example: Findmyip

Ports

- used for communicating between systems
- 65,535 TCP ports and 65,535 UDP ports

Port	Purpose
20/21	FTP
22 ✓	SSH
23	Telnet
25	SMTP
53	DNS
67/68 (U)	DHCP

Port	Purpose
69 (U)	TFTP
80	HTTP
110	POP
143	IMAP
443 ✓	HTTPS
1433	SQL

Port	Purpose
0-1023	well-known
1024-49,151	registered
49,152-65,535	dynamic / private

Example: Telnet to test web, send email

- TCP is connection-oriented, expects and waits for responses, will re-transmit, can slow down, uses 3-way handshake:
  - client: SYN
  - server: SYN-ACK
  - client: ACK

User Datagram Protocol (UDP)

- Connection-less
- Does not wait for responses

- Nmap can identify open ports/services

Exploit

- Turns a vulnerability into an incident
- Code that takes advantage of a software vulnerability

Incident

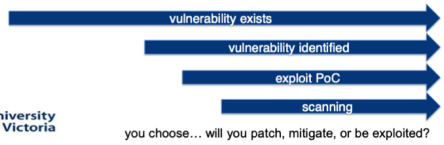
- A vulnerability that has been exploited
- Breach, Compromise

Vulnerability

- An exposure that exists in a system
- Unintended flaw in software code or a system that leaves it open to the potential for exploitation in the form of unauthorized access or malicious behavior

Process

- theoretical vulnerability is identified (eg. by researchers)
- exploit developed
- exploit released (or others get access to)
- exploit seen being used "in the wild"
- exploit being seen used against organization



University of Victoria

Where do vulnerabilities come from?

- Misconfigured systems
- Poor coding
- Insufficient security controls
- People

Impacts of vulnerabilities

- Denial of Service (DoS), system crash, degradation
- Remote code execution
- Disclosure of information, information exposure
- Unauthorized access, authentication by-pass
- Elevation of privilege/privilege escalation

What to do about vulnerabilities…

- stay alert, pay attention to vendors
- patch them…. when a patch is available
- until then take steps to mitigate
- if can't prevent then detect
- implement vendor workarounds
- restrict access
- implement IPS signatures

Types of Attacks

- **spoofing**
  - TCP vs UDP
- **wired, WiFi, wireless**
  - tapping copper, fibre
  - intercepting WiFi, Pineapple
  - intercepting Wireless, IMSI Catchers,
  - Mobile Device Identifiers (MDIs), Stingrays, Radio/RAN
- **host-based**
  - physical, local – USB, hardware keyloggers
  - logical, remote

virus	self-replicating program
worm	self-sustaining running program
trojan	program that does something other than it claims
spyware	malware that enables surveillance

exploit vulnerabilities to conduct

- DoS (denial of service) and DDoS (distributed denial of service)
- privilege escalation
- remote code execution

DDoS

- distributed denial of service
- multiple systems
- high volume, high bandwidth
- botnet, zombies
- amplification attack

Response

- enable anti-spoofing if relevant
- block traffic originating from places it shouldn't
- if pattern then local ACL, call service provider for ACL upstream
- on-premise anti-DDoS, cloud anti-DDoS (scrubbing)
- blackhole source(s), destination(s), remove target

buffer, heap, stack overflow

- exceeding amount of data that can be received without problems

ARP poisoning

- sending illegitimate messages on the network to take over an IP address

BGP hijacking (fake Border Gateway Protocol broadcasts)

- China
- Cryptocurrency
- Google traffic through Russia

DDoS

- volumetric/bandwidth attack sending more data than victim can accept

Defacement

- altering or replacing website

Doxxing

- revealing private information about a person publicly

SQL Injection

ping flood	large volume or large size or both
ping of death	size >65,535 when re-assembled
SYN flood	syn, syn, syn, syn… w/o ACK
UDP flood	fire and forget, large volume
smurf	spoof IP of victim – ICMP/ping a bunch of hosts
fraggle	spoof IP of victim – send UDP traffic to router's broadcast
teardrop	jumbled packets – IP, 1 too small (also NewTear)
land	source and destination ports the same, causing loop

bonk	fragments of packets to port 53 can't assemble
boink	same as bonk but multiple ports
jolt, ssping	similar just larger packets
pepsi	udp flood with varied sources aimed at certain ports
jizz	DNS spoofing, false caching
ICMP nukes	send packets the destination OS can't handle eg. OOB -> port 139 on Win 98 -> BSOD

reflection	spoof IP, send request, response goes to victim
amplification	attacker ensures more traffic hits victim than attacker can send alone
browser hijack	change home page, search, toolbars
backdoors	covert method of bypassing authentication and gaining access to a system
rootkits	program enables access to computer and masks existence
password attacks	dictionary attacks, brute force, rainbow tables

social engineering	psychological manipulation of people into performing actions or divulging confidential info
phishing, smishing, vishing	fraudulent attempt to obtain information over email, SMS, voice
spearphishing	targeted phishing
whaling	phishing targeted at executive
zero day exploits	attack involving previously unknown vulnerability
cross-site scripting	inject scripts into websites
malvertising	displaying infected ads on legitimate websites
waterholing	infecting a site that users are likely to visit

Examples

- **Melissa**
  - MS Word macro
  - disabled safeguards, lowered security settings
  - spread via infected email, sent to top 50 contacts
  - $1.2B damage
- **ILoveYou**
  - spread through email attachment
  - filename was Love-letter-for-you.txt.vbs (vbs didn't show)
  - sent to all contacts, changed home page
  - stole passwords and sent to attacker
  - 10% of computers infected, $15B damage in Y2000

SQL Slammer/Sapphire

- spread via buffer overflow in MS SQL
- infected random IPs after creating millions of copies
- $750 million damage, significant impact on government, banks, 911

Sasser ($500 million in damage)

- exploited vulnerability in LSASS (local security authority subsystem service)
- scanned until found a vulnerable IP
- uploaded to Windows directory; target infected upon next reboot

MyDoom

- spread through KaZaa and emails; initiated DDoS, install backdoor
- searched for email addresses, forged from address
- 6-700k infected, $38 billion in damage

Stuxnet

- targeted Siemens, modified PLCs only used in Iran nuclear treatment plant
- "world's first digital weapon"
- spun up Iranian centrifuges, disabled safety monitoring
- attribution

Cryptolocker (2013)

- zip file with executable looks like PDF

Cryptowall (2014)

- ransomware through spam, malvertising

Cerber (2016)

- 150k devices, $195k ransom

Locky (2016)

- email fake invoice, tricks to enable macros, encrypts

Wannacry (2017)

- leveraged SMB vulnerability; 200k victims

NotPetya (2017)

- leveraged SMB vulnerability, infects MBR, encrypts MFT; $593 million (Merck)

Code Red

- buffer overflow, overwrote memory with instructions for virus
- compromised system and instructions varied based on day of month
- 1-19th target random IPs; 20th – 28th launch DDoS on White House, 29th+ sleep mode
- 1-2 million infected, $2B damage

Nimda

- origin of the name, when it was released, rumours
- compromised system, spread through variety of ways (email, network, vulnerabilities)
- $635 million damage, over 2 million infected in 24 hours

Conficker

- spread by infected USB drives over networks
- disabled anti-malware; created backdoors
- confusion regarding what it was intended to do on April 1, 2009
- $9.1B damage with impact to government, military

HeartBleed

- OpenSSL, tricking servers into leaking information affecting CRA

ShellShock

- bash vulnerability

Poodle (Padding Oracle on Downgrading Legacy Encryption)

- MitM exploits fallback to SSL 3.0

Freak (Factoring RSA Export Keys)

Beast (Browser Exploit Against SSL/TLS)

- exploited weak encryption

Drown

- attacks servers by using support for obsolete, insecure SSL v2

Duqu

- very similar, digitally signed, information gathering/KL
- MS Word dropper, download malware, execute payload

Flame (most complex malware at the time of discovery)

- information gathering, pretends to be Windows update proxy

Gauss

- information stealer – based on Flame

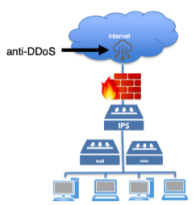
Stuxnet and Duqu same, Flame and Gauss similar

Prevention

- Anti-DDoS (on-prem, cloud)
- Firewall (packet filtering, stateful, NG)
- Intrusion detection/prevention (HIDS, NIDS)
- Web content filtering
- Email content filtering
- SIEM
- VPN (client-to-site vs site-to-site; IPSec vs SSL)
- Anti-malware

Anti-DDoS

- prevents or mitigates high volume attacks
- types
  - on-prem — may be effective up to amount of bandwidth
  - cloud — redirect malicious traffic to scrubbing centre
- methods
  - manual — human detects, human responds
  - hybrid — human decides to invoke automated controls
  - automatic — tools detect and respond



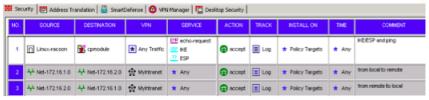
University of Victoria

Considerations
- anti-spoofing
- reflection, amplification attacks

Firewall

- different types
  - circuit-level (operates at transport/session)
  - packet-filtering (examines each packet)
  - stateless (does not track state, packet streams)
  - stateful (aware if packet is part of a larger stream, sometimes called shallow packet inspection)
  - application (operates at application layer, deep packet inspection)
  - next generation NG (combines intrusion prevention and more)

- determines whether packets should be permitted through
  - fundamentally rules are source, destination, port, action
  - start with a "cleanup rule" of "any – any – drop"
  - add exceptions above



Firewall Ruleset Sample

Firewall Ruleset Sample

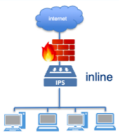
#	Source	Dest	Service	Action	Track
1	Bad People	Any	Any	Drop	No log
2	24.112.86.55	24.110.83.93	25565	Allow	Log
3	123.42.56.107	24.110.83.92	http/80 & https/443	Allow	Log
4	23.73.51.95	24.110.83.93	Any	Drop	Log
5	Any	Any	telnet/23	Drop	Log
6	23.73.51.95	24.110.83.92	Any	Drop	Log
7	Any	Any	Any	Drop	Log

Intrusion Detection/Prevention

- two types
  - intrusion detection (only detects and notifies regarding intrusions)
  - intrusion prevention (detects and stops intrusions)
- two types (same as firewalls)
  - host-based IPS (on the host)
  - network-based IPS (on the network)
    - can be in-line or off a tap
    - can fail open or fail closed
- detection methods
  - signature-based
    - compare traffic against known attack patterns
  - anomaly based
    - create **baseline** of normal activity and identify deviations.. **anomalies**

Intrusion Detection/Prevention

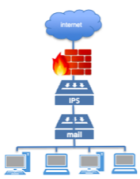
- positioning of security gear
  - do you put the IDS/IPS, for example, in-line or on a tap
  - what are the pros/cons
  - if the system is malfunctioning do you want it to fail open or closed?
  - firewall should fail closed
  - others it's up to the risk appetite of the organization



University of Victoria

Email Content Filtering

- determines whether emails should be let through
- focuses on matching
  - source IP address
  - source email address
  - destination email address
  - email content
  - email attachment
  - …others
- also consider whitelisting/blacklisting, SPF, DKIM, DMARC



Email Content Filtering

- rate of effectiveness
- first check can be blacklist/whitelist
- second check can be reputation-based
  - low score means no connection allowed
  - could be rate-limited or prevented
  - earn negative reputation, earn positive
- third check can be anti-spam, anti-malware

Email Content Filtering

- RBL = realtime blackhole list
  - how do you get on? get off?
- SPF = sender policy framework
  - identifies which IP addresses should be permitted to send email for your domain
  - does your organization have a record?
  - does your organization factor in SPF? enforce?

University of Victoria

also
DKIM = Domain Keys Identified Mail
DMARC = Domain Message Authentication Reporting

Web Content Filtering

- enables employers to determine which sites and categories of sites will and won't be permitted
- ensure you have an appropriate use policy, information security policy, or other code of conduct document
- which sites do you block? how do you decide?

Logging

- all of these platforms generate logs
- can log locally or remotely
- can log decentralized or centralized
- centralized provides visibility to variety of platforms
- common basic logging platform is 'syslog'
- includes where the logs came from – hostname or IP
- timestamp – important to have common time
- then ensure sufficient level of detail in the logs to know who did what when
- ensure you are able to identify 'events of interest'
  - eg. anomalies, intrusions, unauthorized access, unauthorized changes, other violations

Security Logs (certification)

- firewall

```
2020-01-01 22:00:32 ALLOW TCP 192.168.0.1:45137 207.194.28.62:80 1532 0 1 SEND
2020-01-01 22:00:33 DENY TCP 54.12.34.15:45137 207.192.168.0.5:25 332 0 1 SEND
2020-01-01 22:00:35 ALLOW TCP 192.168.0.1:35437 207.194.28.62:80 7531 0 1 SEND
2020-01-01 22:00:38 DENY UDP 67.82.41.2:31337 192.168.0.123:54321 534 0 1 SEND
```

- IPS/IDS

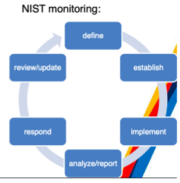
```
Jan 19 16:18:40 HOST_SNORT snort: [116:55:1] (snort_decoder): Truncated Tcp Options (TCP) AAA.BBB.CCC.DDD:80 ->
AAA.BBB.CCC.DDD:1589
Jan 19 16:18:40 HOST_SNORT snort: [119:7:1] (http_inspect) IIS UNICODE CODEPOINT ENCODING (TCP) AAA.BBB.CCC.DDD:23564 ->
AAA.BBB.CCC.DDD:80
Jan 19 16:18:40 HOST_SNORT snort: [1:2307:1] WEB-PHP PayPal Storefront arbitrary command execution attempt [Classification: Web
Application Attack] [Priority:1]: (TCP) AAA.BBB.CCC.DDD:55023 -> AAA.BBB.CCC.DDD:80
Jan 19 16:18:40 HOST_SNORT snort: [119:7:1] (http_inspect) IIS UNICODE CODEPOINT ENCODING (TCP) AAA.BBB.CCC.DDD:55053 ->
AAA.BBB.CCC.DDD:80
Jan 19 16:18:40 HOST_SNORT snort: [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING (TCP) AAA.BBB.CCC.DDD:49065 ->
AAA.BBB.CCC.DDD:80
Jan 19 16:18:41 HOST_SNORT snort: [119:14:1] (http_inspect) NON-RFC DEFINED CHAR (TCP) AAA.BBB.CCC.DDD:49082 ->
AAA.BBB.CCC.DDD:80
Jan 19 16:18:41 HOST_SNORT snort: [1:2003:2] MS-SQL Worm propagation attempt[Classification: Misc Attack] [Priority: 2]: (UDP)
AAA.BBB.CCC.DDD:10000 -> AAA.BBB.CCC.DDD:1434
Jan 19 16:18:43 HOST_SNORT snort: [1:483:2] ICMP PING CyberKit 2.2 Windows [Classification: Misc activity] [Priority: 3]: (ICMP)
AAA.BBB.CCC.DDD -> AAA.BBB.CCC.DDD
```

Monitoring

- common to monitor up/down of systems and whether they are functioning
- are you monitoring for security events as well?
- tricky to determine what is permitted vs. not as there are often exceptions to rules

  eg. users shouldn't be deleted – but sysadmins have to delete when the user is no longer employed
- one example you always want to be alerted on is disabling logs
- also consider file integrity monitoring – good to know when certain files change
- sensitivity
  - false positive: something detected as bad and it's not (type 1 error)
  - false negative: something not detected as bad and it is (type 2 error – dangerous)
  - true positive: something detected as bad and it is
  - true negative: something not detected as bad and it's not

NIST monitoring:



University of Victoria

Honeypots/Honeynets

- honeypot
  - system designed to be an attractive target for attacks
  - can be used to detect them or distract from real targets
- honeynet
  - network designed to be an attractive target for attacks
  - may contain one or more honeypots
- tarpit
  - system designed to slow attackers down
- canary
  - system designed to provide early warning
  - eg. email account, top of GAL, default route alerting, system that should never receive traffic

SIEM (aka SIM, SEIM)

Security Information and Event Management

- must collect logs… good idea to aggregate them
- must look at them… log monitoring
- humans can't keep up
- need a system to correlate to find badness
- try not to send false alarms to humans …. alerting
- humans and their time are valuable

SIEM

- organizations need to keep logs of who did what when
  - who doesn't keep logs?
- ineffective to have humans staring at glass
- need systems to do the collection, aggregation, correlation, monitoring, alerting
- **mandatory tuning**
- goal is to put actionable intelligence in the hands of the security analyst
- next evolution is SOAR (Security Orchestration Automation and Response) systems that help automate portions or all of response to potential attacks

VPN (Virtual Private Network)

- secure access to other systems
- traffic is encrypted while in the "tunnel"
- best used with strong authentication

en

VPN

- Client-to-Site VPN (C2S)
  - IPSec or SSL
  - provides secure remote access into organization network
  - best used with strong authentication / 2FA / MFA
- Site-to-Site VPN (S2S)
  - "always on"; allows secure access between organizations

Anti-virus

- some AV is very basic and offers very limited protection
- may use a software firewall in addition to a hardware firewall and anti-malware
- avoid virus, browser hijacking, infected attachments, malicious links, etc.

Anti-Malware

- anti-malware
  - signature-based
  - behaviour-based
- online options
  - eg. HouseCall anti-virus
  - eg. VirusTotal
- install on desktops, laptops, mobiles, servers
- also sandboxing, quarantining, reverse engineering

Incident Handling & Response Traits

- Assertive
- Sense of urgency
- Bias for action

Incident Handling

- Logistics
- Communications
- Coordination
- Planning functions to resolve an incident calmly and efficiently
- Measured in minutes

Incident Response

- All of technical components required in order to analyze and contain an incident
- Measured in minutes

Incident Management

- Ensures that normal service operation is restored quickly and business impact is mimized
- Goal is to restore service
- Measured in minutes

Investigations

- Examine a real or suspected violation of policy or law to determine who did what, when
- Measured in days, weeks

Security incident: Violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. It implies harm or attempt to harm

Prevent: Guard against
Detect: Discover existence, presence
Deny: Block
Disrupt: Cause it to fail, break or interrupt flow of info
Degrade: Slow the attack, reduce effectivness or efficiency
Deceive: Fool the attacker
Destroy: Reduce the attacker's capability, damage system or entity

...the attack by any legal means possible

- Process does not focus on the theoretical, abstract, or illogical
- Cannot afford to be hampered by ambiguous/confused people, irrelevant questions, slow processes
- Minutes Matter
- Make decisions based on the available information

PICERL Process

Preparation: People, process and tools are in place
Identification: Recognition and reporting of the event or incident and assess scope, convene the team
Containment: Stop the problem from getting worse
Eradication: Remove all traces of the issue
Recovery: Restore service back to normal
Lesson learned: Identify any opportunities for improvement

Preparation

- Build incident response plan
- Ensure you have an incident response team
- Document roles and responsibilities
- Conduct exercises, drills regularly
- Understand environment
- Understand controls available
- Hygiene level technical controls
- Understand impacts
- Prepare war room and conference bridge(s)
- Establish communications plan in advance

Incident handler

- Leading the incident, delegated authority
- Appoint roles, convene team
- Responsible for identification
- Determine when to move to next steps
- Responsible for ensuring progress
- Managing flow of misinformation
- Seldom an enviable position
- Ferries between management and technical bridge
- Establishes an update frequency
- Buffer in front of incident response team

Incident Response on Retainer

- Establish agreements in advance
- Few organizations available to help in event of an incident and even less competent ones
- Engaging external assistance is seen as a sign of maturity
- External organizations may be more able to assist with Incident Response than Incident Handling

Roles

- Incident handler
- Communications
- Note-taker

Note-taking

- Date/Time/Name
- Key decisions
- Actions
- Updates
- Everyone should take notes
- If you are going too fast for notes, you are going too fast

Communications

- Full time role
- May be combined with other roles like note-taking and media relations
- Single point of contact for official updates
- Controls flow of information and misinformation
- Enforces need-to-know
- Serves as a buffer for incident handler

Jump bag/Kit

- Documentation, diagrams
- Contact lists
- Camera, memo recorder
- Media
- USB, hard drive
- Blank media
- Live CDs, software tools
- Hardware/tools
- Cables, dongles, adapters
- Spare batteries
- Notebook(s)

Convene

- Bring together everyone who knows about the issue
- Remind them of their responsibility to maintain need-to-know
- Ensure the right individuals are present
- Contian the information and misinformation
- Communication is vital to incident handling and incident response
- Break/fix and security incidents trump most business processes but not all
- War room or conference bridge
- Two different locations/bridges (Management, Technical)
- Establish procedure for communicating securely during an incident

Notification

- Report the issue
- Don't capture the details in a public ticketing system
- Monitor and alert
- Respond and escalate 24/7

Identification

- Determine whether it is an event or an incident
- Perform triage and ensure a common understanding of how it was detected, who is aware
- Determine urgency and initial impact
- Review information and actions taken to date

Event vs Incident

Event: Change in the normal behavior of a given system, process, environment or workflow

Incident: Change in a system that negatively impacts the organization, municipality, or business

All incidents are events, but not all events are incidents

Containment

- Prevent further damage
- Stop the problem from getting worse
- Determine the source, what vulnerability was exploited, and contain it, plug holes
- Preserve the evidence (keep a sample system, make a forensic copy)

Chain of custody

- Always handle evidence as if you are going to court
- Maintain evidence log
- Have an established process
- Store in secure location when not in possession
- Must demonstrate evidence was not tampered with

Lessons learned

- Walk through and review play-by-play of incident report
- Objective to identify opportunities for improvement to better prepare for next time
- Essential for continuous improvement

Risk

- Probability that a vulnerability will be exploited and the impact if it does
- Likelihood that something bad will happen that causes harm
- Potential for loss, damage, destruction of an asset as a result of a threat exploiting a vulnerability

Risk = probability x impact

Risk appetite: Amount of risk an entity is willing to accept in pursuit of value

Risk tolerance: Consider how much risk you're able to take and how much you're willing to take

Risk register: Inventory of risks to an organization

Risk assessment: Determines risk by assessing quantitative and qualitative factors

Risk owner: Individual responsible for ensuring a risk is managed appropriately

Examples of incident types

- Violation of explicit or implied security policy
- Unauthorized access
- Denial of service
- Unauthorized or inappropriate use
- Changes without owner's knowledge, instruction, or consent
- Malicious code

Eradication

- Objective is complete removal of all traces of the infection or incident
- Ensure the holes are closed
- Ensure the incident cannot re-occur
- Compromised machines cannot be trusted

Recovery

- Objective is to return systems to normal operation
- Test, monitor, and validate as each system is returned to production
- Determine if it should be restored
- Monitor closely for suspicious signs, ensure you have visability

Threat

- Any potential danger associated with the exploitation of a vulnerability
- Anything that has potential to do harm
- Something that could have a negative impact to the organization

Threat agent: Entity that takes advantage of a vulnerability

Quantitative Risk Assessment

- Determine asset value (AV) for each asset
- Identify threats
- Determine exposure factor (EF)
- Calculate SLE, ARO, ALE
- Objective, calculated

Qualitative Risk Assessment

- Ranks seriousness of threats by standard
  - Low, Medium, High
- Subjective

Single Loss Expectancy (SLE)

SLE = AV x EF

- Value you lose when the risk becomes real

Annual Loss Expectancy (ALE)

ALE = SLE x ARO

- ARO: Annualized rate of occurrance
- Value you will measure if risk becomes real in one year

Countermeasure (Controls)

- Measure taken to reduce risk
- Value = $ALE_{previous} - ALE_{now}$
- Total cost of ownership: Cost of a safeguard

Inherent Risk

- Natural level of risk; level of raw or untreated risk
- Rating exposure in absence of controls (countermeasures)
- Existing risk before controls are applied

Residual Risk

- Remaining risk as it is impossible to identify all risks or fully mitigate/eliminate all risks
- Risk remaining after controls are applied

Risk remediation: Fix or correction to a vulnerability decreasing or eliminating risk

Risk transference: Measures to place responsibility on another entity

Risk mitigation/deterrence: Measures put in place to protect against a risk

Risk Treatment

- Risks often can't be eliminated
- Threats and vulnerabilities impact likelihood or consequence of risk
- Risks can be
  - Ignored/rejected
  - Accepted
  - Avoided
  - Transferred
  - Mitigated/reduced/treated

Types of controls

- Deterrent
- Preventive
- Detective
- Corrective
- Recovery
- Compensating

When to do a risk assessment

- Introducing a new system
- Material change to an existing one

STRA: Security Threat and Risk Assessment

SoAR: Statement of Acceptable Risk

ROSI: Return on Security Investment

Risk Assessment Steps

1) Identify target/scope, stakeholders, background
2) Identify criticality
3) Identify vulnerabilities
4) Identify risks
5) Identify actions
6) Obtain approvals/signatures

Threat Modeling

- Way to identify threats, visualize, understand security
  1) Defining security requirements/security objectives
  2) Identify assets and dependencies
  3) Identify trust zones
  4) Identify threats/vulnerabilities
  5) Document threat model

Asset Management

- Asset lifecycle
  1) Identify/classify
  2) Secure
  3) Monitor
  4) Recover
  5) Dispose

Asset commissioning: Have policies that say what you track, asset inventory, asset ownership, asset retention

Asset decommissioning: Have policies that say what you do with assets with it's time to get rid of

Reverse logistics: Process to harvest value out of products or final disposal

Secure Disposal of Information

- Physical destruction
- Logical destruction
- Harddrive shredding
- Evil Destroyer of Delicate Internal Electronics (EDDIE)

Clearance

- Pre-employment screening
- Background/reference checks
- Criminal record check
- Credit check
- Security clearance
  - Level 1 (Confidential)
  - Level 2 (Secret)
  - Level 3 (Top Secret)

Linux commands

ping: Test connectivity between a source and destination

traceroute: Trace the path between a source and destination

netstat: Multiple uses including checking what ports are listening on a machine and current connections (netstat --an) or checking the routing table (netstat --rvn)

whois: Find out information regarding a domain

nmap: Often used for port scanning

nessus: Often used for network vulnerability scanning

Metasploit: Often used to exploit vulnerabilities

Steganography: Used to conceal information in a file

John the Ripper

- Password cracker used in pentesting exercises
- Takes in encrypted password and encrypts strings and compares output
- Can supply a wordlist or brute force