SENG 460 / ECE 574
Practice of Information Security and Privacy

Prevention

(left over from last time)

Gary Perkins, MBA, CISSP

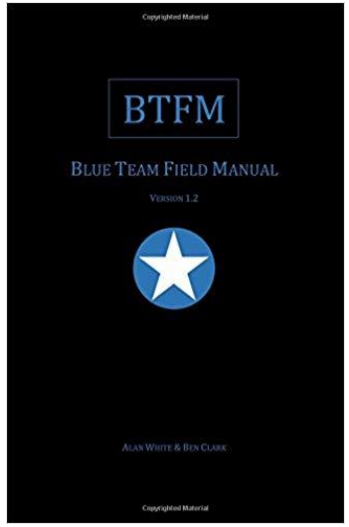
garyperkins@uvic.ca

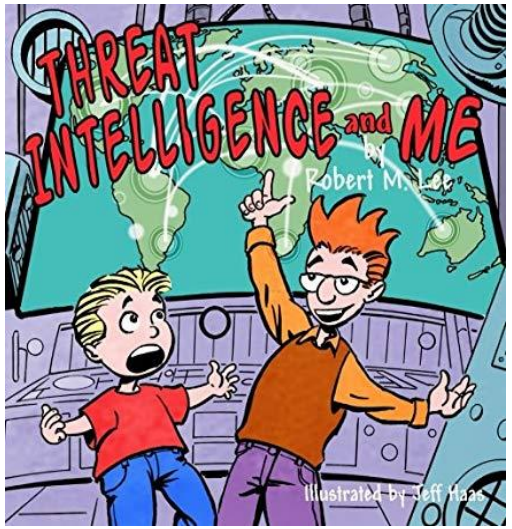
University of Victoria

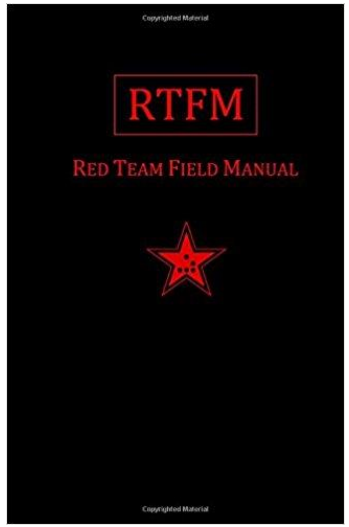
Dilbert by Scott Adams

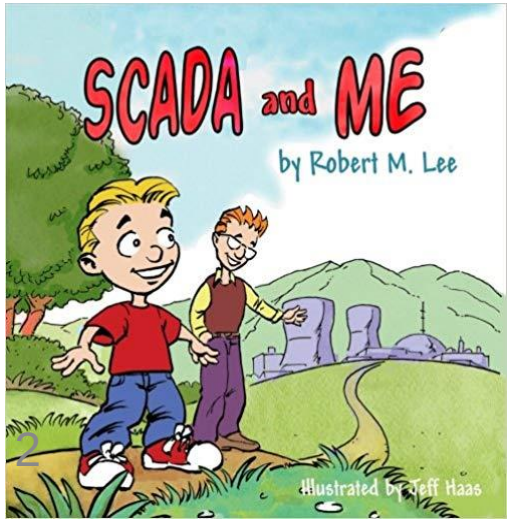
Prevention

- blue team
  - defenders, preventive
  - harden systems
- red team
  - attackers, external, blind
  - goal is to compromise the organization
- purple team
  - single group that does blue and red team
  - attacks and defends





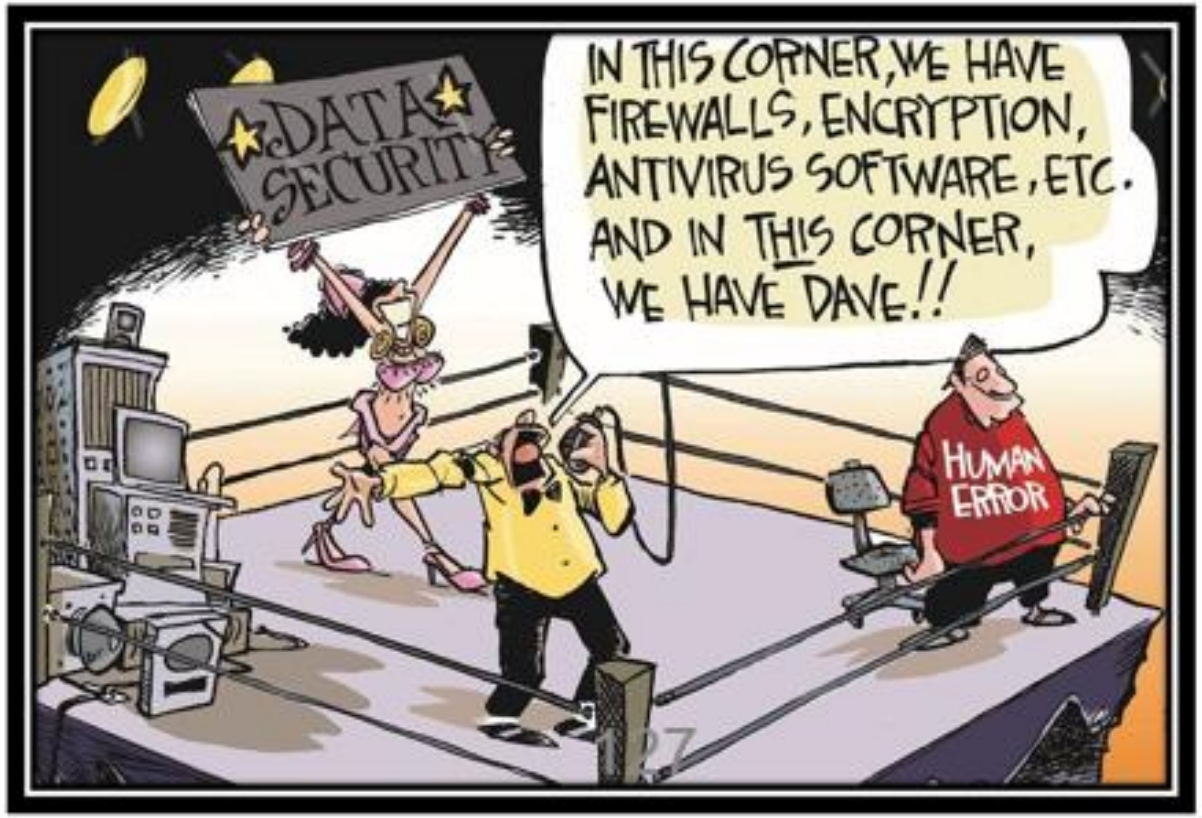




University of Victoria

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

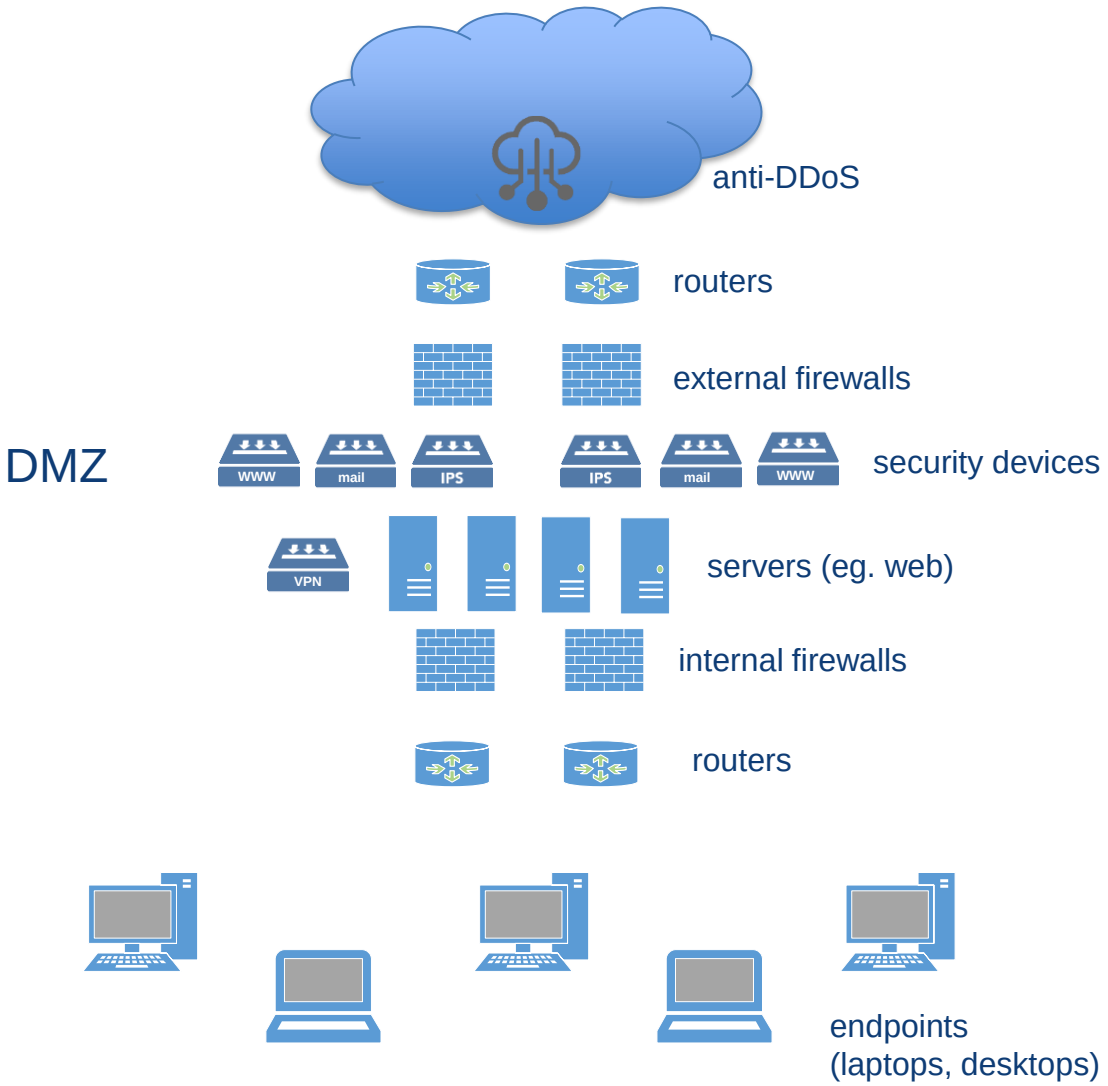


University of Victoria

Sample Network Diagram

- simplified network diagram
- security stack
- DMZ
- direction of traffic
- redundancy & availability

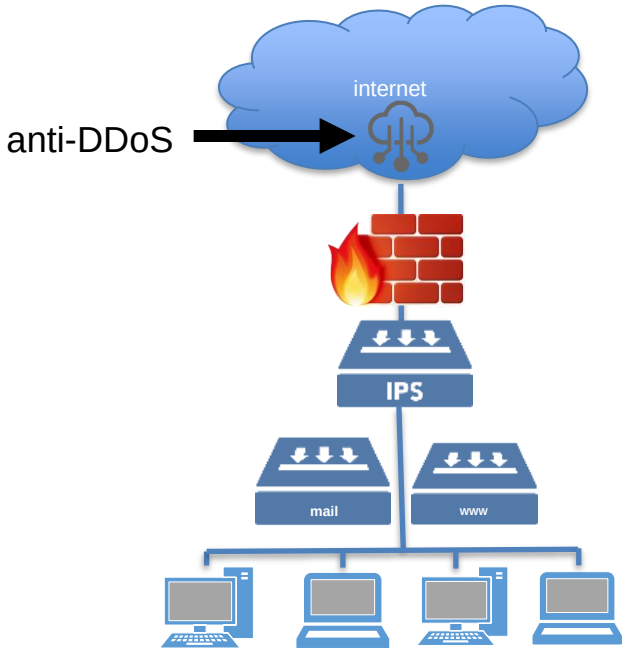
other topics
- impact of device placement (eg. IPS)
- impact of encrypted traffic
- naming conventions (eg. bcfw01.acme.com)



University of Victoria

Anti-DDoS

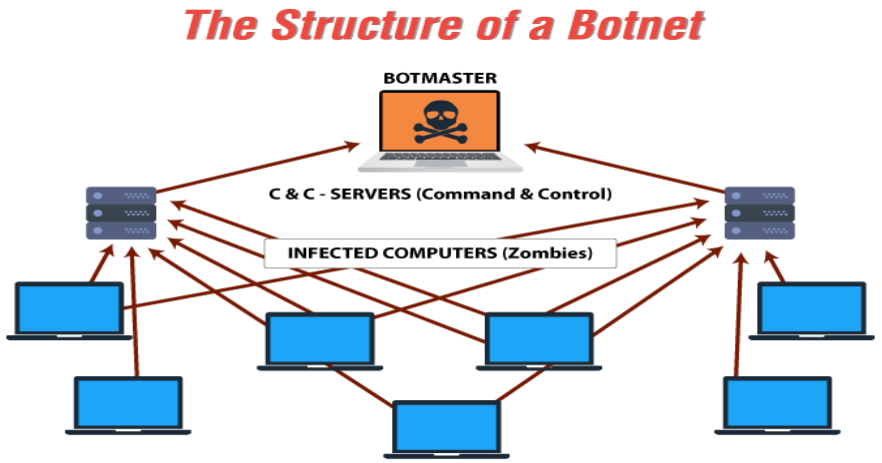
- prevents or mitigates high volume attacks
- types
  - on-prem may be effective up to amount of bandwidth
  - cloud redirect malicious traffic to scrubbing centre
- methods
  - manual human detects, human responds
  - hybrid human decides to invoke automated controls
  - automatic tools detect and respond



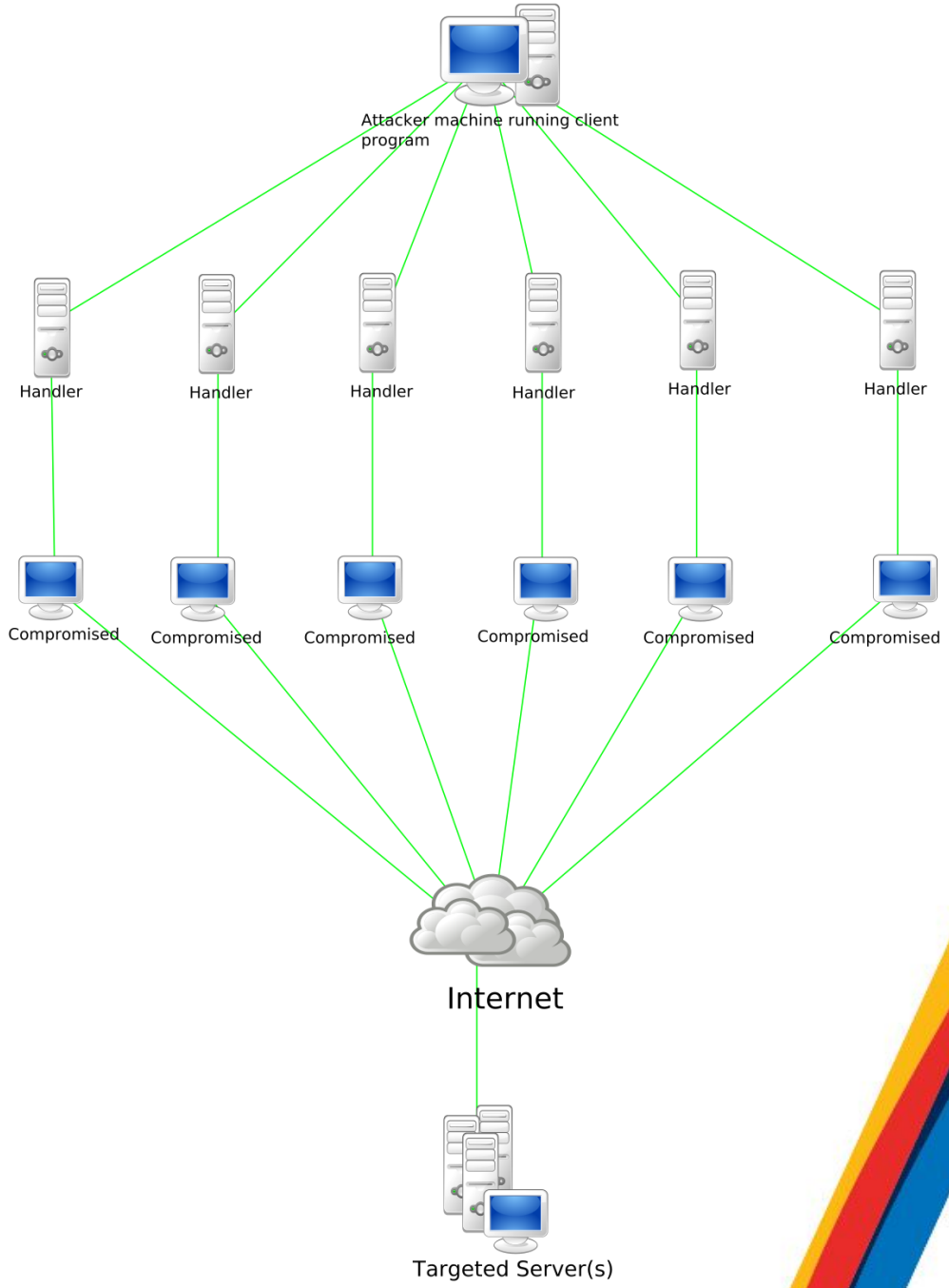
Considerations
- anti-spoofing
- reflection, amplification attacks

University of Victoria

Anti-DDoS

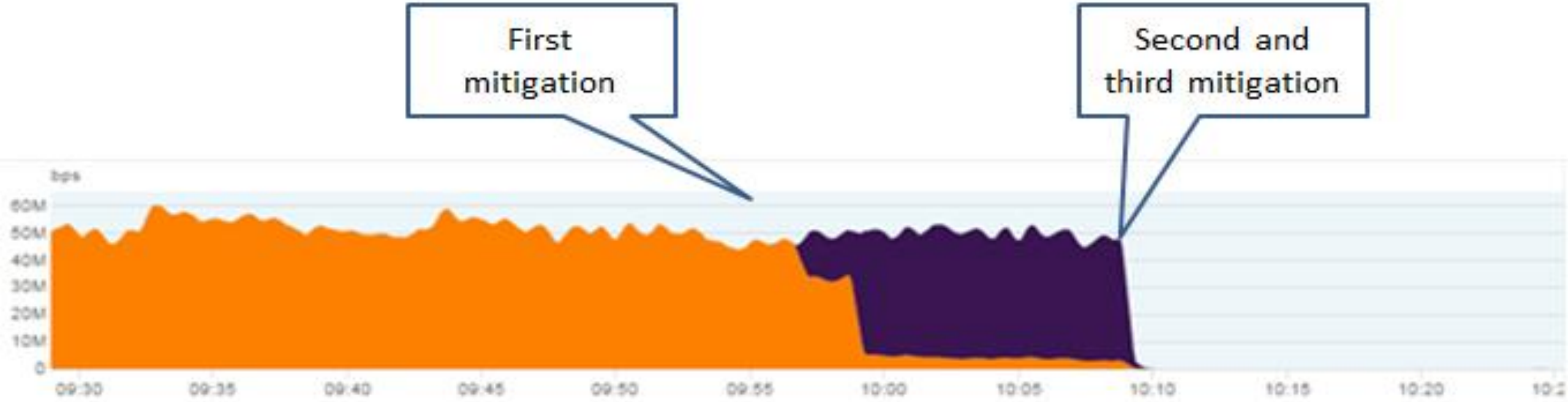


https://blog.eccouncil.org/botnets-and-their-types/



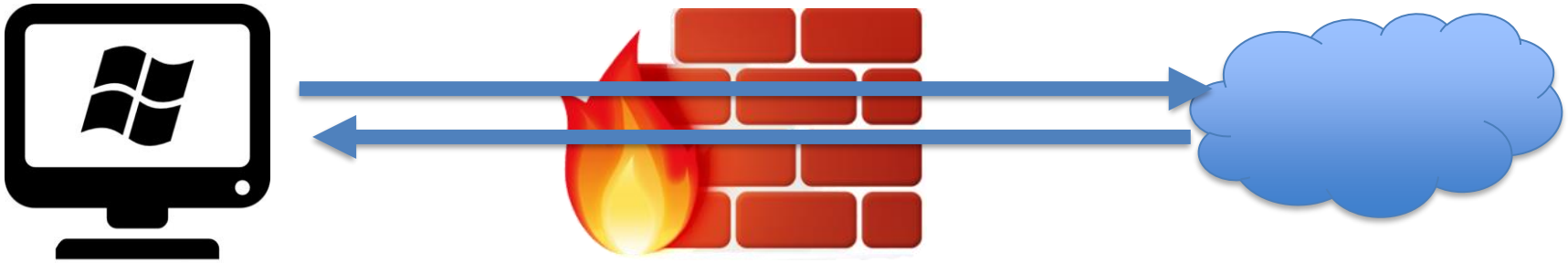
University of Victoria

Anti-DDoS

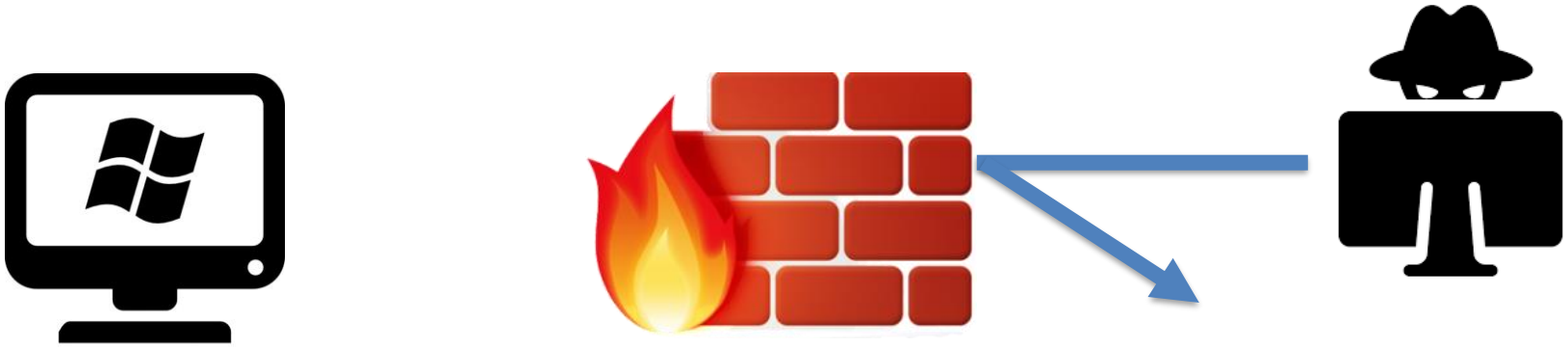


Key	Graph	Category	Bytes Blocked	bps Blocked	Packets Blocked	pps Blocked
		Spoofed SYN Flood Prevention	11.64 GB	25.87 Mbps	286.17 M packets	79.49 kpps
		Blacklisted Hosts	3.73 GB	8.29 Mbps	91.63 M packets	25.45 kpps
		ICMP Flood Detection	352.19 kB	782.63 bps	4.72 k packets	1.31 pps
		TCP SYN Flood Detection	215.48 kB	478.84 bps	721 packets	0.20 pps

Firewall



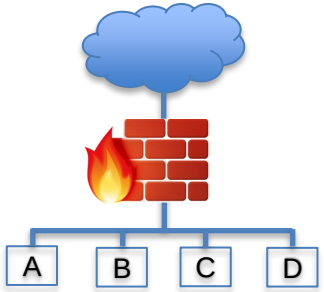
5-tuple: source IP/port, destination IP/port, protocol



University of Victoria

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)



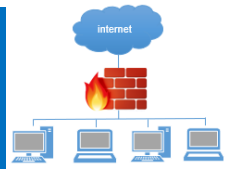
- determines whether packets should be permitted through
  - fundamentally rules are source, destination, port, action
  - start with a “cleanup rule” of “any – any – drop”
  - add exceptions above

Security | Address Translation | SmartDefense | VPN Manager | Desktop Security

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	Linux-racoon	cpmodule	Any Traffic	ICMP echo-request UDP IKE ?? ESP	accept	Log	Policy Targets	Any	IKE/ESP and ping
2	Net-172.16.1.0	Net-172.16.2.0	MyIntranet	Any	accept	Log	Policy Targets	Any	from local to remote
3	Net-172.16.2.0	Net-172.16.1.0	MyIntranet	Any	accept	Log	Policy Targets	Any	from remote to local
4	Any	Any	Any Traffic	NBT TCP microsoft-ds	drop	None	Policy Targets	Any	There are always some W* hosts around...which shouldn't fill the log
5	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any	Drop all other traffic

University of Victoria

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

University of Victoria

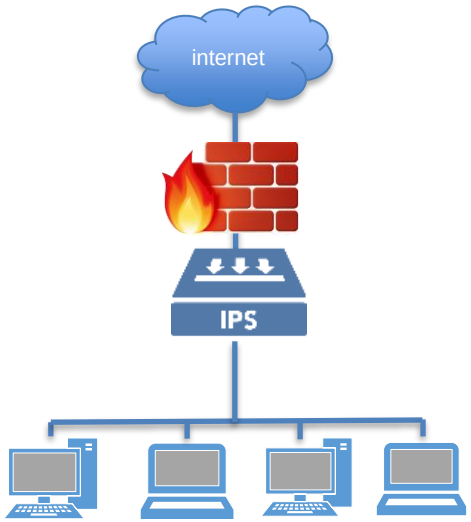
Firewall Ruleset Sample

#	Source	Dest	Service	Action	Track
1					
2					
3					
4					
5					
6					
7					

University of Victoria

Intrusion Detection/Prevention

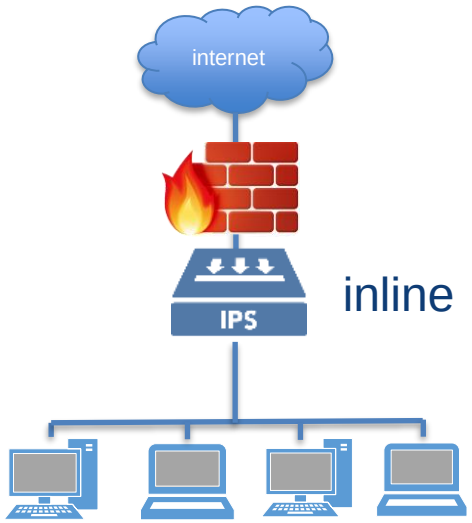
- two types
  - intrusion detection (only detects and notifies regarding intrusions)
  - intrusion prevention (detects and stops intrusions)
- two types (same as firewalls)
  - host-based IPS (on the host)
  - network-based IPS (on the network)
    - can be in-line or off a tap
    - can fail open or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



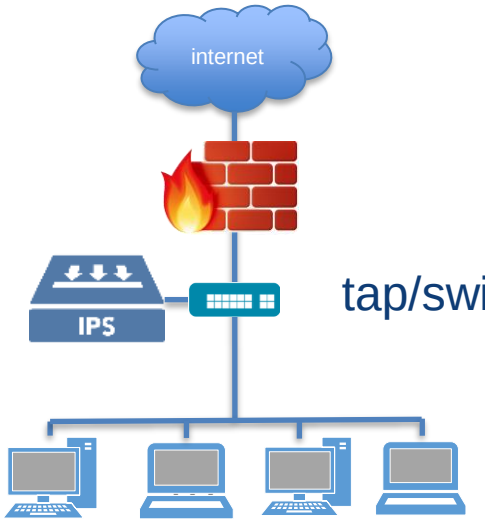
University of Victoria

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



inline

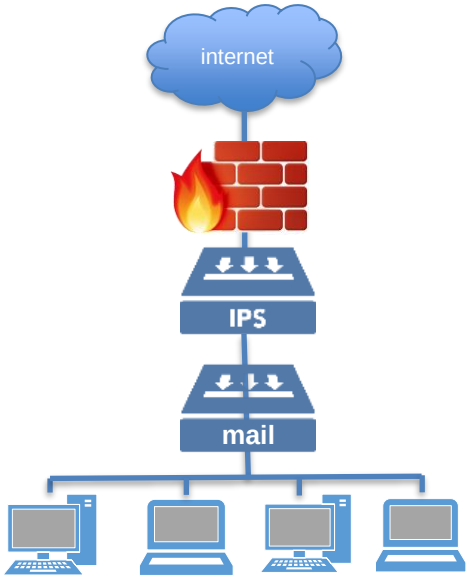


tap/switch

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



University of Victoria

Example: Telnet

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

University of Victoria

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?

also

DKIM = Domain Keys Identified Mail

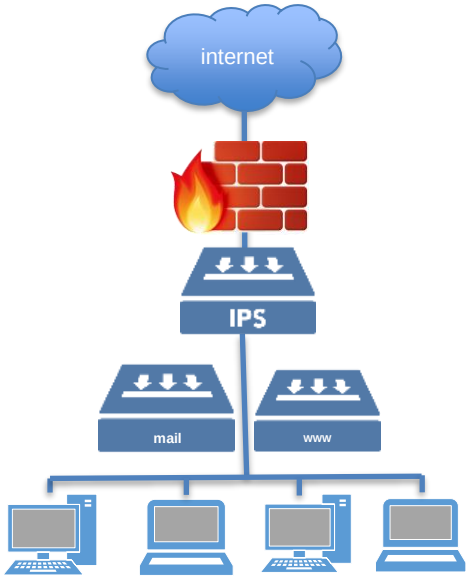
DMARC = Domain Message Authentication Reporting

University of Victoria

Web Content Filtering

- lets companies pick which sites and categories are allowed
- how do you decide what sites to block?

Alcohol & Tobacco
Anonymizer
Art / Culture
Blogs / Personal Pages
Botnets
Browser Plugin
Browser Toolbar
Business / Economy
Child Abuse
Cloud Services
Computers / Internet
Cryptocurrency
Download Manager
Education
Email
Encrypts communications
Entertainment
Fashion
File Storage and Sharing
File Upload
Financial Services
Friendster Widgets
Gambling
Games
General
Google Plus Widgets
Government / Military
Greeting Cards
Hacking
Hate / Racism
Health
High Bandwidth
IPTV
Illegal / Questionable
Illegal Drugs
Inactive Sites
Instant Chat
Instant Messaging
Job Search / Careers
Lifestyle
Lingerie and Swimsuit
LinkedIn Widgets
Marijuana
Media Sharing
Media Streams
Microsoft & Office365
Mobile Software
MySpace Widgets
Nature / Conservation
Network Protocols
Network Utilities
News / Media
Newsgroups / Forums
Ning.com Widgets
Non-profits & NGOs
Nudity
P2P File Sharing
Personals / Dating
Phishing
Political / Legal
Pornography
Real Estate
Recreation
Religion
Remote Administration
Restaurants / Dining / Food
SCADA Protocols
SMS Tools
Search Engines / Portals
Sex
Sex Education
Shopping
Social Networking
Social Plugins
Software Downloads
Software Update
Spam
Sports
Spyware / Malicious Sites
Stealth Tactics
Suspicious Content
Tasteless
Translation
Travel
Twitter Clients
URL Filtering
Uncategorized
Vehicles
Video Conferencing
Violence
Virtual Worlds
VoIP
Weapons
Web Advertisements
Web Browser
Web Browser Acceleration
Web Conferencing
Web Content Aggregators
Web Services Provider
Web Spider



University of Victoria

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?

University of Victoria

Web Content Filtering

Alcohol & Tobacco
Anonymizer
Art / Culture
Blogs / Personal Pages
Botnets
Browser Plugin
Browser Toolbar
Business / Economy
Child Abuse
Cloud Services
Computers / Internet
Cryptocurrency
Download Manager
Education
Email
Encrypts communications
Entertainment
Fashion
File Storage and Sharing
File Upload
Financial Services
Friendster Widgets

Gambling
Games
General
Google Plus Widgets
Government / Military
Greeting Cards
Hacking
Hate / Racism
Health
High Bandwidth
IPTV
Illegal / Questionable
Illegal Drugs
Inactive Sites
Instant Chat
Instant Messaging
Job Search / Careers
Lifestyle
Lingerie and Swimsuit
LinkedIn Widgets
Marijuana
Media Sharing
Media Streams
Microsoft & Office365
Mobile Software
MySpace Widgets

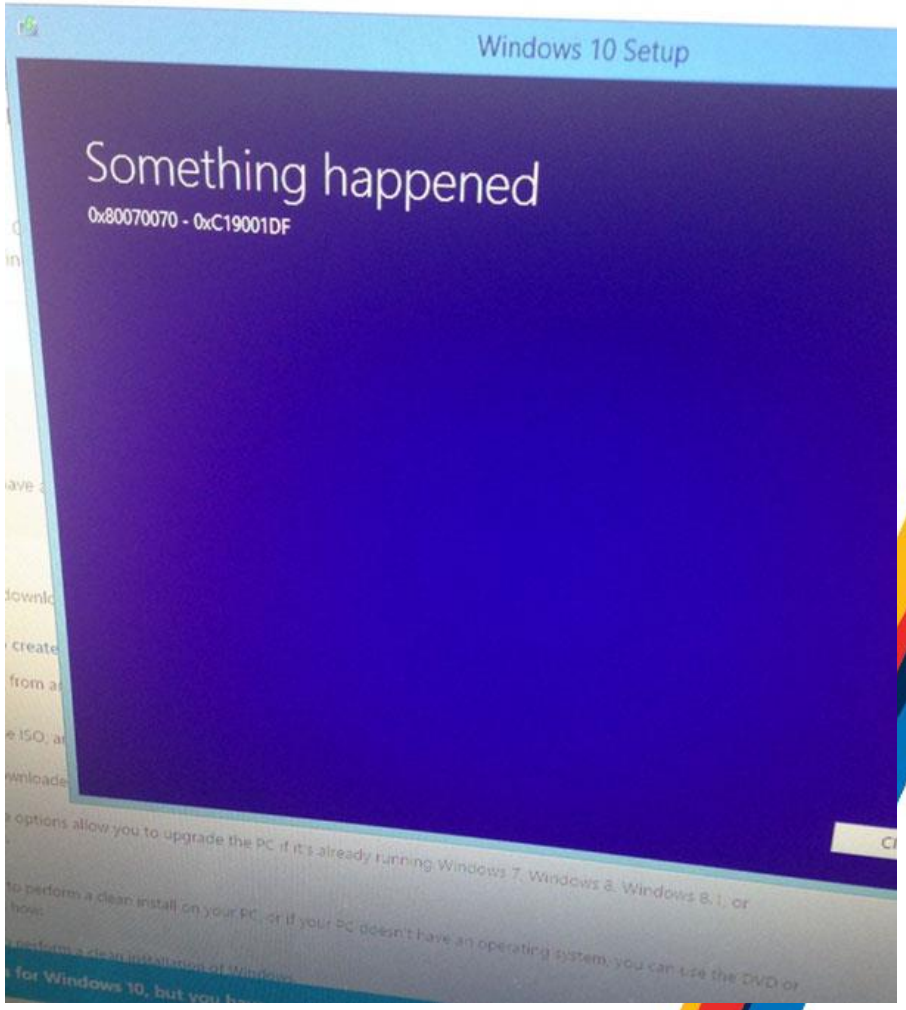
Nature / Conservation
Network Protocols
Network Utilities
News / Media
Newsgroups / Forums
Ning.com Widgets
Non-profits & NGOs
Nudity
P2P File Sharing
Personals / Dating
Phishing
Political / Legal
Pornography
Real Estate
Recreation
Religion
Remote Administration
Restaurants / Dining / Food
SCADA Protocols
SMS Tools
Search Engines / Portals
Sex
Sex Education
Shopping
Social Networking
Social Plugins

Software Downloads
Software Update
Spam
Sports
Spyware / Malicious Sites
Stealth Tactics
Suspicious Content
Tasteless
Translation
Travel
Twitter Clients
URL Filtering
Uncategorized
Vehicles
Video Conferencing
Violence
Virtual Worlds
VoIP
Weapons
Web Advertisements
Web Browser
Web Browser Acceleration
Web Conferencing
Web Content Aggregators
Web Services Provider
Web Spider

University of Victoria

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



University of Victoria

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

University of Victoria

Security Logs (certification)

- proxy logs

172.29.10.1, James, -, Y, 2/4/96, 8:22:56, SERVERNAME, PROXYNAME, -, www.yahoo.com, -, 80, 5277, 4792, 890, http, TCP, GET, http://www.yahoo.com/, TEXT/HTML, Inet, 200, -
172.29.10.1, James, -, Y, 2/4/96, 8:22:58, SERVERNAME, PROXYNAME, -, www.cnn.com, -, 80, 401, 5501, 1104, http, TCP, GET, http://www.cnn.com, IMAGE/GIF, VCache, 304, -
172.29.10.1, James, -, Y, 2/4/96, 8:22:59, SERVERNAME, PROXYNAME, -, www.atw.fullfeed.com, -, 80, 471, 3280, 1104, http, TCP, GET, http://www.atw.fullfeed.com/atw/gfx/ispcdeco.gif, IMAGE/GIF, VCache, 304, -
172.29.10.1, James, -, Y, 2/4/96, 8:22:59, SERVERNAME, PROXYNAME, -, www.atw.fullfeed.com, -, 80, 231, 638, 1094, http, TCP, GET, http://www.atw.fullfeed.com/atw/gfx/www.gif, IMAGE/GIF, VCache, 304, -
172.29.10.1, James, -, Y, 2/4/96, 8:22:59, SERVERNAME, PROXYNAME, -, www.atw.fullfeed.com, -, 80, 371, 4745, 1112, http, TCP, GET, http://www.atw.fullfeed.com/atw/gfx/intouch-icon.gif, IMAGE/GIF, VCache, 304, -

- antivirus logs

Date, Location, Malware Name, Action, Status, Alert

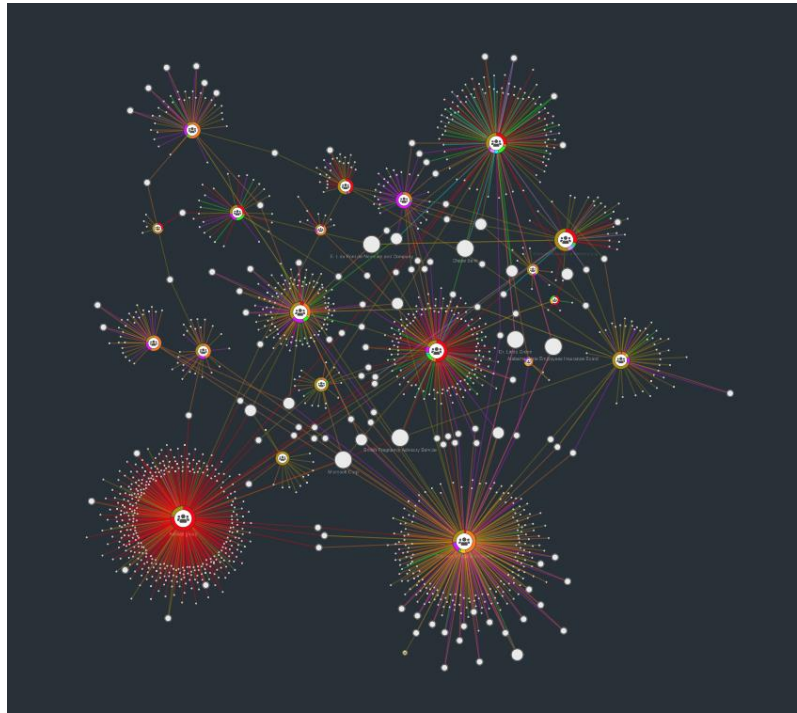
12/3/2019 08:30:00, c:\windows\system32\driver.exe, Trojan.Backdoor, Quarantine, Success
12/3/2019 08:30:00, c:\progra~1\flash\file.dll, Unwanted Application, Ask, Success
12/3/2019 08:30:00, c:\temp\ssaver.scr, BrowserHijack, Detect, Success
12/3/2019 08:30:00, c:\users\john\downloads\attachment.pdf, Adware, Quarantine, Success
12/3/2019 08:30:00, c:\windows\test.bat, HackTool, Detect, Success

- netflow data

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Pkts	Bytes	Flows
2010-09-01 00:00:00.459	0.000	UDP	127.0.0.1:24920	->	192.168.0.1:22126	1	46	1
2010-09-01 00:00:00.363	0.000	UDP	192.168.0.1:22126	->	127.0.0.1:24920	1	80	1

University of Victoria

Helps to be able to visualize and analyze data (eg. Gephi)

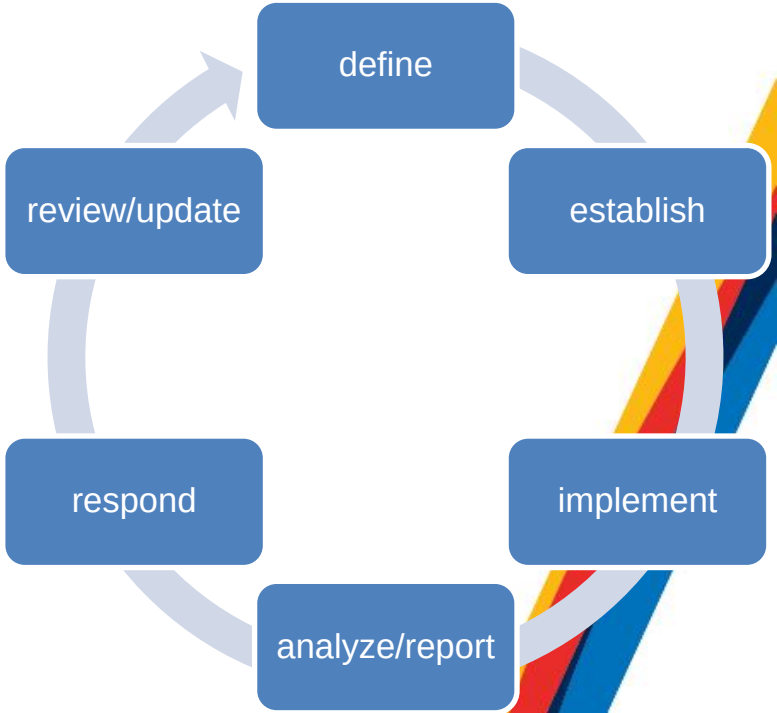


Monitoring

- 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

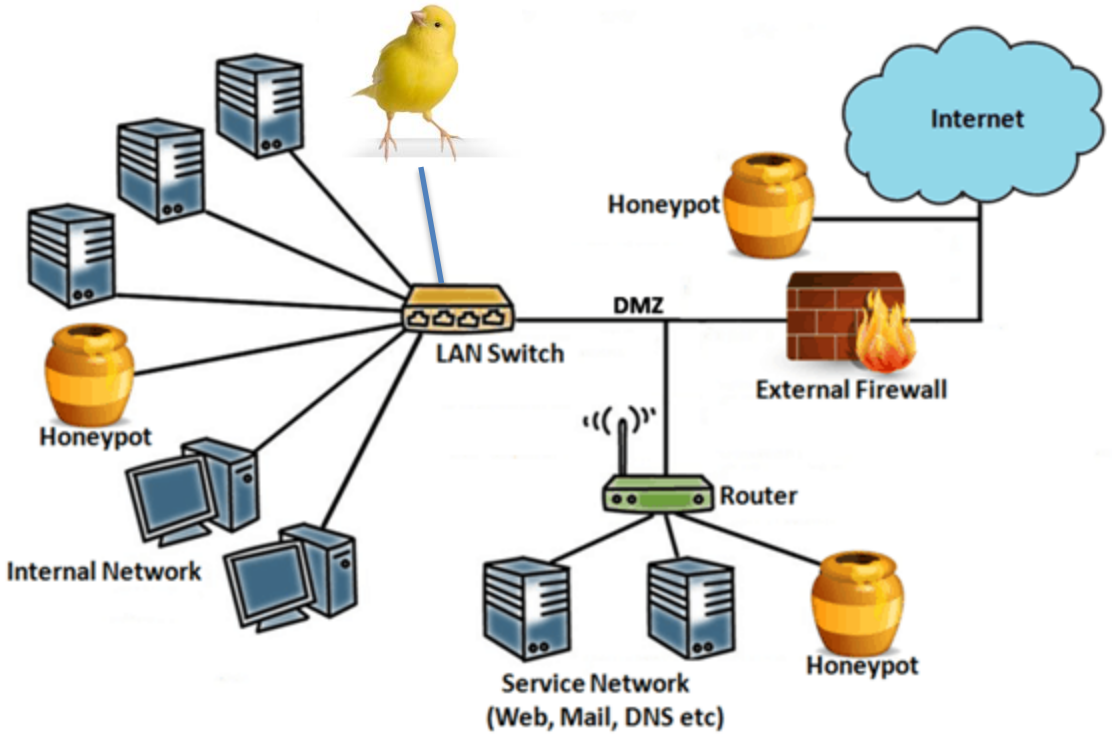
NIST monitoring:



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

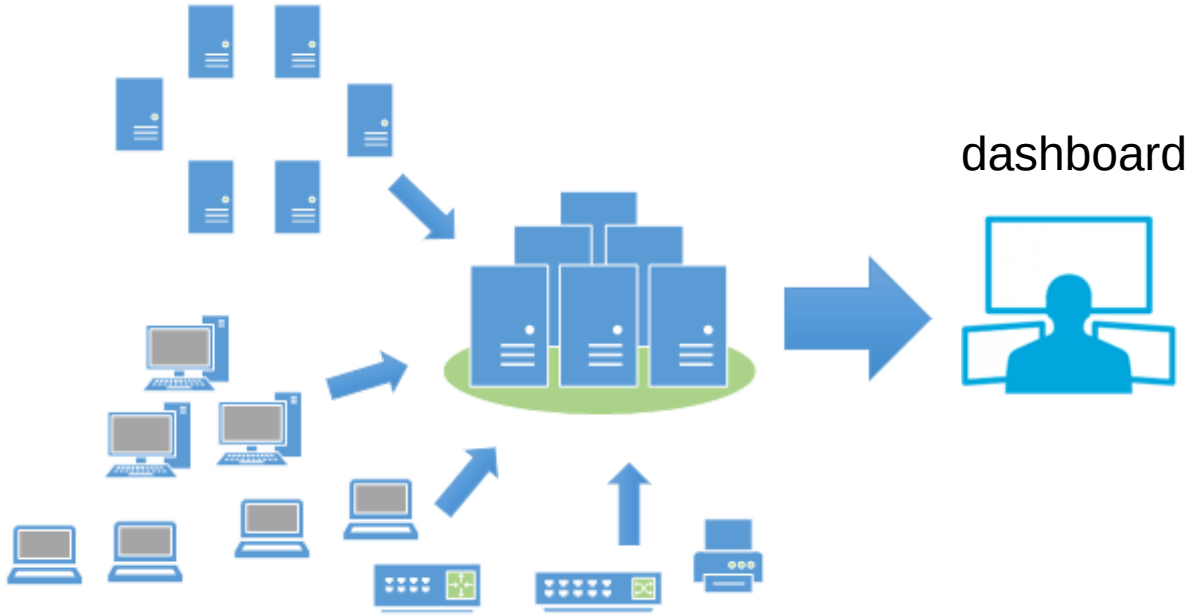


University of Victoria

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



University of Victoria

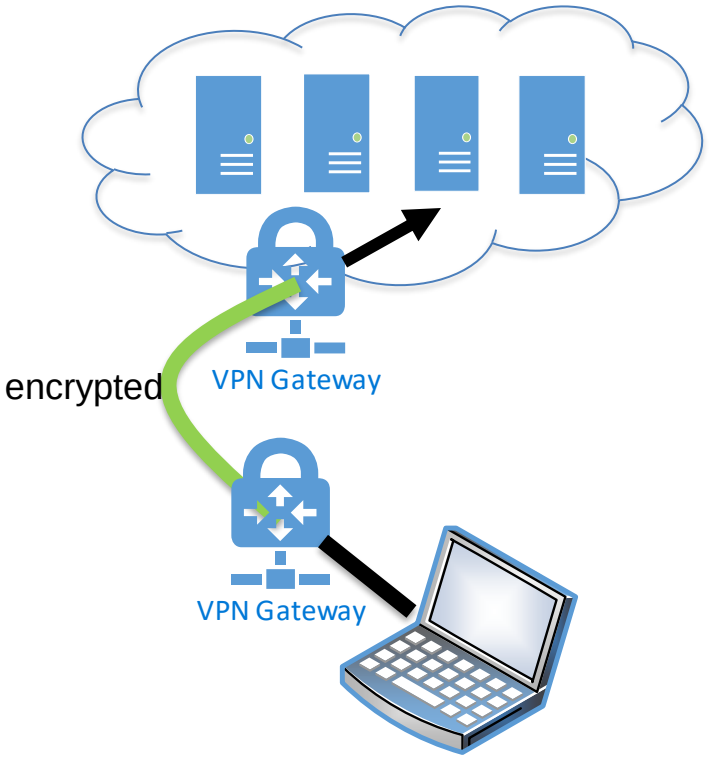
SIEM

- 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

University of Victoria

VPN (Virtual Private Network)

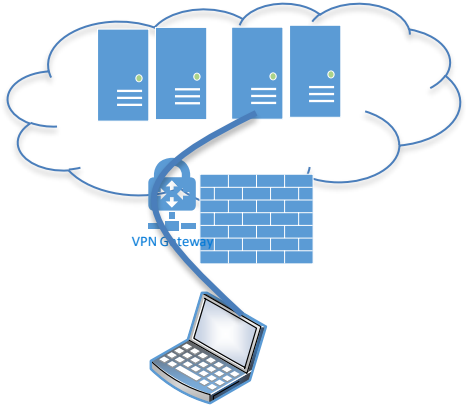
- secure access to other systems
- traffic is encrypted while in the "tunnel"
- best used with strong authentication



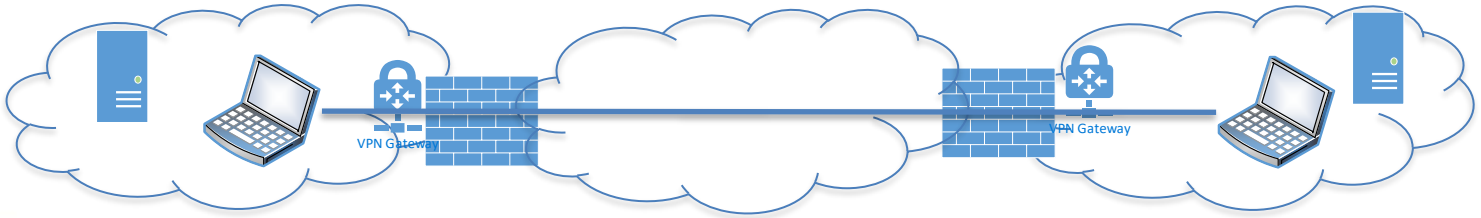
University of Victoria

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



University of Victoria

Strong Authentication

Multifactor Authentication

Factors:

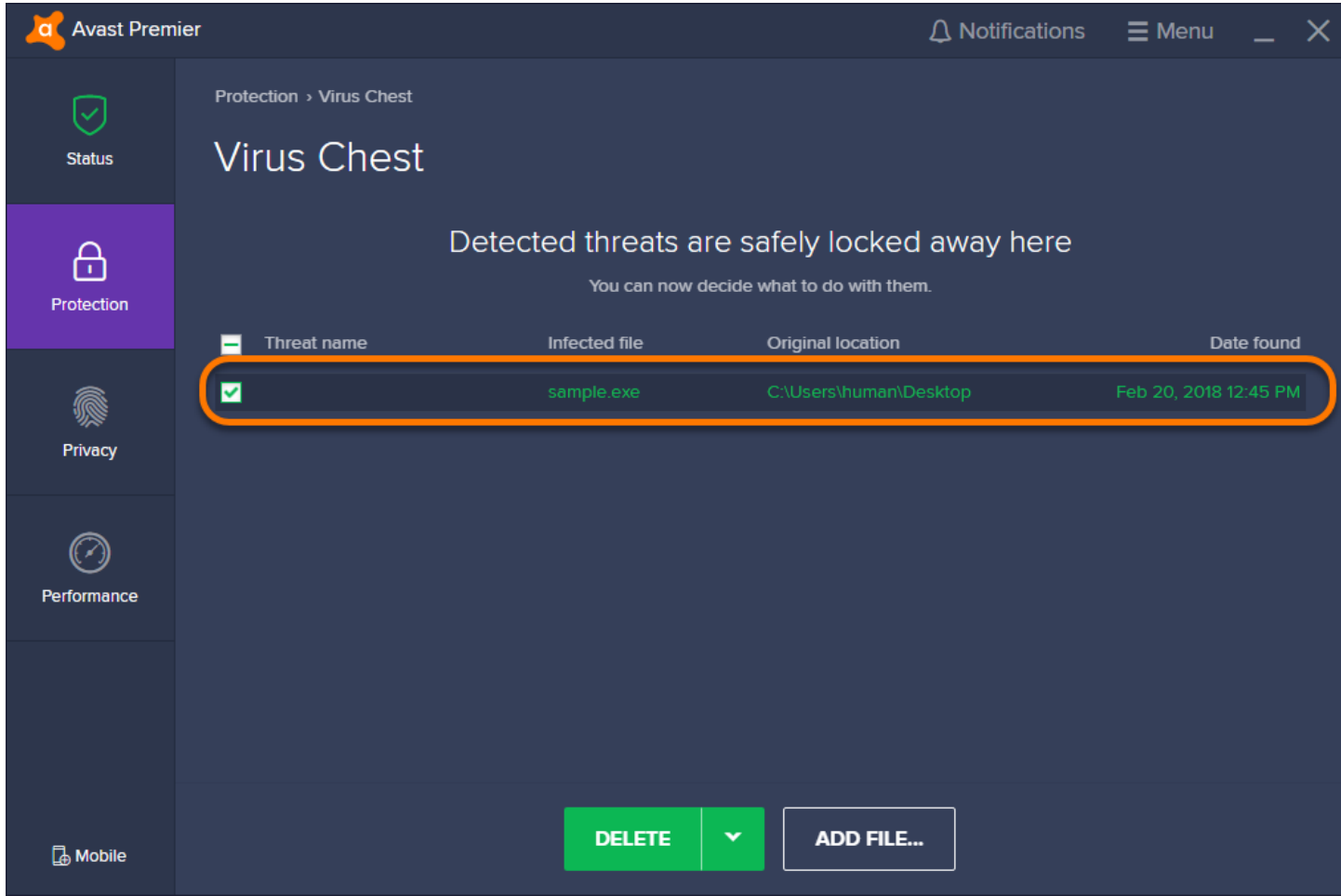
- something you know (eg. password, PIN)
- something you have (eg. token or phone)
- something you are (eg. fingerprint, iris)

…2 or more of the above…

University of Victoria

Anti-virus

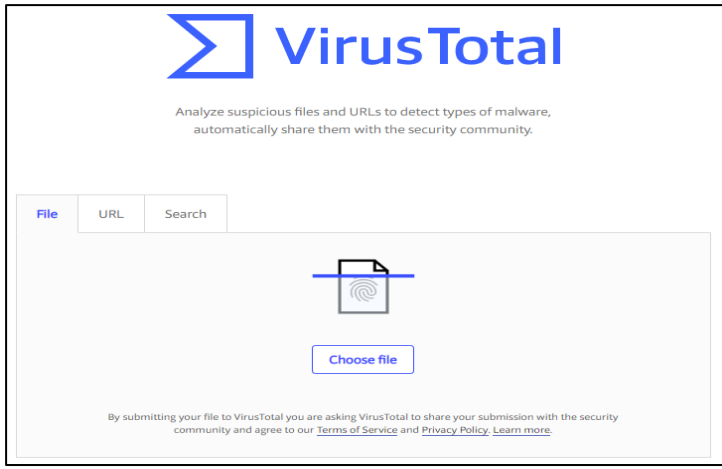
- some AV is very basic and offers very limited protection
- may use a software firewall in addition to a hardware firewall and anti-malware
- avoid virus, browser hijacking, infected attachments, malicious links, etc.

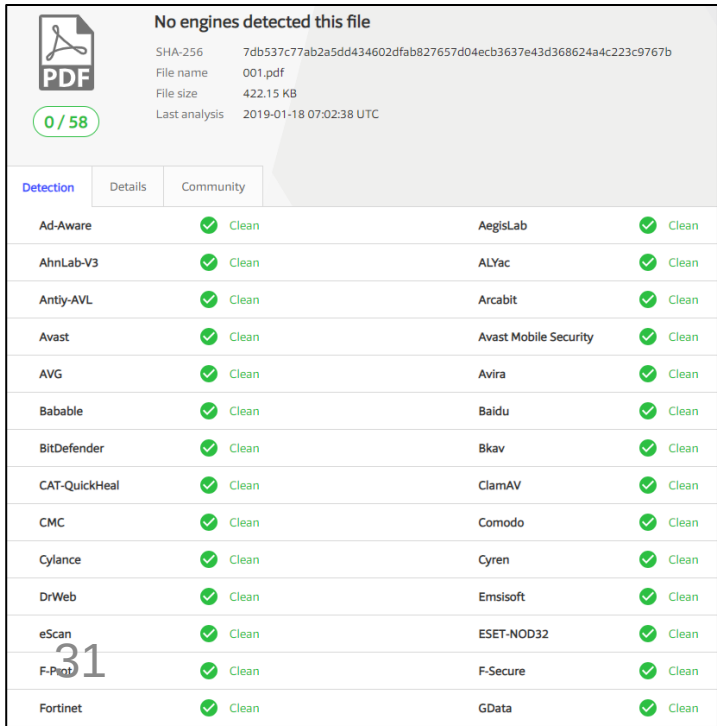


University of Victoria

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





University of Victoria

Example: Malware

Certification

- data
  - full packet capture
  - session data — summary data between devices, conversations, flows
  - transaction data — application records derived from network traffic; more connection-level info (eg. HTTP, SMTP data)
  - statistical data — summary or profile of network traffic
  - metadata — data about the flow (eg. what netflow captures)
  - alert data — identified by tools as information about potential attacks

- also
  - agent-based and agentless protection – some solutions have an agent that goes on the system, others don't
  - evasion and obfuscation techniques (eg. tunneling, encryption, proxies)

University of Victoria

Summary

- build security in from the ground up
  - security by design
  - build in layers, defence in depth
- no organization globally is immune to attack
- doing the basics stops 80% of the problems
  - do the basics well
- prepare for the known, deal with the unknown

University of Victoria

SENG 460 / ECE 574
Practice of Information Security and Privacy

Incident Handling/Response

& Recovery

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

Objectives of this Session

1. educate on what incident handling and incident response are
2. identify those who will benefit from additional training
3. help organizations be better prepared for the next incident

University of Victoria

Learning Outcomes

- prepare for incidents
- differentiate between an event and incident
- understand the different roles required
- effectively communicate during incidents
- capture necessary notes and evidence
- value of conducting exercises and drills
- confidence assisting your organization through security incidents

University of Victoria

Incident Handling & Incident Response

- organizations will be judged not only on their ability to prevent but detect and respond
- significant demand across organizations for incident response (IR) including “on retainer”
- shortage of skilled incident handlers, incident responders
- shortage of economic training options
- how prepared is your organization?

Dilbert by Scott Adams

University of Victoria

What this workshop is

- introduction to security incident handling with some incident response
- familiarity with concepts and approaches
  - cover learning outcomes and avoid common pitfalls
- opportunity to share experiences, ask questions

learning outcome

common pitfall

University of Victoria

What this workshop is not

- incident management
- technical or ethical hacking
- investigations/forensics
- exhaustive
- substitute for experience
- guarantee you will be successful

University of Victoria

Incident Handling & Incident Response

- which traits are desirable?
  - ❑ calm
  - ❑ hesitates
  - ❑ ambiguous
  - ❑ unitasker
  - ❑ timid
  - ❑ quiet
  - ❑ luddite
  - ❑ non-security
  - ❑ concise
  - ❑ high stress
  - ❑ excitable
  - ❑ impulsive
  - ❑ clear
  - ❑ multitasker
  - ✓ ❑ assertive
  - ❑ loud
  - ❑ technical
  - ❑ security
  - ❑ verbose
  - ❑ low stress
  - ❑ takes initiative
  - ❑ communicates
  - ❑ logical
  - ❑ decisive
  - ❑ resourceful
  - ❑ polite
  - ❑ takes risks
  - ✓ ❑ sense of urgency
  - ✓ ❑ bias for action
  - ❑ many others….

University of Victoria

Definitions

- incident handling
  - logistics, communications, coordination, and planning functions needed in order to resolve an incident in a calm and efficient manner
  - part of goal is to determine if service should be restored
  - measured in minutes

- incident response
  - all of the technical components required in order to analyze and contain an incident
  - measured in minutes

Incident Handling
procedural and logistical response to an incident

Incident Response
technical response to an incident

University of Victoria

Definitions

- incident management
  - unplanned interruption to an IT Service or reduction in the quality of an IT service (also if redundancy is impaired)
  - ensures that normal service operation is restored as quickly as possible and business impact is minimized
  - goal is to restore service
  - measured in minutes

- investigations
  - *investigating something or someone; formal or systematic examination or research to uncover evidence in support of*
    whether a set of circumstances is likely to have taken place
  - examining a real or suspected violation of policy or law to determine who did what, when
  - measured in days, weeks

University of Victoria

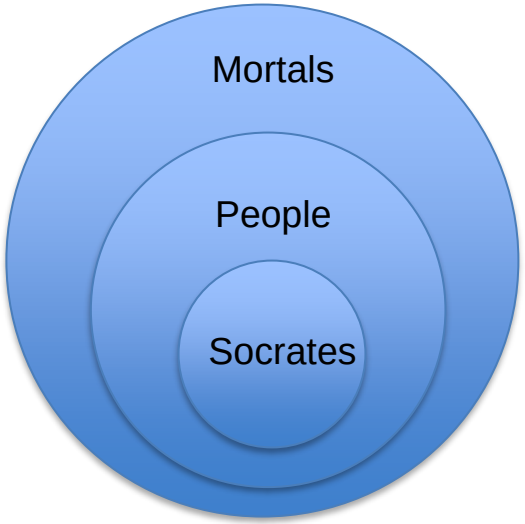
Definitions

- **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 (eg. DDoS)
  - a vulnerability that has been exploited
- **breach**: system has been compromised
- **compromise**: vulnerability that has been exploited
- **vulnerability**: exposure that if exploited would be an incident
- **exploit**: turns a vulnerability into an incident

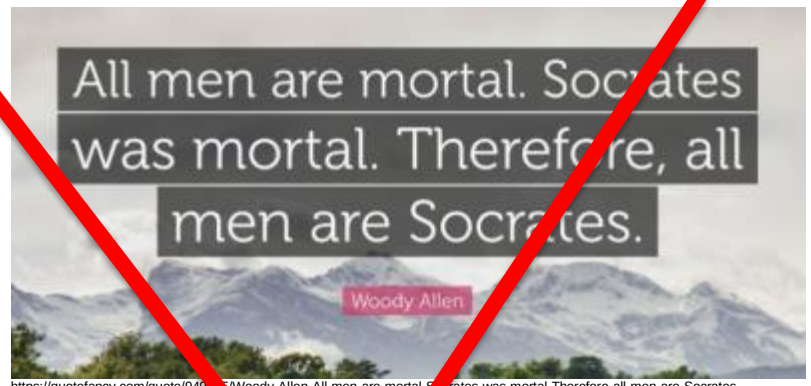
University of Victoria

Deductive Reasoning & Logic

All people are mortal.
Socrates is a person.
Therefore Socrates is mortal.



VS



https://quotefancy.com/quote/949[illegible]/Woody-Allen-All-men-are-mortal-Socrates-was-mortal-Therefore-all-men-are-Socrates

$P \supset Q$
$Q \supset R$
$P \supset R$

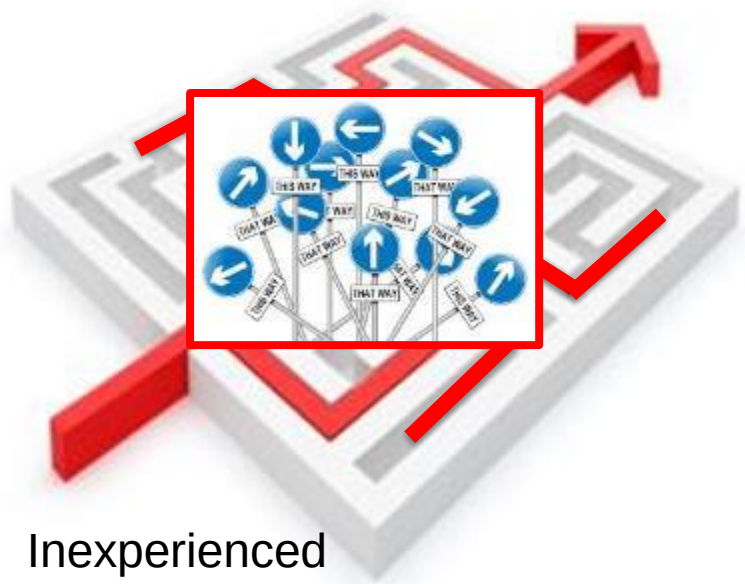
P	Q	If P then Q
T	T	T
T	F	F
F	T	T
F	F	T

University of Victoria

Approaches

Attacker

Hacker Mindset



Inexperienced

Incident Handler

Definition Summary

- incident handling and incident response are often used interchangeably but are different for this workshop
- incident handling & incident response share some similarities with incident management and investigations but are not the same thing
- important to follow the evidence and make data-driven decisions though this isn't always possible
- designed to **prevent, detect, deny, disrupt, degrade, deceive, corrupt, or destroy** the attack by any legal means possible

University of Victoria

Definition Summary

- **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 effectiveness or efficiency**
- **deceive** — **fool the attacker**
- **destroy** — **reduce the attacker's capability, damage system or entity**

…the attack by any legal means possible

University of Victoria

Additional Notes

- process does not focus on the theoretical, abstract, or illogical
  - not a democracy or brainstorming exercise
- cannot afford to be hampered by ambiguous or confused people, irrelevant questions, slow processes
- **minutes matter** – consider the effect of waiting for approvals
- process does not stop on Friday or at 5 pm*
  - keep driving until the risk has been mitigated
  - no prolonged breaks until organization is whole
  - follow the process deliberately and efficiently

- get resourceful, there are many ways to solve problems – often you're treating the symptoms when you should be going to the source
  (eg. prying attacker's fingers off the keyboard)

University of Victoria

Additional Notes (con't)

- make decisions based on the available information
  - goal is to be able to say you did what you could with the information available at the time
- this relies heavily on being able to discern fact from fiction
  - what you know vs. what you believe (or think or want)
  - deal with what is the case not what is supposed to be the case (eg. diagram vs. current config)
- go to the mattress, don't give up
  - know when you are running out of options
  - if can't stop it then slow it down
  - ask for help (eg. group members, peers, third party)

University of Victoria

Objectives of Incident Response

- Minimize business losses and subsequent liabilities to the company
- Minimize the possible impact of the incident in terms of information leakage, corruption and system disruption
- Ensure that the response is systematic and efficient and that there is prompt recovery for the compromised system;
- Ensure that the required resources are available to deal with incidents, including manpower and technology
- Ensure that all responsible parties have a clear understanding regarding the tasks they need to perform during an incident by following predefined procedures
- Ensure that all response activities are recognised and coordinated
- Prevent further attacks and damage
- Deal with related legal issues

University of Victoria

https://www.infosec.gov.hk

Objectives of Incident Response

- Mitigate risk
- Prevent incidents
- Decrease frequency of incidents, ensure service availability
- Manage the incident, evaluate damage potential
- Timely containment
- Minimize damage/loss
- Recovery, rebuild systems, remove traces, restore service/data
- Preserve evidence, identify the attacker

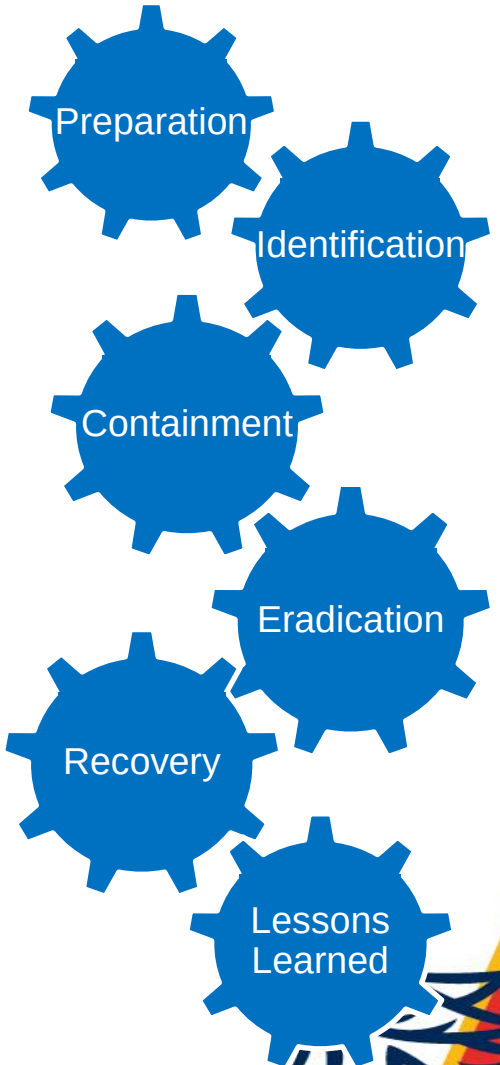
  :
- Continuous improvement

Be better prepared, more organized, efficient, effective so you are faster to respond, contain, and limit damage by minimizing spread…

University of Victoria

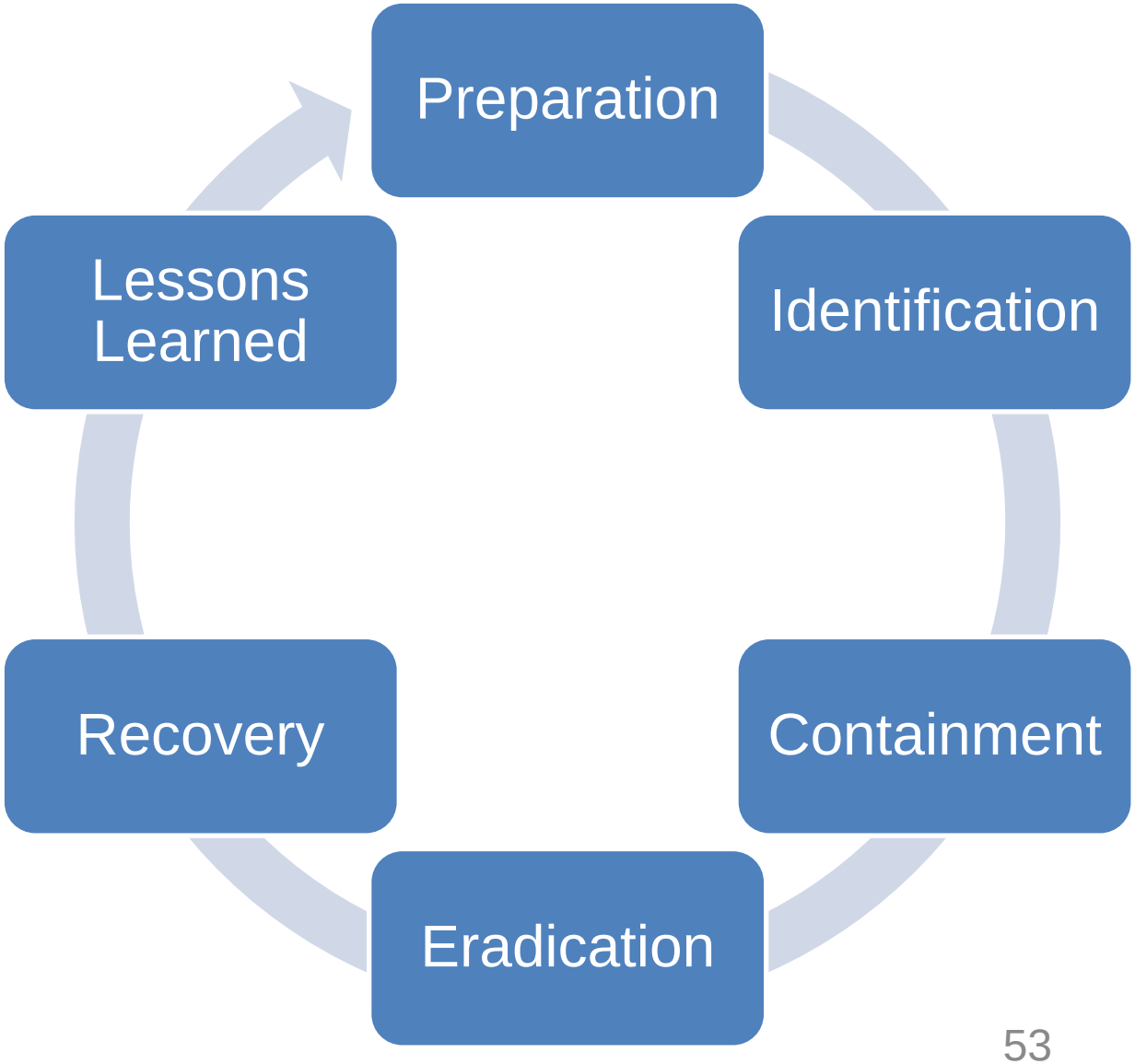
PICERL Process

- **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
- **lessons learned**: identify any opportunities for improvement

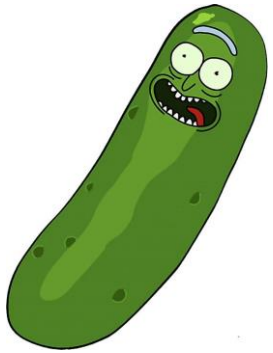


University of Victoria

PICERL Process



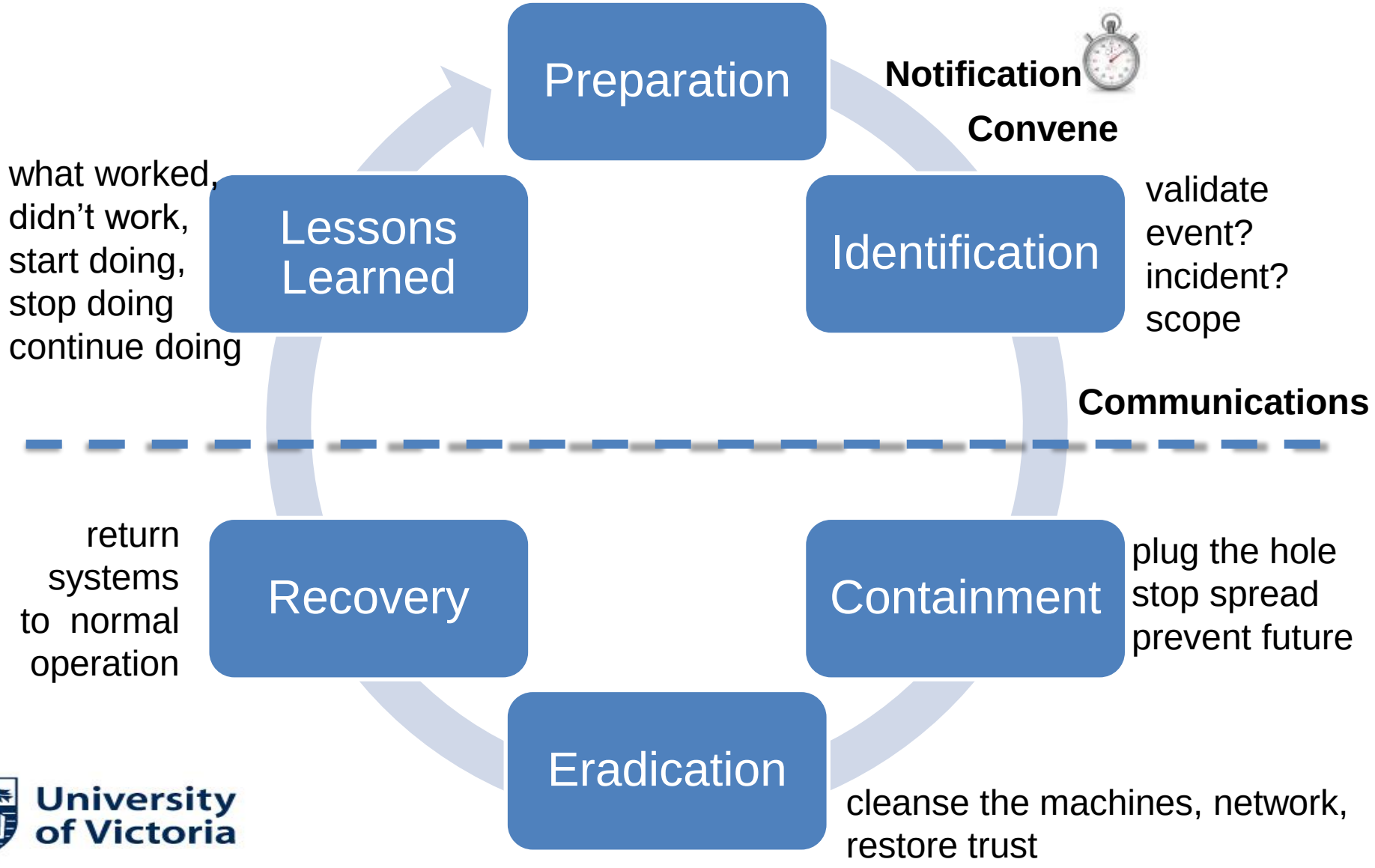
I SAID PICERL



NOT PICKLE

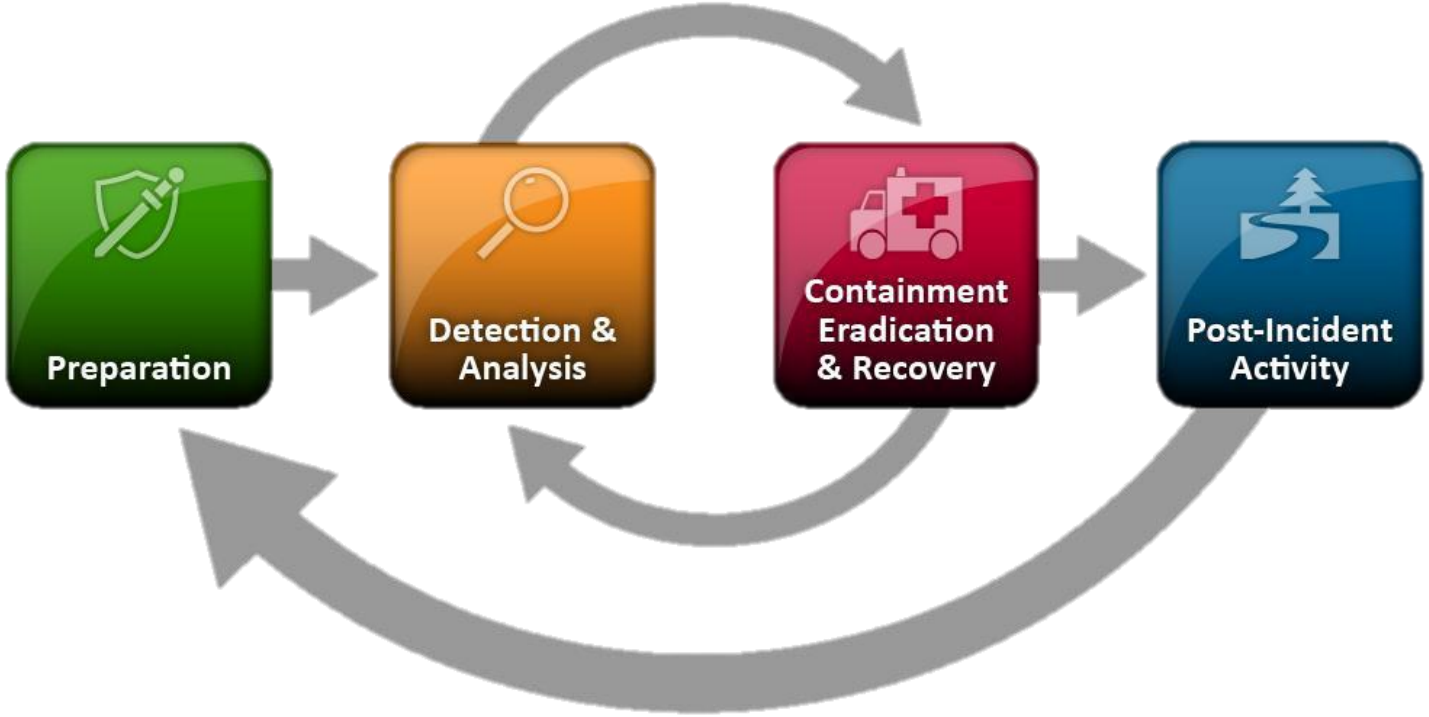
University of Victoria

PNCICERL Process



University of Victoria

Similar Process



NIST 800-61

Or this one:

- Preparation
- Detection, analysis, and escalation
- Containment
- Eradication
- Recovery
- Lessons learned/implementation of new countermeasure

Or another approach:

- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Remediation
- Lessons learned

University of Victoria

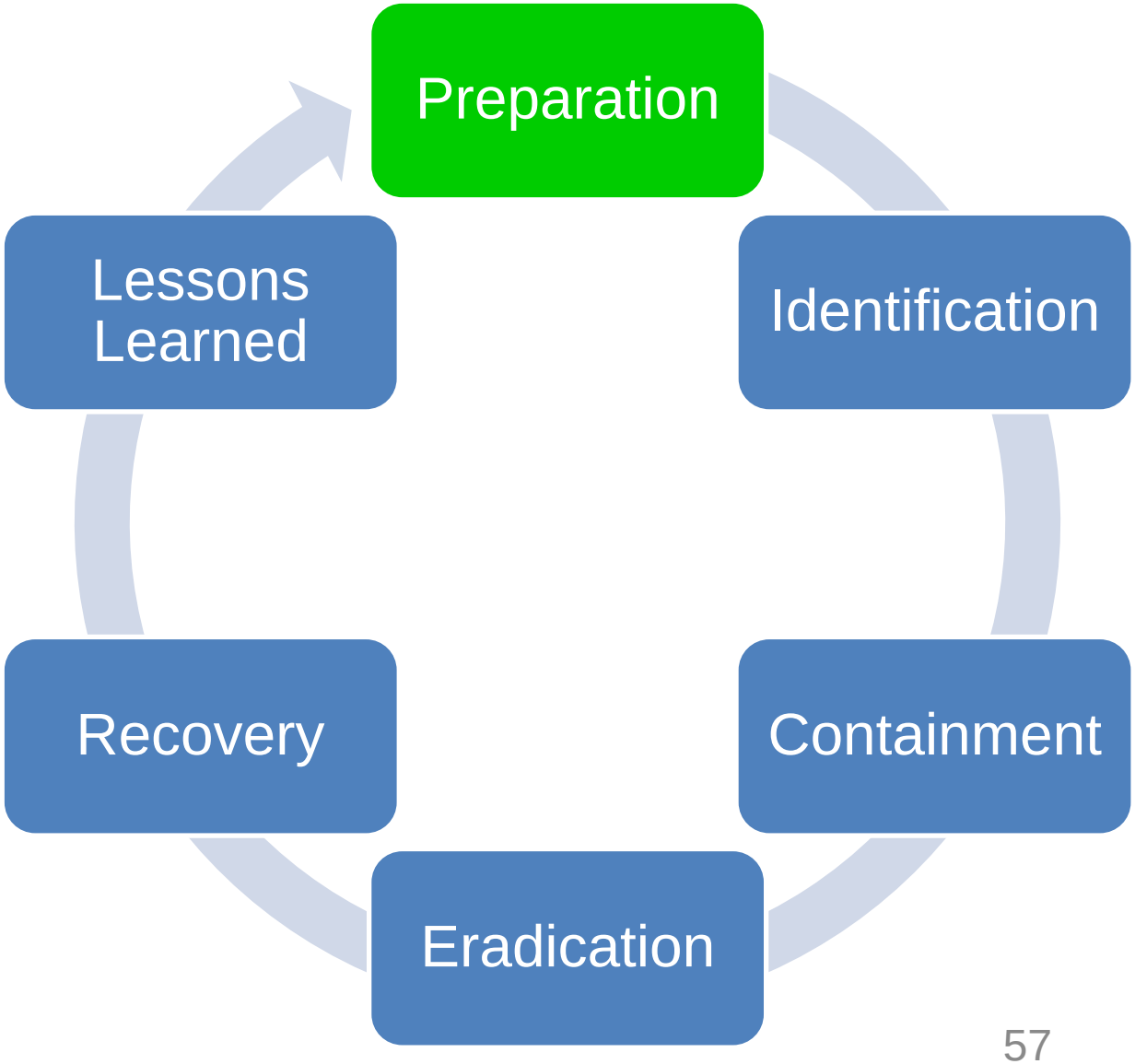
How prepared are you?

"By failing to prepare you are preparing to fail."
- Benjamin Franklin

"No battle plan survives contact with the enemy."
- Helmuth von Moltke

University of Victoria

PICERL Process



University of Victoria

Preparation

- build **incident response plan**
  - establish mandate, delegate authority, decisions (eg. internet)
  - review/update annually
- ensure you have an **incident response team**
  - dedicated, virtual, or on-retainer
  - invest in team, training
- document **roles and responsibilities**
  - education and training
  - pre-authorization for spending and decision-making
- conduct **exercises**, drills regularly
  - most of the scenarios are known in advance
  - prepare for the known so can focus on the unknown
  - test the plan, team, tools

Preparation

- understand environment
  - network diagrams
  - crown jewels (critical systems and data)
  - vendor environment, supply chain
  - people, processes, tools, technology
  - understand dependencies, prepare for each component of plan to fail
  - keep printed copies in case network unavailable

Preparation

- understand controls available
  - prevention where possible
  - are the controls sufficient to mitigate risk to an acceptable level?
  - ensure backups captured, protected, tested
  - time synchronized on systems, logs
  - logging, retention, monitoring, alerting on systems

- hygiene level technical controls
  - firewall, intrusion prevention, web content filtering, email content filtering, anti-malware
  - what capabilities do these platforms have that will assist the incident response efforts
  - logs and visibility are key

University of Victoria

Preparation

- understand impacts
  - how much downtime can you tolerate?
  - how much will it cost you?
  - what will your liability be?
  - prioritized list of assets and downtime

- prepare war room and conference bridge(s)
  - adequate space, seating, table, clock
  - communications (phones, network, TV)
  - collaboration aids (whiteboards, flipcharts, printer, shredder, projector)
  - create capacity, scalability, sustainability (shifts, food/water)

University of Victoria

Preparation

- establish communications plan in advance
  - reporting frequency
  - recipients of communication
  - store information off of the network
  - include call out list
  - alternatives to network, email, VoIP
  - know what communications options you have

Incident Response on Retainer

- establish agreements in advance
  - if you pay 0 that could be the level of value you're getting
  - if you do pay a recurring fee ensure:
    - annual plan review/update
    - regular exercises
    - familiar with environment in advance
    - preferred pricing
    - established SLA, response times

- there are few organizations available to help in the event of an incident and even less competent ones

University of Victoria

Incident Response on Retainer

- engaging external assistance is seen as a sign of maturity
  - realize you could benefit from help and know to ask for it
- despite everything going on, ability to step back and realize even if you could get out the other side of this, that others can help
- external organizations may be more able to assist with Incident Response than Incident Handling
- firms may be better able to help with IR than IH or support in a coaching capacity

University of Victoria

Roles

- **incident handler**
- incident response, forensics
- **communications**, media relations
- **note-taker**
- investigations
- law enforcement, intelligence
- privacy
- legal
- regulatory
- vendor manager, vendors, service provider
- sysadmins, network technicians
- others… human resources?!

University of Victoria

Roles – MUST BE SOMEONE LEADING

- 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 (help them!)
  - often have 6 people telling them what should be done during and after
  - ferries between management and technical bridge
  - establishes an update frequency
  - buffer in front of incident response team

University of Victoria

Note-taking

- date/time/name
- key decisions, actions, updates

F5

Date	Name	Page
2017-08-16	John D.	1 of 8

Time:	Action:	Type:
14:03	Event reported	Update
14:08	Convened group	Update
14:13	Validated incident	Update
14:16	Notified executive, privacy, communications	Update
14:18	Assessed severity as medium	Update
14:28	Shutdown affected server to contain incident	Decision
14:33	Server drives to be captured by forensics (Mary S.) Server to be rebuilt by hosting (Mike F.) and returned to service at 17:00	Action

Note-taking

- Incident name, Author, Date, Summary
- Attacker description, actions, capabilities, motivation
- Victim description, impacts, affected assets
- Discovery to date
- Detect future actions
- Deny block the attacker
- Disrupt cause attack to fail
- Degrade slow the attack
- Deceive fool the attacker
- Destroy reduce attacker's capability
- Correlation with other attacks

If you are going too fast to take notes, you are going too fast.

Communications

- communications is a 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 the incident handler

Incident response team members should have other skills in addition to technical expertise. Teamwork skills are of fundamental importance because cooperation and coordination are necessary for successful incident response. Every team member should also have good communication skills. Speaking skills are important because the team will interact with a wide variety of people, and writing skills are important when team members are preparing advisories and procedures. Although not everyone within a team needs to have strong writing and speaking skills, at least a few people within every team should possess them so the team can represent itself well in front of others. ~ NIST 800-61

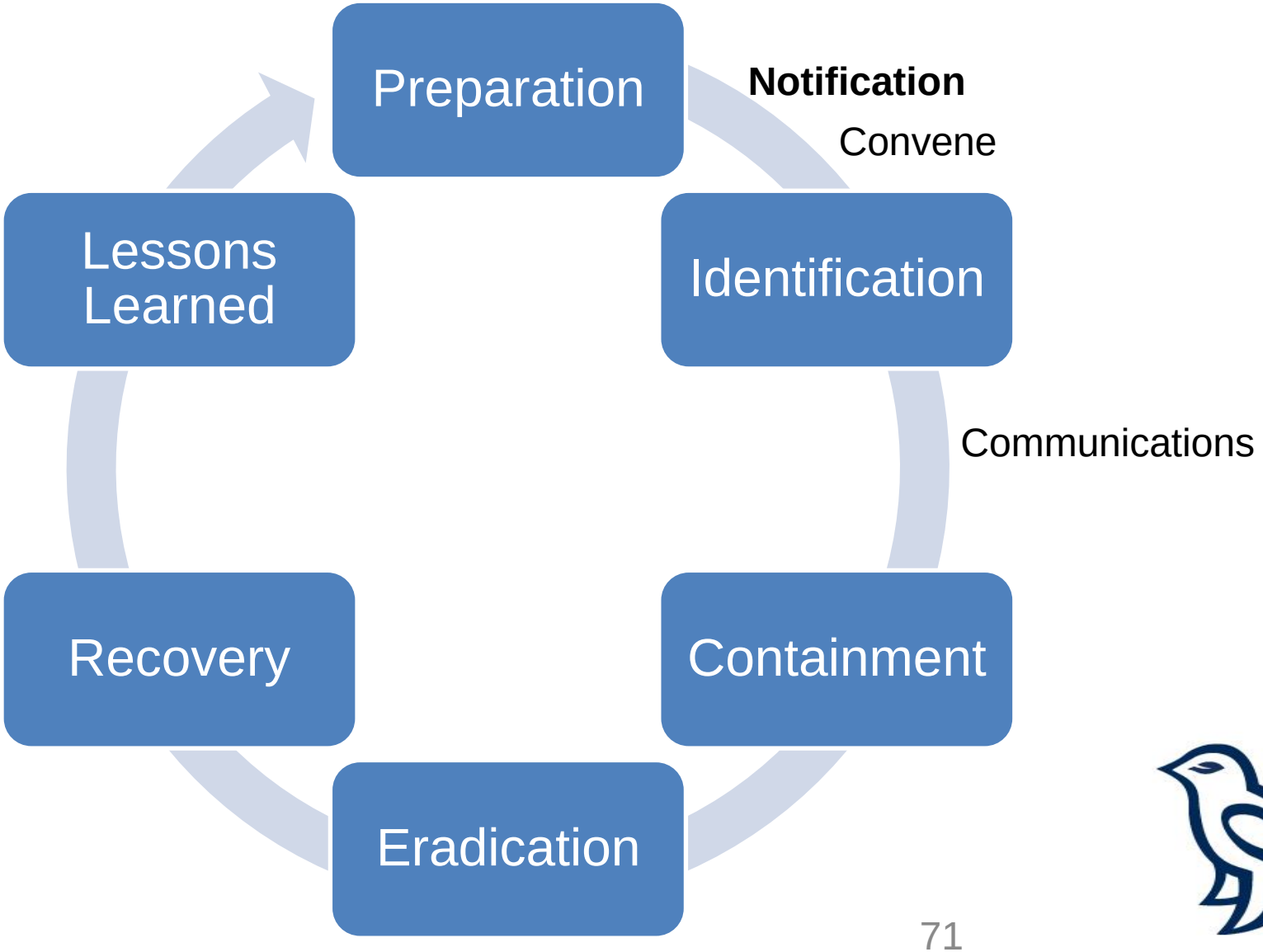
University of Victoria

Incident Response

- have necessary tools to be successful with contents of your 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)

University of Victoria

PNCICERL Process



University of Victoria

Notification

- report the issue
  - ensure you have policy requiring employees to report suspicious events immediately
  - rather have false positives than false negatives

- **do not capture the details in a public ticketing system**

- monitor and alert

- respond and escalate 24/7

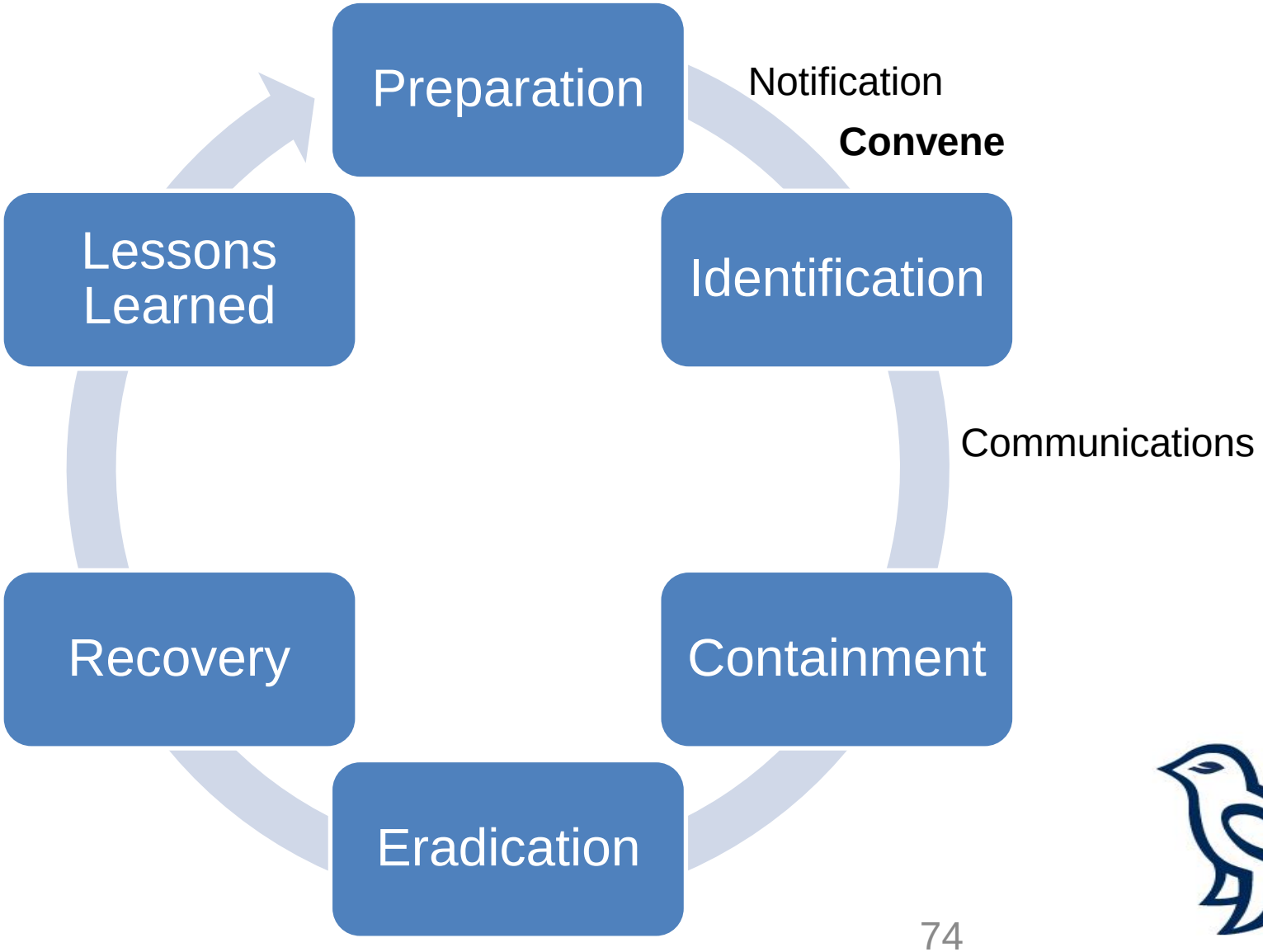
University of Victoria

Notification

- preparation
  <notification>
  <convene>
- identification
  <communication>
- containment
- eradication
- recovery
- lessons learned
  - notification
  - strong authentication
  - personal/business

University of Victoria

PNCICERL Process



University of Victoria

Convene

- bring together everyone who knows about the issue
- remind them of their responsibility to maintain need-to-know, instruct them not to share it
  - otherwise repercussions can be counterproductive
  - any requests for information should be forwarded to the communications person
- ensure the right individuals are present
  - summon those who are absent
  - remove those who should not be there
  - this is not a “more the merrier” case
- contain the information (and misinformation)

University of Victoria

Convene

- communication is vital to incident handling and incident response
  - compartmentalize asks where necessary
  - define circumstances when employees, customers, and partners may or may not be informed
  - communicate the importance when making requests (pre-arrange within organization)
  - eg. use key words “this request is in relation to an ongoing security incident”

- break/fix and security incidents trump most business processes but not all (eg. human safety, IPO, product/service launch)

University of Victoria

Convene

- convene in war room or conference bridges
  - be wary of VoIP and email unless encrypted
  - consider POTS conference bridge
- two different locations/bridges
  - management
  - technical
- incident handler typically ferries between
- establish procedure for communicating securely during an incident
  - use encrypted and/or out of band channels to share information where possible

University of Victoria

Convene

- have the courage to:
  - ask individuals to leave
  - ask individuals to stop speaking
  - tell people “no”
  - accept help
  - engage a third party
  - make decisions where others won’t
  - take control

- styles vary however this is the time for your authoritative management style to flourish
  - not as participative, not brainstorming
  - may request groups to go into a breakout room to solve specific problems and return

University of Victoria

Sample Principles

- do no harm, do not jeopardize human safety
- prosecute the attacker, hold them responsible
- keep it quiet, go undetected,
  ensure no-one finds out
- keep the system online
- resume business operations (fix the problem)

University of Victoria

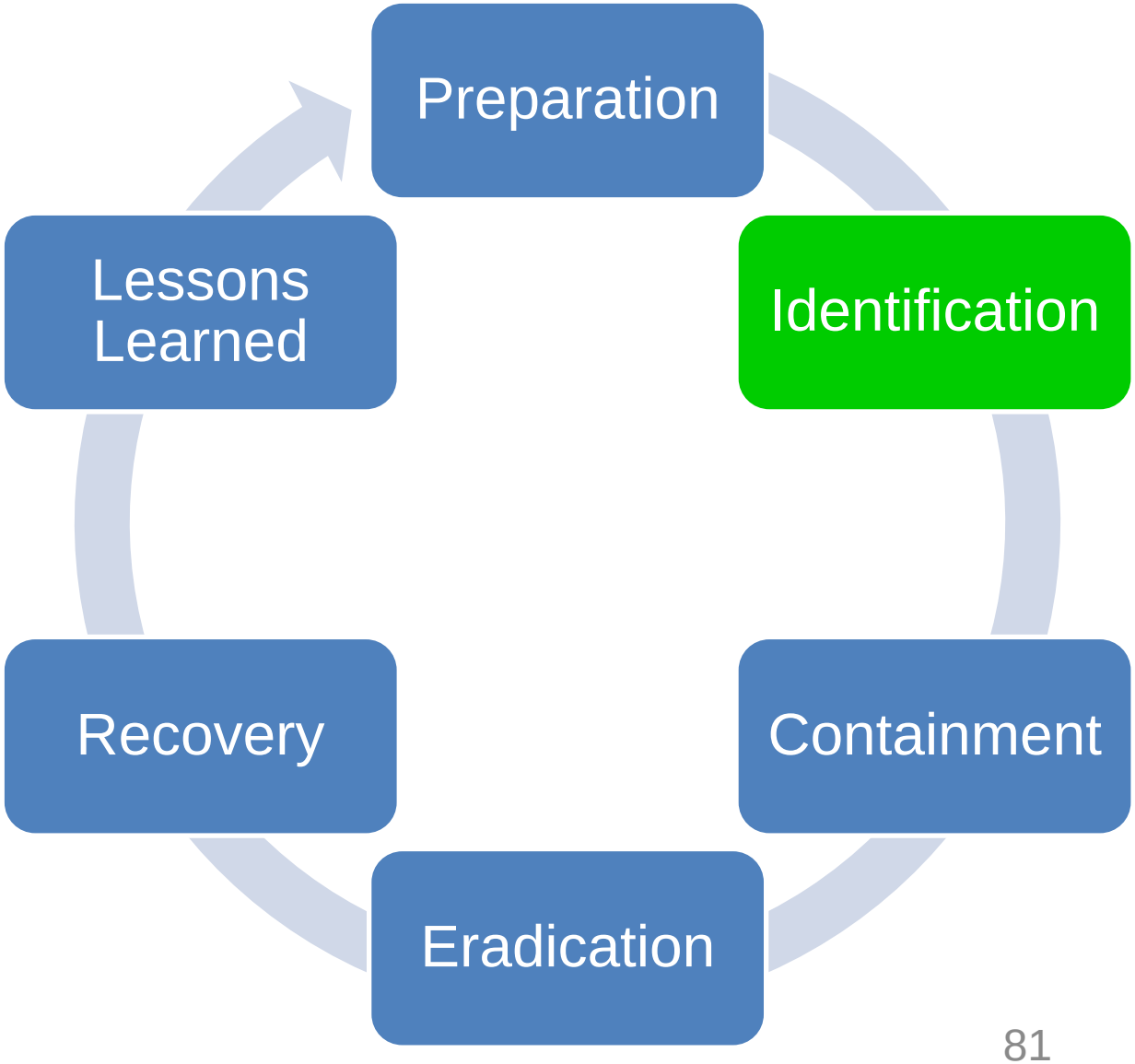
Public Safety – CCIRC (now CCCS)

- contact in the event of an incident
- will assist as possible
- able to sanitize info and share with others
- perform malware reverse engineering

BEhavioural Analysis using Virtualization and Experimental Research (BEAVER)

GeekWeek

PICERL Process



University of Victoria

Identification

- determine whether it is an event or an incident
  - validate and determine whether it is a distraction
- perform triage and ensure a common understanding of how it was detected, who is aware
  - type of threat if known, scope (how widespread)
  - whether isolated or part of a campaign
- determine urgency and initial impact
  - assess severity, rate it low/med/high
  - low if started and stopped, high if still ongoing
  - always high until you know the magnitude
- review information and actions taken to date
  - how long has it been going on (APT)
  - how long is it likely to continue (resources)
  - likely attack vector

University of Victoria

Severity

Category	Indicators	Scope	Action	Containment	Recovery
1 - Critical	Data Loss, Malware	Widespread and/or with critical servers or data exfiltrated	Implement SIRT, Incident Response Plan (Security Incident Created) Organization wide (reactive)	Possible reimage or Block access, containment etc… if no action in X amount of Time	May have to revert snapshots/recover data
2 - High	Theoretical Threat becoming Active – Zero Day Like (Vulnerability with no active exploits)	Widespread and/or with critical servers or data exfiltrated	Implement SIRT, Incident Response Plan (Security Incident Created) Organization wide (reactive)	Out of Band Patching, potential signatures/mitigation controls (proactive)	Scan and monitor for additional issues
3 - Medium	Email Phishing or Active spreading Infection	Widespread	Implement SIRT, Incident Response Plan (Security Incident Created) Organization wide (reactive)	Possible reimage or Block access, containment etc… if no action in X amount of Time	Purge exchange or file and folders
4 - Low	Malware or Phishing	Individual Host or Person	Notify SIRT and (Security Incident Created) Internal	Possible reimage or Block access, containment etc… if no action in X amount of Time	Purge exchange or file and folders

Event vs. Incident

Event:

An *event* is an observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, or a user sending email.

An example of an event can be:

- An email
- A phone call
- A system crash
- A request for virus scans to be performed on a file or attachment

Incident:

An adverse event in an information system, and/or network, or the threat of the occurrence of such an event. An *incident* is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. It implies harm or the attempt to harm.

An example of an incident can be:

- A violation of an explicit or implied security policy
- Attempts to gain unauthorized access
- Unwanted denial of resources
- Unauthorized use
- Changes without the owner's knowledge, instruction, or consent.

University of Victoria

Identification

- Examples of types of incidents

a) violation of explicit or implied security policy
b) unauthorized access
c) denial of service
d) unauthorized or inappropriate use
e) changes without owner's knowledge, instruction, or consent
f) malicious code

University of Victoria

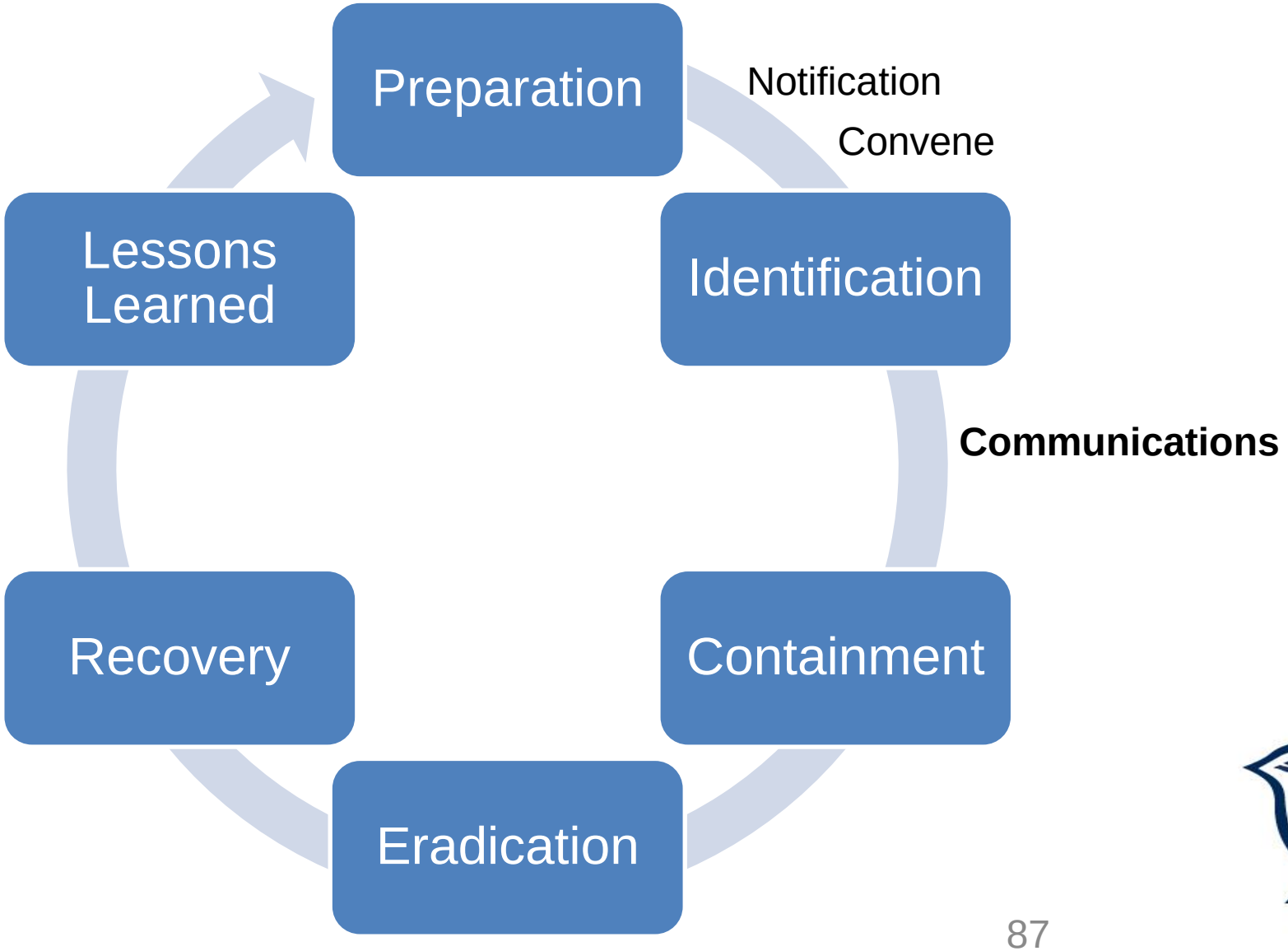
Identification

- Monitor abnormal events, e.g. error messages, suspicious events in logs, poor performance and unusual capacity growth.
- Determine type of problem and extent of impact.
- Start taking record using a standard incident logging form.
- Handle information with reference to the guideline on evidence collection.
- Make a full backup of compromised system as soon as you find it a real incident and store it in secure place.
- Capture records of incidents, e.g. auditing log, accounting log, etc.
- Inform the management and other "Right" people using the call list (IRT, ISP, network service provider…) and call tree (system owner notification).
- Enforce the "Need to Know" policy and use secure out-of-band communication channel when necessary.

University of Victoria

https://www.infosec.gov.hk/english/business/step_2.html

PNCICERL Process



University of Victoria

Communications – Videos

- sample video links

IBM:
https://www.youtube.com/watch?v=sHrgVqKW1RQ
https://www.youtube.com/watch?v=nG36lKhy7ko

Deloitte:
https://www.youtube.com/watch?v=qLg3e4TNQIU
https://www.youtube.com/watch?v=SRut3xTfAQY

University of Victoria

Event vs. Incident Exercise

University of Victoria

Communications

- notification requirements
  - who needs to know, what do they need to know
  - when do they need to know
  - who will notify them and how

- examples:
  - public safety for assistance
  - media relations
  - executive and Board of Directors,
  - customers/clients, vendors/partners, helpdesk
  - legal, regulatory, OIPC, privacy
  - **law enforcement**, intelligence
  - interconnected organizations (examples)

University of Victoria

Communications – Summary

- capture factual information
  - how was the problem initially discovered and reported?
  - how contained is the information, misinformation (eg. social media)?
- exercise discretion, compartmentalize as necessary
- know current status at all times
  - ensure status categories are understood in advance
    eg. investigating/validated/remediating/closed
- stakeholders will want information before you can provide it, and will want to know when it will be over
- prepare to answer questions what happened, why, who did it, how severe, whether security inadequate

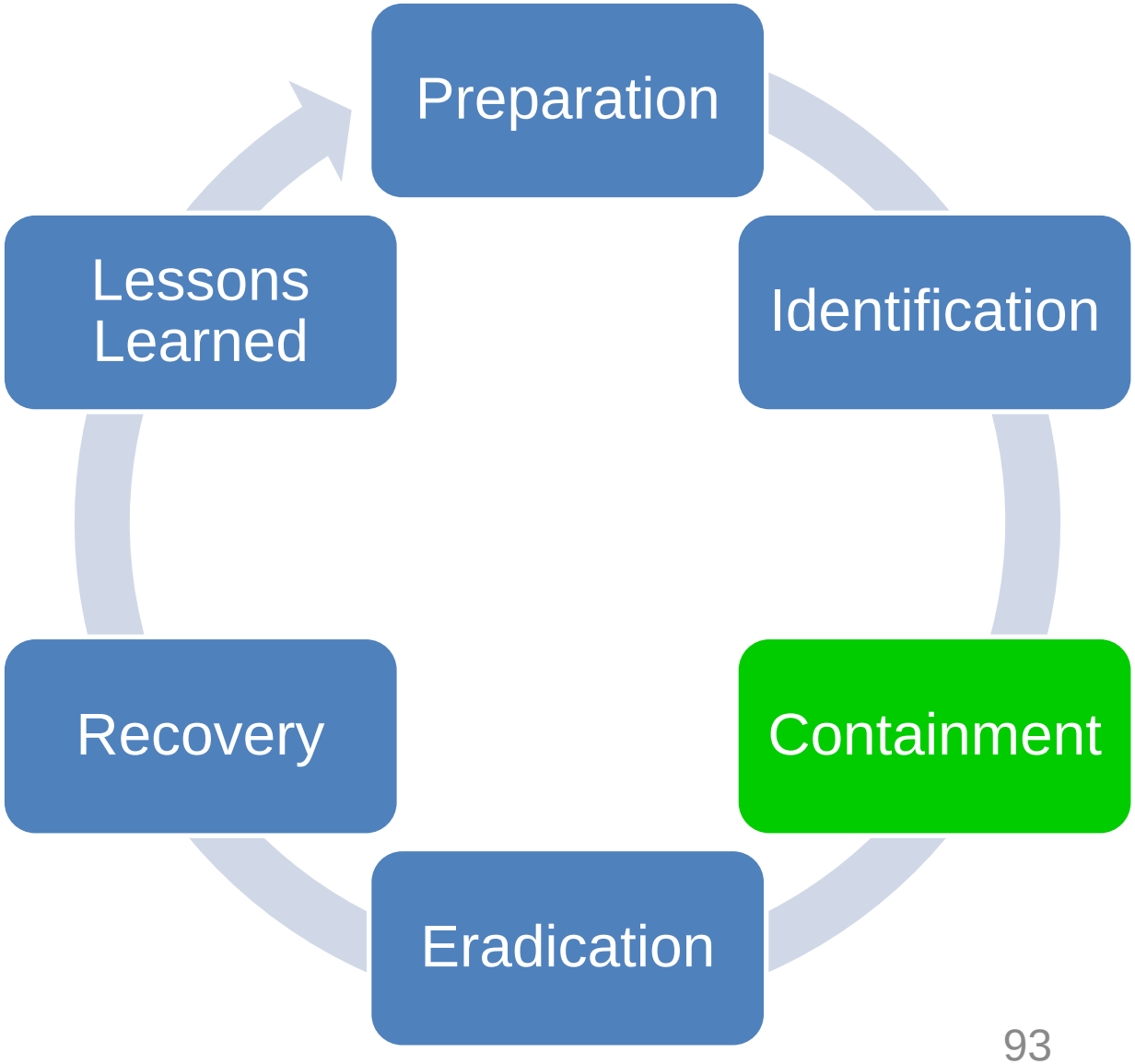
University of Victoria

Communications – Media

- our organization takes privacy and security incidents very seriously
- we (are investigating | have confirmed) the reported incident
- we have (not) determined the extent of the impact
- “there is no evidence that …”
- choice of language (eg. defaced vs hacked or compromised)
- control the use of terms like hack, DDoS, and compromise

University of Victoria

PICERL Process



University of Victoria

Containment

- objective is to prevent further damage
- stop the problem from getting worse
- determine the source, what vulnerability was exploited, and contain it, plug the holes
- continue impact/damage assessment and confirm the scope of the incident
- figure out what was changed (files, connections, processes, accounts, access)

University of Victoria

Containment

- prevent the spread, infection of other systems
- protect the crown jewels
- continue to take notes, ensure a detailed log about what you found and what you did about it
- often the threat has not be fully contained and will “reoccur”
- don’t overcomplicate it – in many cases the simplest answer is the right one

PRESERVE THE EVIDENCE
(KEEP A SAMPLE SYSTEM, MAKE A FORENSIC COPY)

University of Victoria

Containment

- consider the principles, what is the priority?
- is it to restore to operations or hold the attacker responsible
- do you:
  - disconnect the machine? turn it off? turn it on?
- any changes made to the system will alter the contents
  - this is why it can be necessary to take pictures of screen contents and always use write blockers when making copies of hard drives

University of Victoria

Chain of Custody

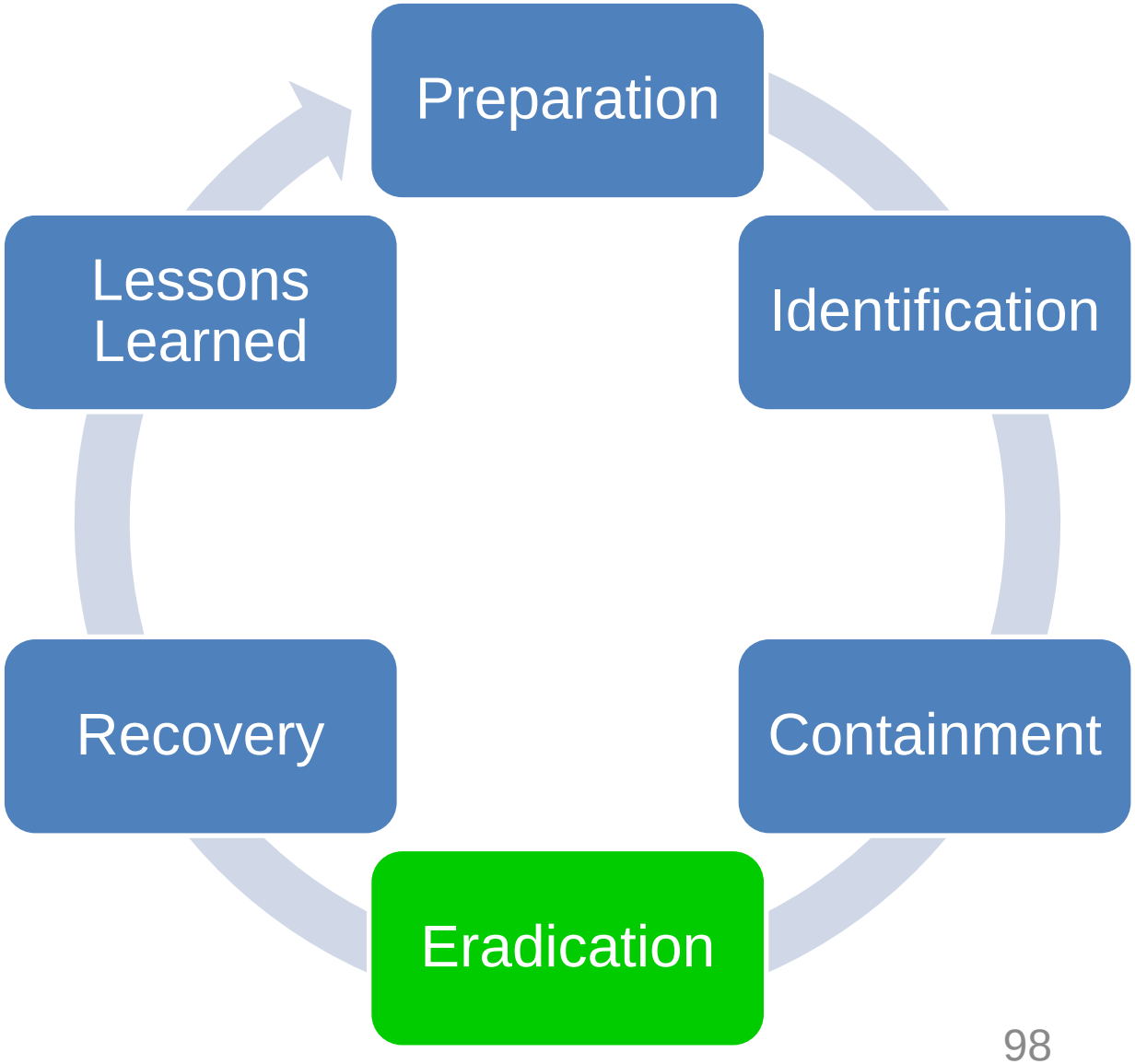
- always handle evidence as if you are going to court
  - ensure integrity
  - can always decide not to later
- maintain evidence log
  - what the evidence is
  - who has/had it
  - when they had it
- have an established process
  - use a template
- store in secure location (evidence locker) when not in possession
- must be able to demonstrate evidence was not tampered with

EVIDENCE / PROPERTY CHAIN OF CUSTODY

REFERENCE NO.	DESCRIPTION		
ITEM NO.	QUANTITY	DESCRIPTION OF ARTICLES (If physical device, include manufacturer, model, and serial number)	
Date/ Time	From	To	PURPOSE OF CHANGE OF CUSTODY
	Name:	Name:	
	Organization:	Organization:	
	Signature:	Signature:	
Date/ Time	From	To	PURPOSE OF CHANGE OF CUSTODY

University of Victoria

PICERL Process



University of Victoria

Eradication

- objective is complete removal of all traces of the infection or other incident
- ensure the holes are closed
- ensure the incident cannot re-occur
- further understand the attack vector
  - review all logs, timestamps
  - scan systems in environment
  - look for symptoms of compromise
- build confidence the incident is contained

University of Victoria

Eradication

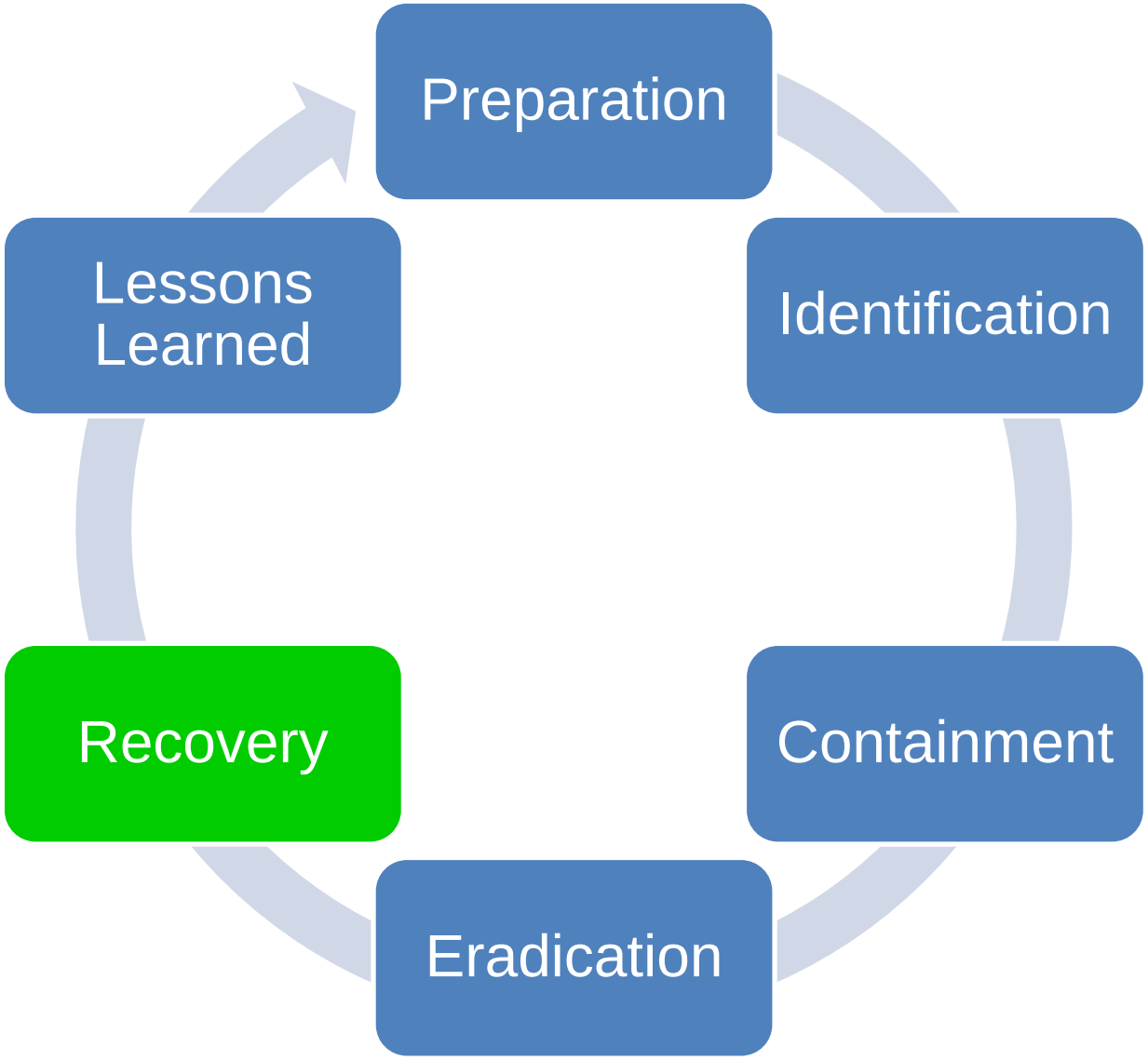
- **compromised machines cannot be trusted**
  - ensure have sufficient evidence
  - format affected systems (may not be enough)
  - anything beyond basic browser hijacking

- would you feel safe performing your personal banking transactions on the machine?

- must permanently remove all traces
  - don’t leave any elements of persistence behind
  - open ports, passwords, accounts, connections
  - require visibility to network, servers, endpoints

University of Victoria

PICERL Process



University of Victoria

Recovery

- objective is to return systems to normal operation
  - systems re-imaged from known good copy
  - ensure systems no longer vulnerable
- test, monitor, and validate as each system is returned to production environment
  - carefully re-introduce each element so as to avoid re-infection or being victimized again
  - after this happens a couple of times you will understand
- business decision when to execute recovery plan
  - determine best time
  - communicate with stakeholders

University of Victoria

Recovery

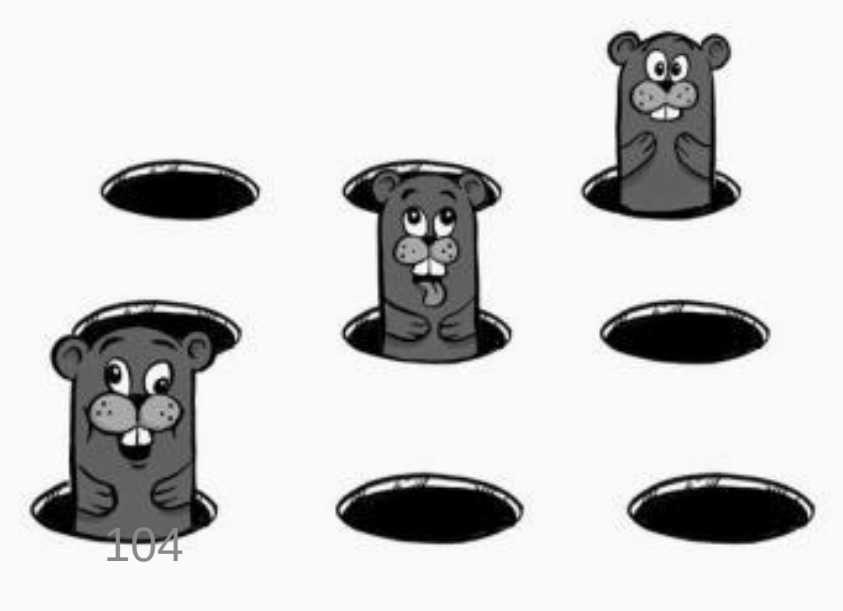
- inform the damage assessment
- determine what all was done
- **determine if it should be restored**
- restore elements at a time
- restoration should be prioritized based on criticality of asset and acceptable downtime
- **monitor closely for suspicious signs, ensure you have visibility**
- realize many attacks are programmed to go dormant when no connectivity or environment changes

University of Victoria

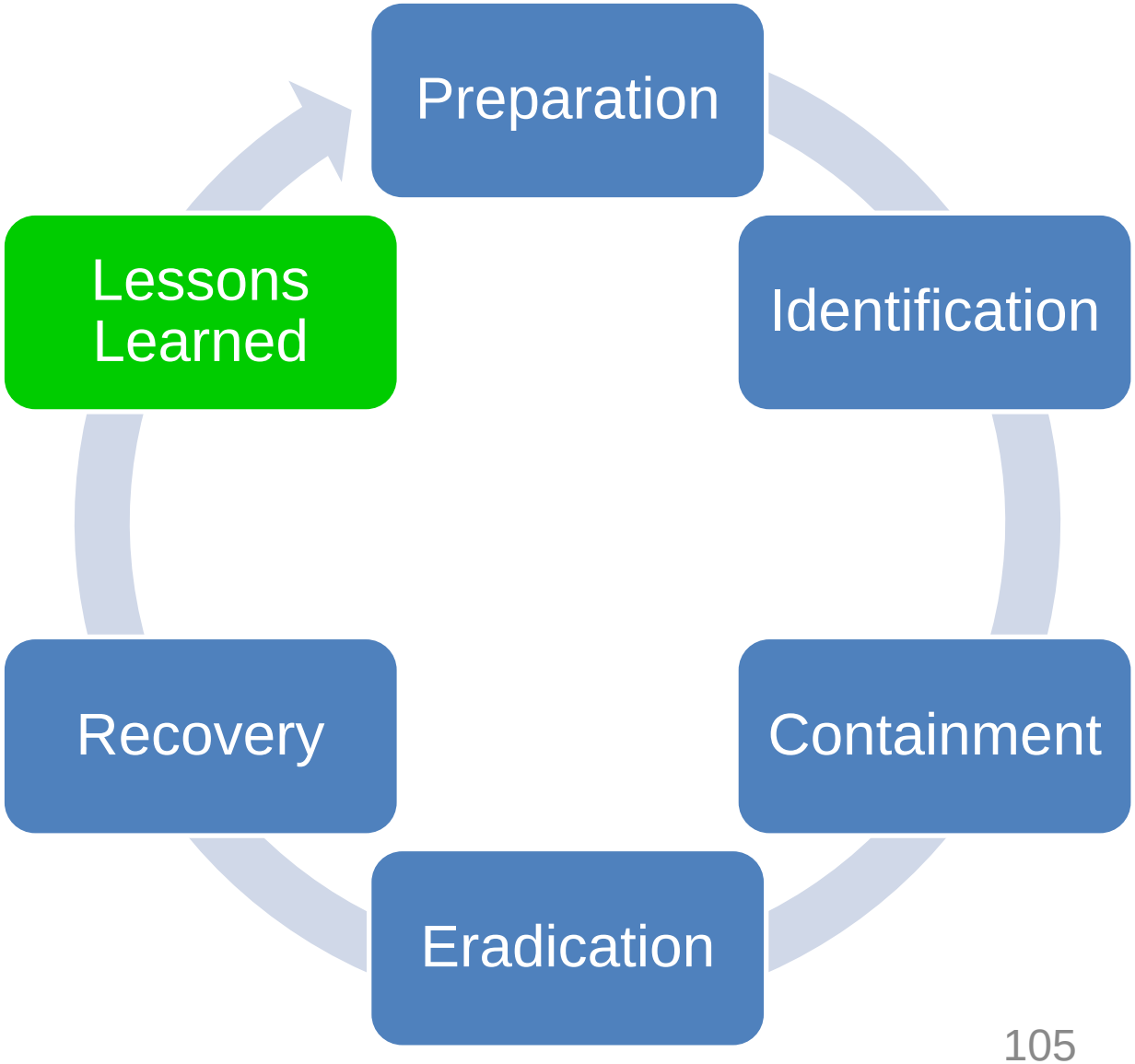
Recovery

- return to production use, systems to normal operation
- restore from TRUSTED source
- ensure no longer vulnerable and no trace of the infection remains
- to confirm functioning normally require a baseline or “known good”

VS



PICERL Process



University of Victoria

Lessons Learned

- walk through and review play-by-play of incident report
  - how was the incident detected, by whom, and when
  - scope and severity of the incident
  - methods used in containment and eradication

University of Victoria

Lessons Learned

- objective to identify opportunities for improvement to better prepare for next time
- essential for continuous improvement
- not a blame game
- what worked, what didn’t work
- what should you start/stop/keep doing
- was any missing information identified or missing roles, additional training required

DO NOT SKIP THIS STEP

University of Victoria

Lessons Learned - Strengths

- identify areas of strength
  - people
  - process
  - tools

- examples
  - availability of team members
  - responsiveness
  - sense of urgency
  - level of collaboration

University of Victoria

Lessons Learned - Opportunities

- identify and document opportunity areas
  - not about blame
  - assign owners and due dates

- examples
  - level of preparation
  - tools to communicate in absence of preferred systems
  - propagation of misinformation
  - single points of failure
  - technology countermeasures
  - security awareness opportunities
  - chain of custody
  - vendor access

University of Victoria

Lessons Learned

- what else do you need to do to bolster your security controls to prevent future incidents
  - eg. anti-DDoS, application whitelisting, education and awareness
- identify requirements of others (eg. vendors)
- capture what you learned that will help you prevent future incidents of this kind
- if you cannot prevent then what will help you respond more effectively and efficiently

University of Victoria

Lessons Learned

- perform the “Lessons Learned” meeting within 2 weeks of the incident to ensure availability of people, details, and experience is fresh
- you paid a price to learn a lesson, capture the **tuition value**
- gather the identified items, prioritize, plan, and execute
- provide necessary reports and ensure accountability for following up on identified items

University of Victoria

Lessons Learned

- ensure you have a common understanding of what happened, why it happened, who did it, and impacts
  - if useful for your business can estimate damages
- ensure you remediated across all platforms
  - eg. if one webserver is vulnerable it's reasonable to check others in your environment
- obtain feedback from all parties
- focus on anything that would have prevented the incident from happening

University of Victoria

Lessons Learned

- do you need to:
  - review and update your incident response plan
  - augment the membership of your incident response team
  - contract with another organization to provide a security assessment or incident response
  - purchase cyber insurance
  - provide staff additional training
  - conduct additional exercises
  - validate list of crown jewels, review security controls, and whether they are sufficient to mitigate risk to an acceptable level

University of Victoria

Lessons Learned

- create executive summary
  - include metrics on frequency/severity of incidents
  - consider including cost of the incident
- highlight recommended actions
- develop a plan, have it approved
- implement approved actions

University of Victoria

Next Steps

- verify the existence of your security incident response plan and that it is up to date
- ensure you have an incident response team whether dedicated, virtual, or on retainer
- support the training and development of team members
- ensure your organization benefits from reasonable security controls
- perform regular exercises, drills whether table top, war games, attack simulations, cybersecurity drills, or actual events
- do not forget to capitalize on lessons learned (after all, you paid to learn them)

University of Victoria

End-to-end

- notified of incident, found, reported
- forwarded to appropriate contact
- initiate security incident response
- bring together those who know and response team
- activate roles and start taking notes
- ensure control flow of information
- identify/validate incident and scope
- look to contain – if can't stop it then slow it down or force them to expose themselves, increase their risk
- do not fall into traps (eg. distractions) or do what they want you to do; resist the urge to do their work for them

University of Victoria

End-to-end

- work until there are no traces, no symptoms
- ensure visibility, monitoring, centralized logging in place
- activate shifts if necessary; obtain the necessary resources
- determine if service should be restored
- make sure to learn from the process

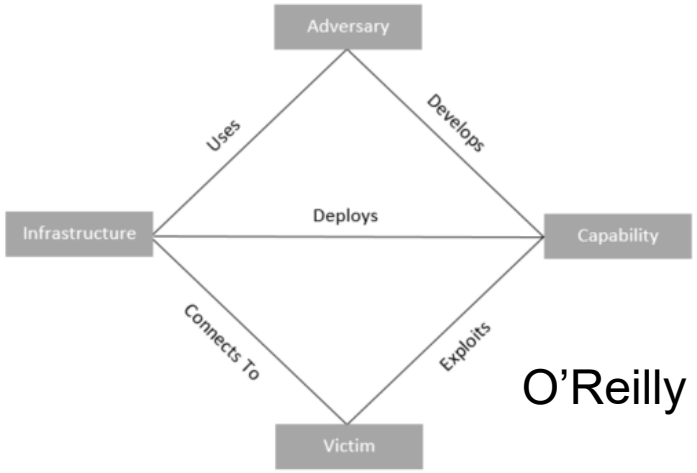
Follow the evidence, don’t jump to conclusions, manage the misinformation, preserve the evidence, and control the misinformation. Step up and lead the incident.

University of Victoria

Certification

- classify intrusion events into categories as defined by security models such as Cyber Kill Chain Model and Diamond Model of Intrusion

https://www.netsurion.com/articles/eventtracker-enterprise-and-the-cyber-kill-chain



O'Reilly

- describe relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

University of Victoria

Assigned Reading

- read Chapters 7-12, 29, 30, 40, 41 for next time
- consider the lab


University
of Victoria

Drills to Follow

University of Victoria