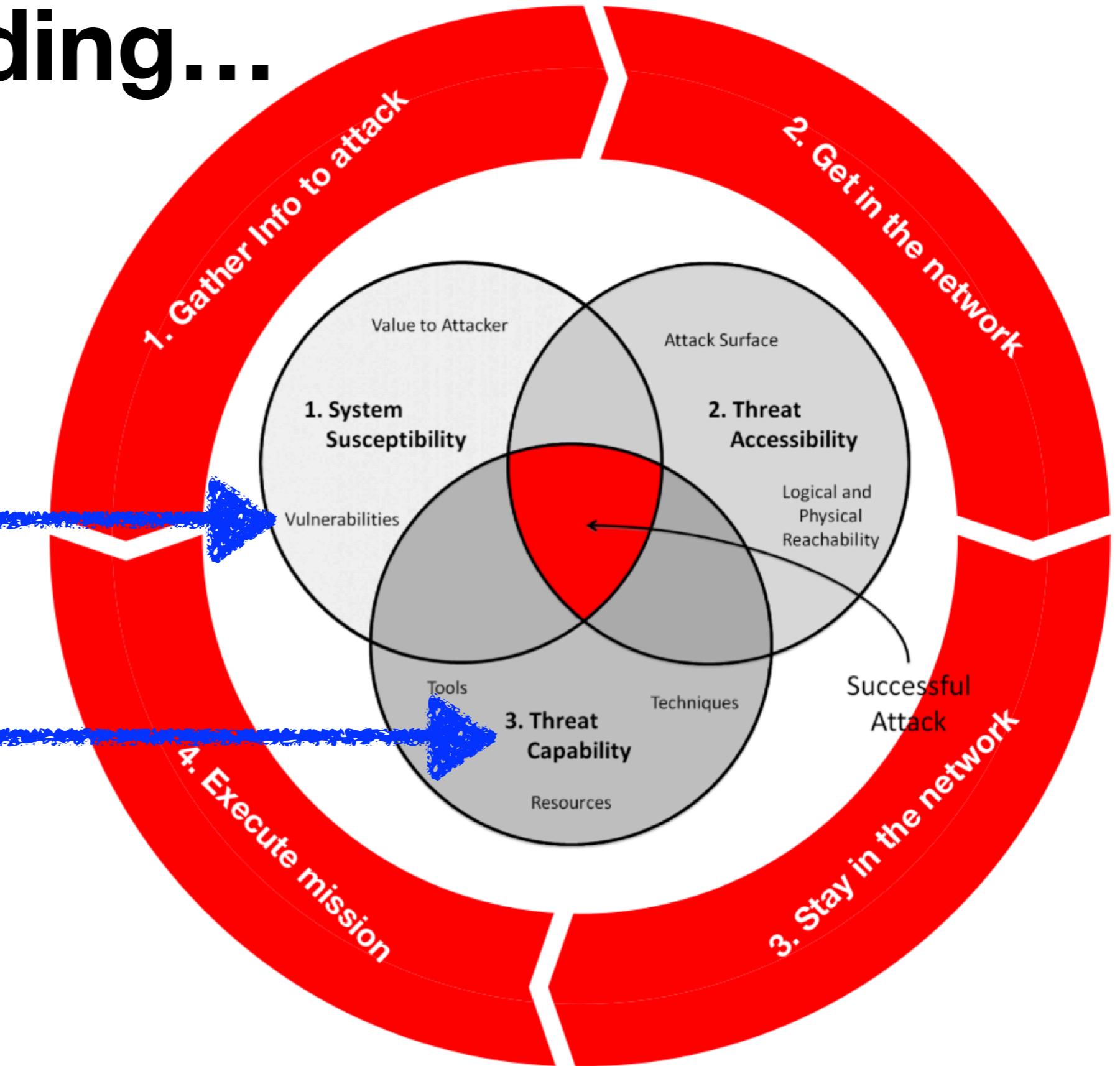


Increasing cost-of-attack through **Isolation**

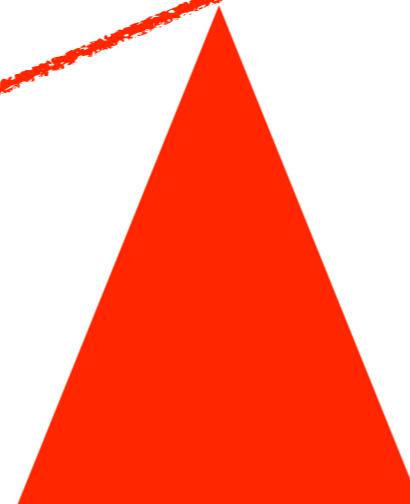
prepared by J.C

Never Ending...



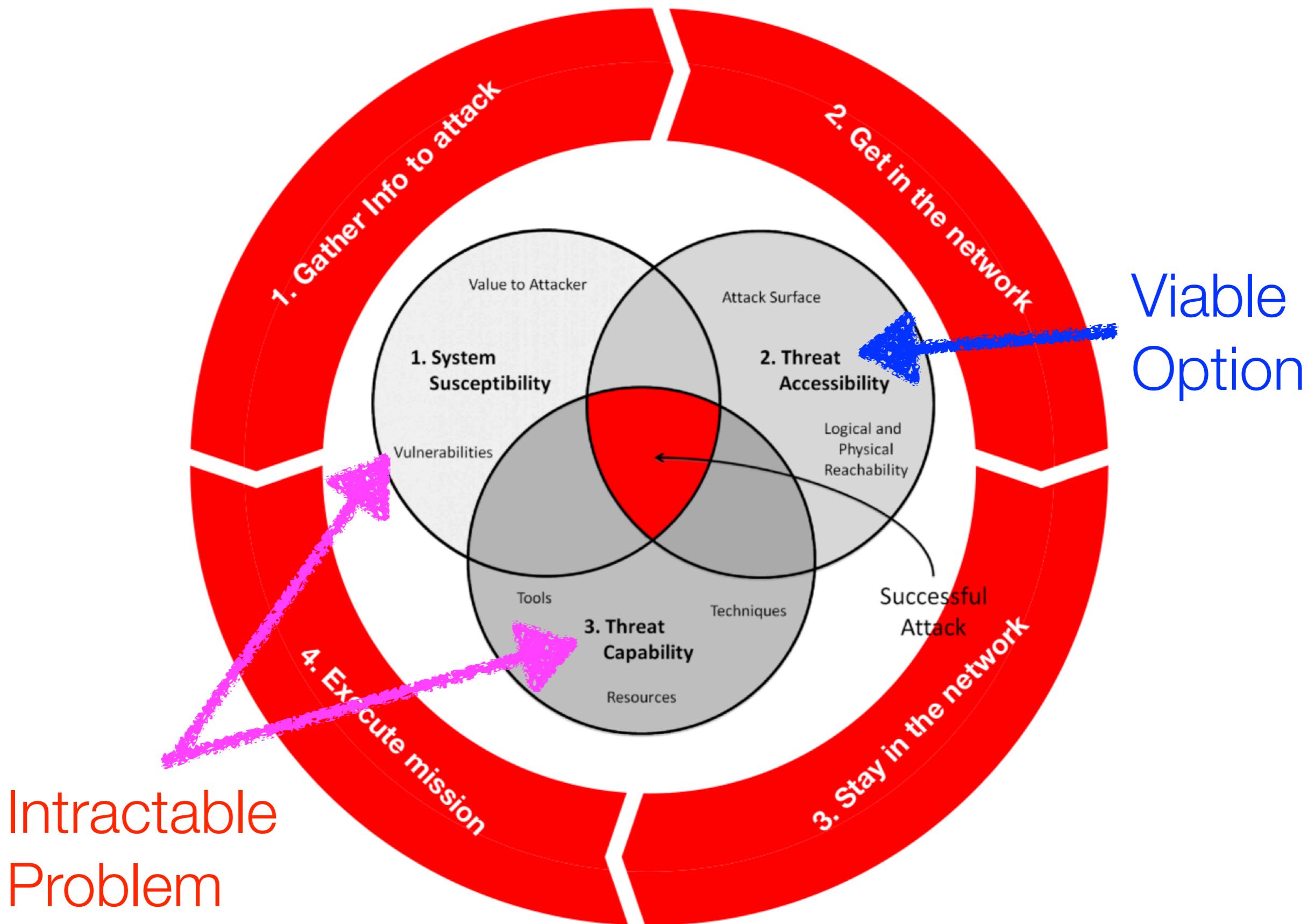
Realities

- Free/leaked offensive tools, source-codes, tutorials...
- Detail research available online freely but unfortunately give malware authors/threat-actors better offensive techniques
- Direct monetary rewards, no need degrees/certs
- Complex & vulnerable systems; no end to patching (vendors' failures/incompetencies becomes our problem)
- Demanding use-cases/SLAs to support
- Low/no budget for security
- Shortage of skilled/certified technical staffing



#WannaCry 

**ALL successful attacks require all 3 conditions to exists;
susceptibility, accessibility & capability**

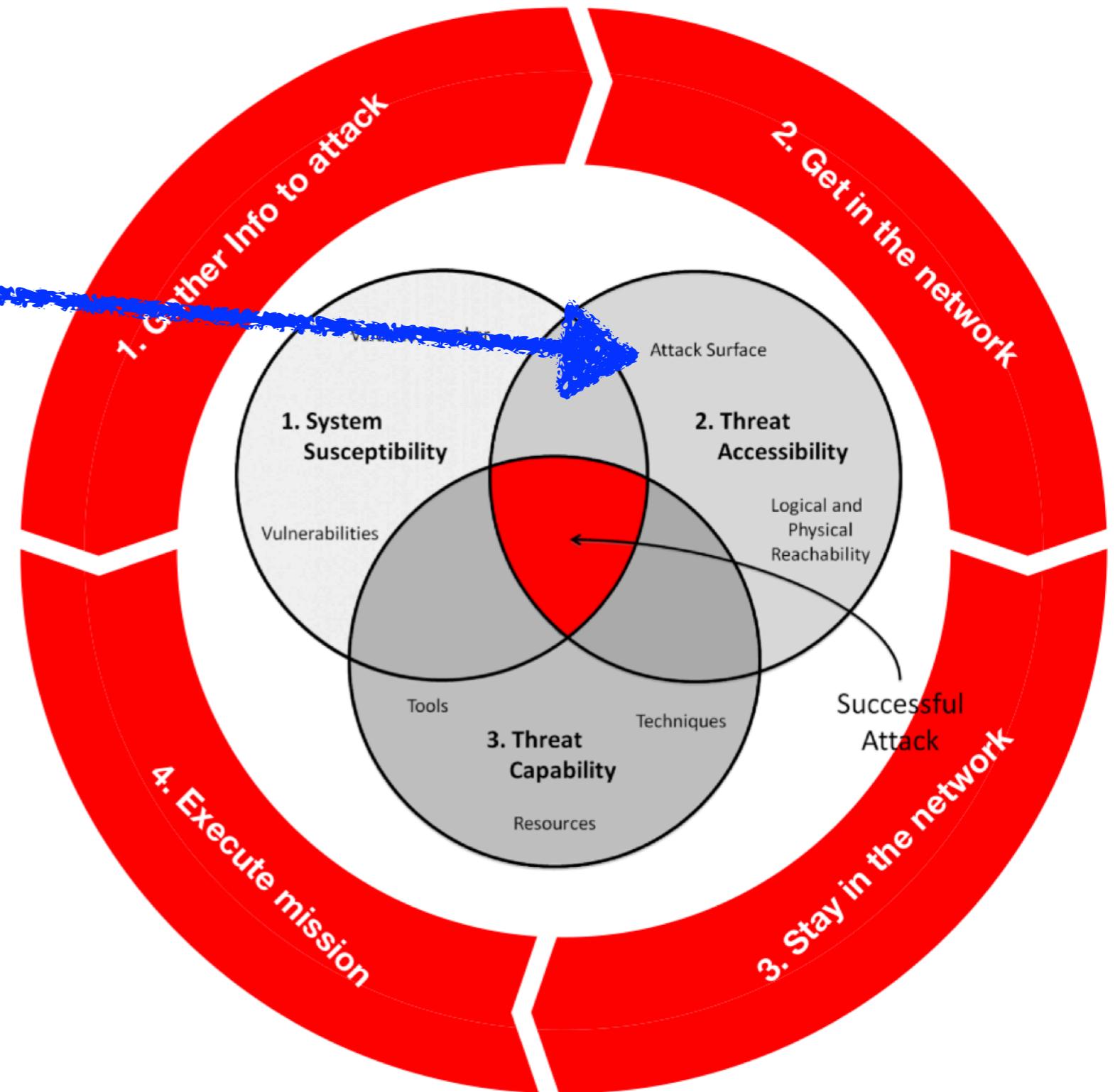


“Enumerating bad things is a bad idea...”

“Knowing what not to do doesn’t mean
we know what to do...”

Top ways to get to victims

- 1. Email**
- 2. Browser**
3. Others (eg. installing tainted apps, removable media, Man-in-the-Middle/Browser/Device...)



Isolation deals with “Stage 2” of externally controlled attack...

	Tactics	Users	Services	Networks
External Actors	<i>Stage 1 Gather Info</i>	External Reconnaissance	Social Engineering Awareness	Deceptive Traps
External & Internal Actors	<i>Stage 2 Get in</i>	Deliver payload Run payload Install payload External control	Moving Target & Layered Endpoint Defense	Isolation
External & Internal Actors	<i>Stage 3 Stay in</i>	Internal reconn. Gain privilege-access Abuse credentials Internal control	Deceptive Traps Least Privilege Principle Multi-Factor Authentication Privilege User Management & Monitoring	
External & Internal Actors	<i>Stage 4 Execute mission</i>	Steal (Confidentiality) Tamper (Integrity) Deny (Availability) Damage (Safety)	Application Security, Data Protection & Key Management Redundancy & Recovery	Outbound Controls Isolation

What can Isolation do?

- Disrupts delivery of payload (Threat Accessibility)
- Even if somehow payload runs within isolated networks, it is harder to contact typical remote **Command-&-Control** servers
- Not limited to APT, blocks ransomware too

	Tactics	Users	Services	Networks
Stage 1 Gather Info	External Reconnaissance	Social Engineering Awareness		Deceptive Traps
Stage 2 Get in	Deliver payload	Moving Target & Layered Endpoint Defense	Isolation	
	Run payload			
	Install payload			
	External control			
Stage 3 Stay in	Internal reconn.		Deceptive Traps	
	Gain privilege-access	Least Privilege Principle Multi-Factor Authentication	Privilege User Management & Monitoring	
	Abuse credentials			
	Internal control			
Stage 4 Execute mission	Steal (Confidentiality)	Application Security, Data Protection & Key Management	Outbound Controls	
	Tamper (Integrity)			
	Deny (Availability)	Redundancy & Recovery	Isolation	
	Damage (Safety)			

COTS “Isolation” Solutions

Host Isolation



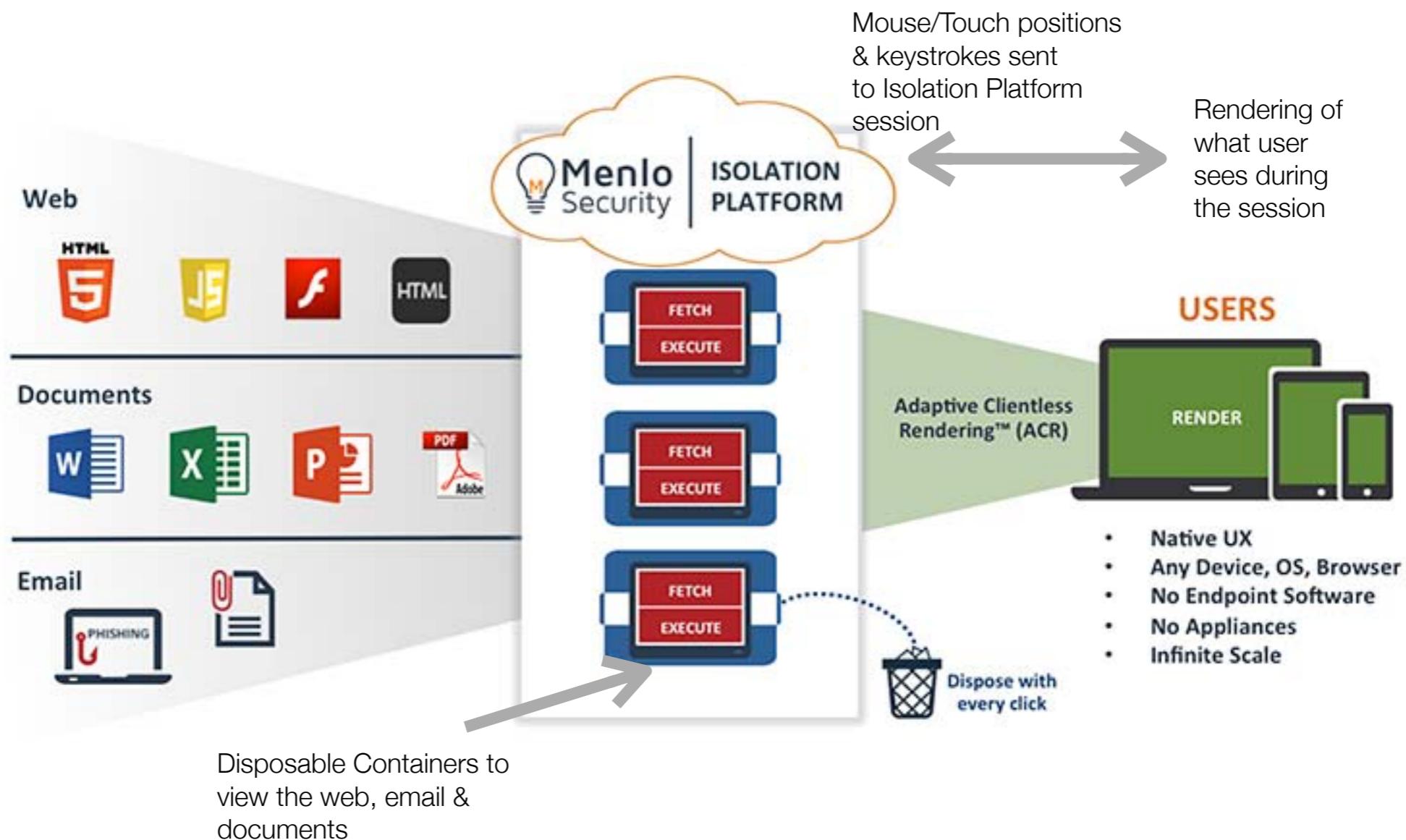
Network Isolation



- Just to list a few examples; I don't do (pre)sales...
- Network layer easier to deploy; zero-client setup

Working Principles of “Isolation Platforms”

Malicious payloads are contained within these disposable Containers*.
Users' devices are unaffected.



Isolation solves ‘Threat Accessibility’ but how to get & use external contents?

- Typical use-cases: copy-&-paste, screen-capture, print out physical copy, save to disk **as files**, **view email/URL/document**... the last two are typically how bad guys get in & take-control remotely.
- Traditional/physical air-gaps will need multiple keyboards, mice or KVM switches + wiring; **A hassle in terms of getting content across disjoint networks & peripherals support!**
- **External contents need to get into isolated machines.**
How to ensure that these contents are safe for consumption?

Let's say we have **low budget** for ~~IT security~~

- Two separate **Virtual Desktop Infrastructure**; one for internet surfing, the other for intranet clients.
- VDI is nothing new, can reduce cost in terms of \$\$\$, electricity bill\$, IT-operations efforts.
- Low power ARM processor thin-clients are cheap, ~US\$60, MoQ = 1
- Many thin clients have dual display ports & some with dual ethernet ports. Let's see how to support a 'seamless' experience

VDI Server(s) for Internet Zone

Safe ingestion of
external contents

VDI Server(s) for Intranet Zone

Mouse positions &
keystrokes

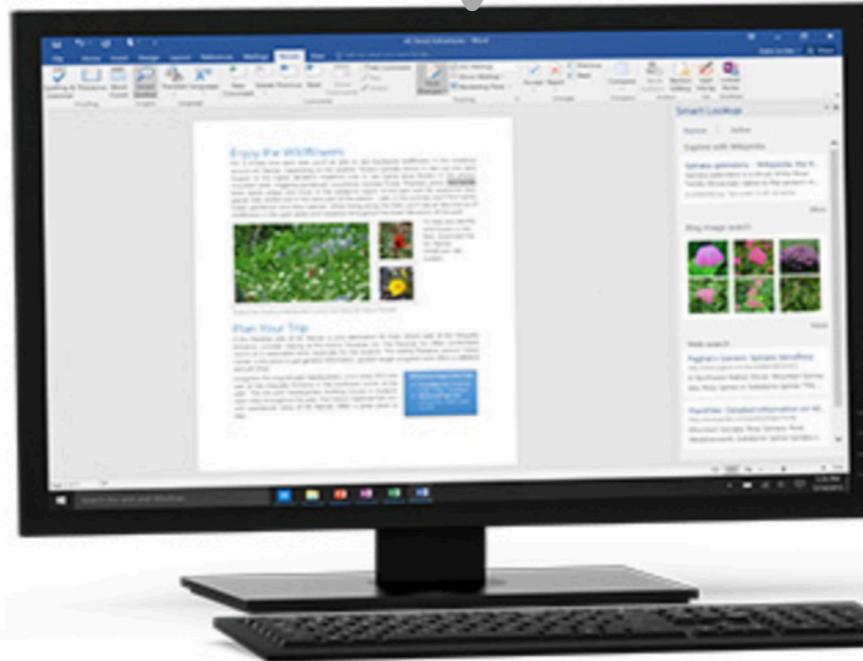
RDP session to
disposal VM running
browser & document
viewers

Image rendering



Low-cost
thin client with
little/zero storage

RDP session to VM
for intranet
applications



- No KVM switches/cables to deal with!
'Seamless' since 1-set of keyboard + mouse, if needed, audio redirection for internet tele-conferencing
- Users can copy-&-paste text, screen-capture images, view/save files... automated content transfer to intranet client-zone
- Can be adapted for laptop + monitor. When used out-of-premise, use Isolation Platforms like Menlo-Security or Fire.Glass as forward-proxy

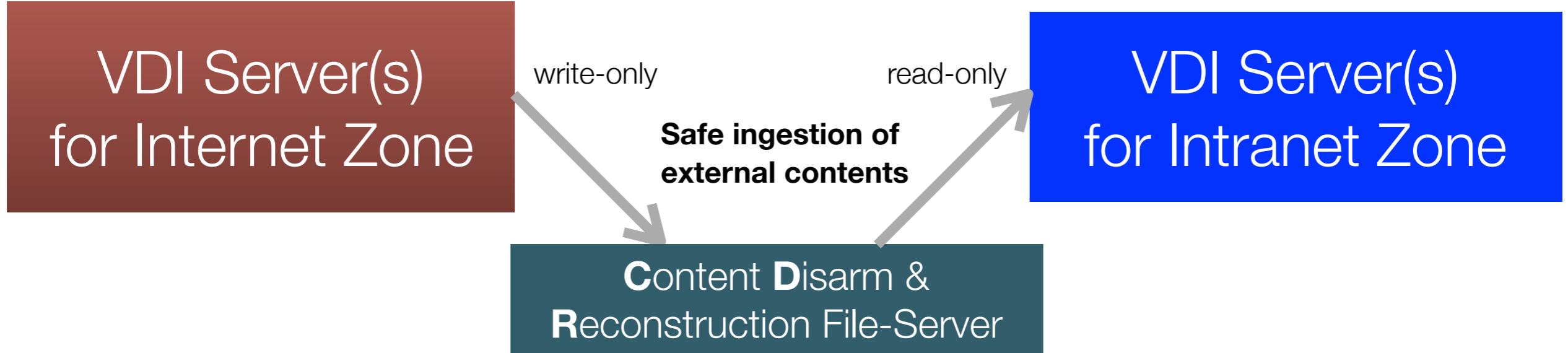
VDI Server(s)
for Internet Zone

**Safe ingestion of
external contents**

VDI Server(s)
for Intranet Zone

What is this ‘Disposal’ Internet VM?

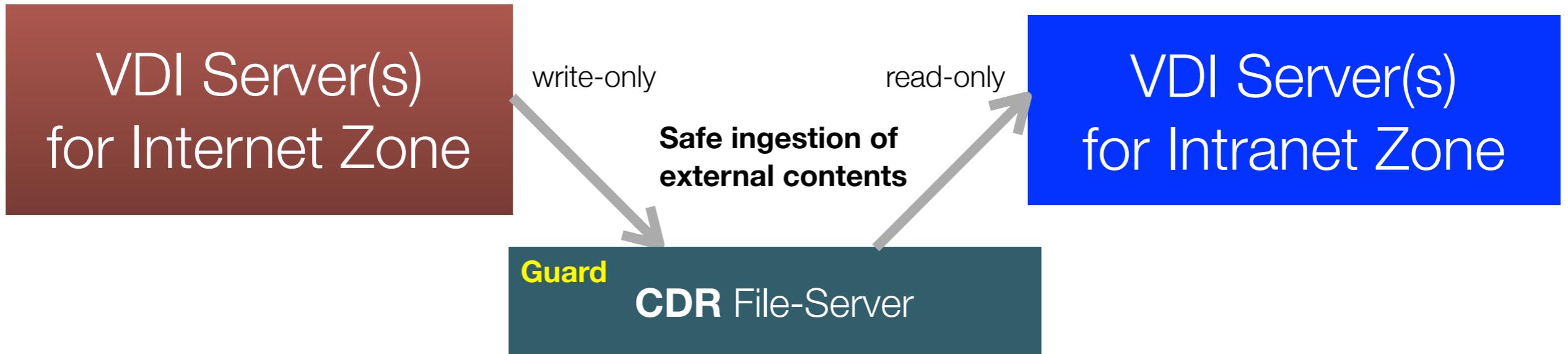
- Essentially a hardened Windows/Linux VM running in Internet-kiosk mode, allocated with minimal computing-resources for use browser for both surfing & viewing of documents
- Use built-in application-whitelisting Software Restriction Policies/AppLocker for Windows-based VMs.
- Install free malware analysis/debugging tools to fool malware & threat-actors. Honey-tokens as trip-wires eg fake credentials in sysprep files. #Deception
- Use freeware like [ToolWiz Time Freeze](#). Revert VMs to original state after reboot. Deters any backdoor/persistence after successful code-execution. Have another master-copy VM template, turn on Time-Freeze to deploy after patching. Linux can do “Live/read-only mode”.
- A simple clip-board-to-file tool that writes to a network folder. File saving writes to the same dedicated folder for ‘Safe Ingestion’.



What is ‘Safe Ingestion’?

- Let's say attackers took over a VM within internet zone... Assume he didn't fall for honey-tokens/traps/fake-debugging...
- Between the 2 zones, there's a file-server that **only expose write-only folders** to Internet Zone & **read-only folders to Intranet**. All other ports/services blocked on the file-servers.
- File-server performs CDR using file-format conversion* to “flatten” malicious active-contents. Rejects ALL executable files.

* if budget permits, go for static-content-analysis products that block any shell-codes/malicious-scripts within **data contents, especially for contents that cannot be converted**. Don't waste money on sandboxes or anti-virus.



Past Present Future



Let's look at the theory behind this approach...

Three-Tenets Threat Model

<http://www.dartmouth.edu/~gvc/ThreeTenetsSPIE.pdf>

Conceptual Ingredients	Attacker → Target		
Attack Requirements	Capability	Accessibility	Susceptibility
Defender's 3 Tenets	Detect, React, Adapt Deceive*	Move Key Assets “Out-of-band”	Focus on What's Critical
Routine Activity Theory (RAT) of Crime	Motivated Offender	Lack of Guardianship	Suitable Target
Criminal Law	Means	Opportunity	Motive

* Not part of the original paper

Defenders' Three-Tenets

- Tenet 1 *Focus on What's Critical* - The first *Tenet* instructs the designer to consciously and methodically focus on including only those system functions that are essential to the mission. This is an acknowledgement of Occam's Razor by the system designer. Adherence to this *Tenet* reduces the number of potential susceptibilities, and therefore, the paths between the attackers' starting state (the system access points) and goal states in which mission essential functions, critical security controls, or critical data are compromised. This *Tenet* eliminates those access points and susceptibilities associated with unneeded functionality.
- Tenet 2 *Move Key Assets Out-of-Band* - The second *Tenet* instructs the designer to consciously differentiate between user access and attacker access for a given system's mission. This *Tenet* modifies system availability and is accomplished by moving the data/processes used by mission essential functions, their security controls, and associated access points out-of-band of the attacker either logically, physically, or both. By "out-of-band" we mean not accessible by the attacker through their preferred or available access methods. Adherence to this *Tenet* reduces threat access for a given mission (use case) and may enable unalterable observations of system state by a security control sensor. The extent and strength of access differentiation between the user and attacker is greatly influenced by the type of out-of-band mechanism employed and whether its done in software or hardware.
- Tenet 3 *Detect, React, Adapt* - The third *Tenet* instructs the designer to employ dynamic sensing and response technologies (i.e a security control sensor or reference monitor) that mitigate the threat's capabilities and exploitation attempts through automated (preferably autonomic) system behavior. Adherence to this *Tenet* confounds the attacker's capabilities by making the system's defenses unpredictable (nonstationary) and adaptive (with penalties) instead of merely being passive.

Proposed Approach mapped to 3-Tenets

	Thin-Clients	Internet Zone	Safe Ingestion of Contents	Intranet Zone
Tenet 1 Focus on What's Critical	Can only RDP or equivalent protocol. Block file-transfer & USB device forwarding.	Limited use-cases to viewing & saving external contents to sanitisation folders.	Limit to sanitisation of contents & logical 1-way content flow. Use data-diode if budget permits.	Run only necessary intranet apps. Limit outbound content transfer, use monitored channels for outbound file transfers.
Tenet 2 Move key assets Out-of-Band	No sensitive/internally generated contents, all done within intranet.	No sensitive/internally generated contents, all done within intranet.	All external contents are stored temporarily for sanitisation. It is mounted as read-only for intranet clients.	Locked thin-clients mitigate Insider USB exfiltration & internal content hidden in outbound TLS/SSL
Tenet 3 Detect, React, Adapt	Any attempt to run anything other than whitelisted app(s) will trigger disablement of thin-client	Use deception to deter threat actors. Use honey-token as sensor to reboot VM to clean state.	Monitor this path closely for anomaly <u>instead of so many possible paths</u> . Shut it off when necessary.	Without noisy internet traffic means better detection with higher signal-to-noise ratio.

What about Small-Medium-Businesses?

- This approach was conceived under a scenario of low/no budget for security products. We rearrange assets & configure them in accordance of 3-Tenets guidance.
- Look up Alibaba for “thin-client”, you will find the diagrams & sizing for VM-hosting servers for digital signages, Internet kiosks/classrooms...
- Content sanitisation file-server that enforces a “logical” one-way transfer is intended as a ‘poor-man’s data-diode.
- If it is too difficult to implement, then pay for Menlo-Security, Fire.Glass or similar cloud-based “isolation-proxy” subscriptions. **But still need to deal with safe content consumption.**
- All these catch-the-bad-signatures solutions are mostly waste of time (false-positives) & \$\$\$ because it is easy to generate evasive RAT payloads & abuse system component to execute such malicious codes... with a freeware like Time-Freeze just reboot to get disposable VM to fresh state.

Let's say there's **more budget** for IT security

- Use **application-protocol aware** firewalls to limit only RDP network traffic between thin-clients & zones. Guard against abusing thin-clients as pivot points. (Tenet 1 & 2)
- Likewise, **limit network to only file-share write-only** traffic from Internet-VDI-zone to file-server & **read-only** from file-server Intranet. (Tenet 1 & 2)
- Deploy **anti-exploitation** agents (eg. Morphisec or PANW TRAPS) &/or **host-isolation** like Bromium or BufferZone to guard file-server. (Tenet 3 & 2)

Thanks for reading this far... Next round will focus
on deception & detection!