SANS | GIAC CERTIFICATIONS

Defenders:
What to do NOW if Expecting Nation-State Attackers

Mick Douglas & Jon Gorenflo

20220302

Agenda

1. Resource:
   Six Defensive Techniques to Make Your Attackers Cry
2. Global Events/You are a target
3. Using the “Six Defensive Techniques” workflow
4. You can win as a defender

SANS | GIAC CERTIFICATIONS

"Just give me the checklist"

This document, this deck, links to this recording are all here.
https://www.sans.org/blog/ukraine-russia-conflict-cyber-resource-center/

Additional resources will be posted here as they become available.

SANS | GIAC CERTIFICATIONS

Live interaction:
Please ask questions...
We will answer what we can.

SANS | GIAC CERTIFICATIONS

Global Events

SANS | GIAC CERTIFICATIONS

Current State

Highly fluid

In region, major issues

Outside region...
Status quo... so far.

- **Expect attacks, you are a target.**
- **For most Orgs, you will not be targeted by Russian Cyber Operators.**
- **Social engineering attacks on dramatic rise.**

Some REALLY bad takes are out there…

"Just another day on the internet."

Do not treat this as any other day.

- Do you want to be doing this fire drill again?
  - → Why not move to a more sustainable model?
  - → Leverage the attention to enact meaningful change.
  - → Make a shift to sustainable security

SANS | GIAC CERTIFICATIONS

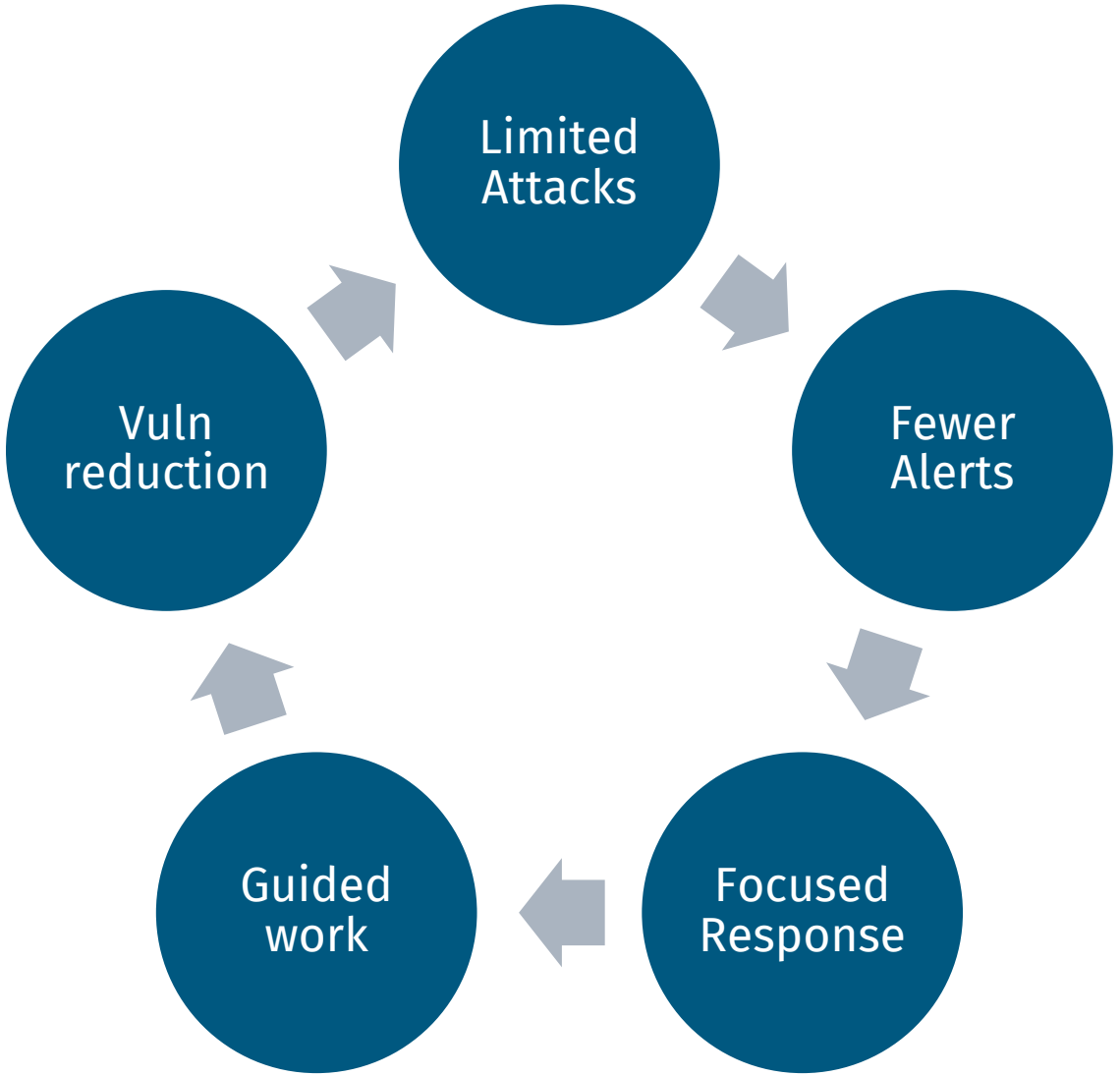
Using the Six Defensive Techniques workflow

SANS | GIAC CERTIFICATIONS

You can win as a defender.

The Cycle of IT/Security Failure

Create a Positive Feeback loop



Defensive Technique #1

PATCHING

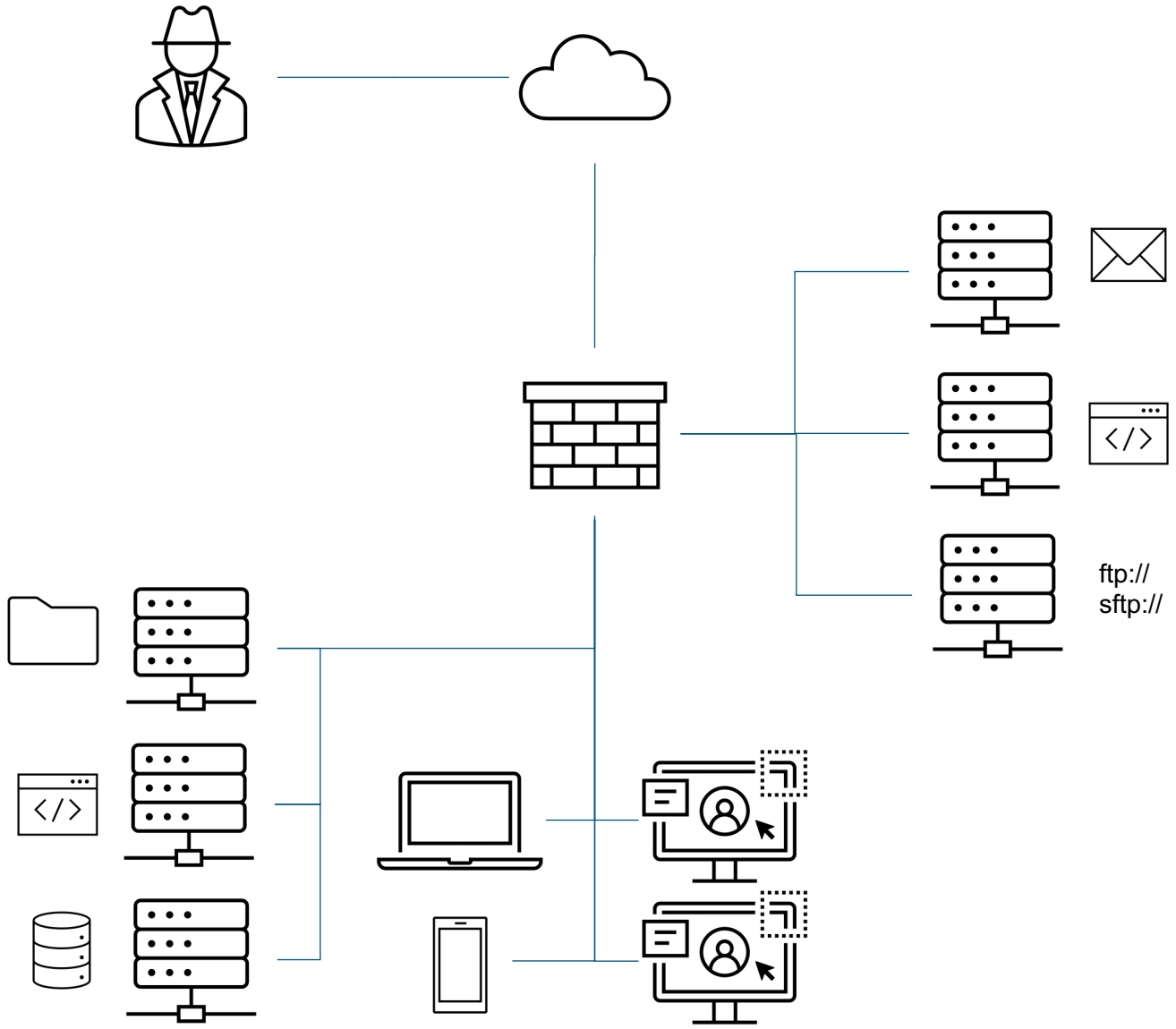
Patches work.

99.7% of CISA's Known Exploited Vulnerabilities Catalog can be patched

How to Do It

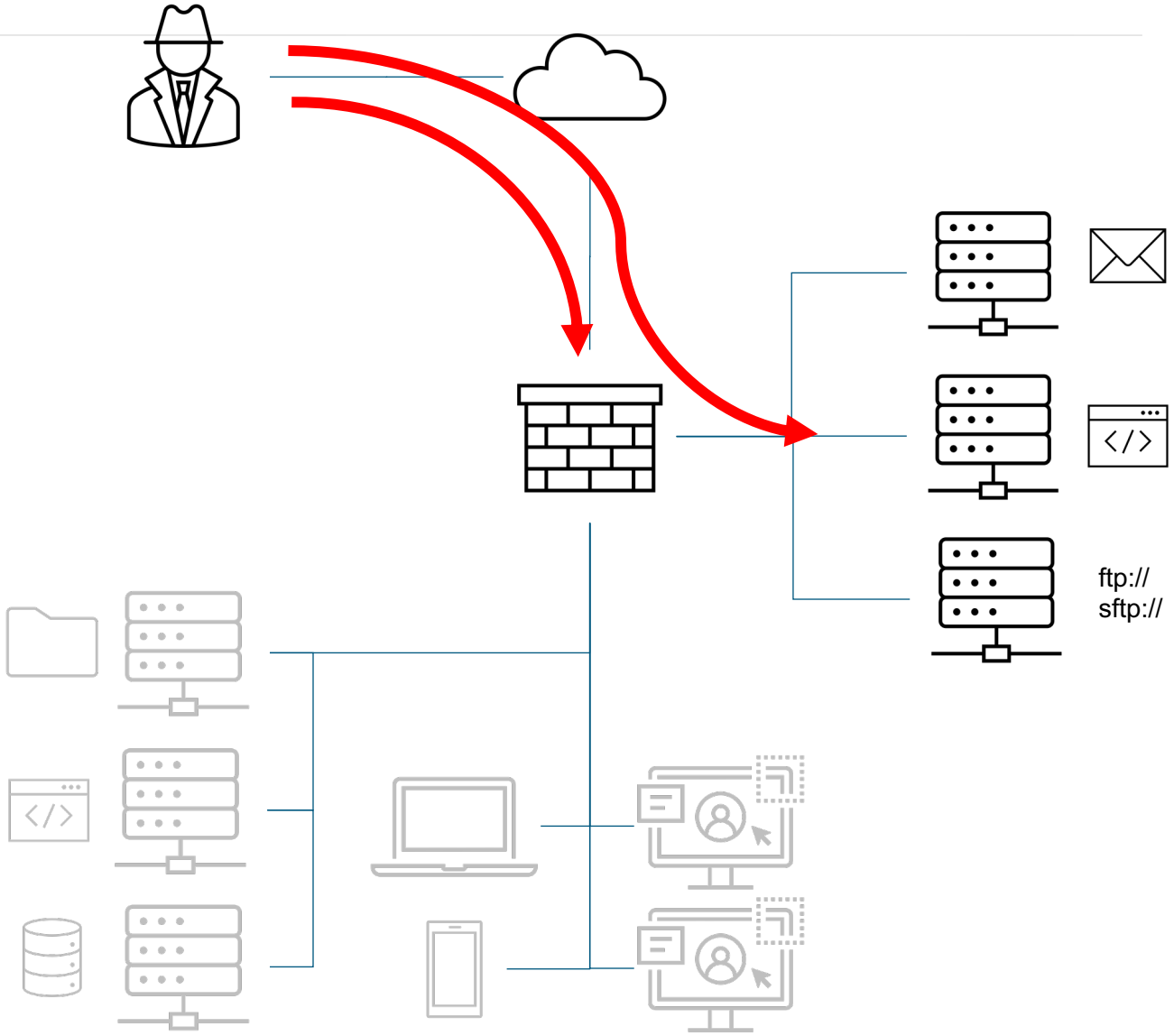
- Prioritize by common attack paths
- Configure Automatic Updates
- Manually patch where necessary
- Scan for CISA Known Exploited Vulnerabilities
- Repeat

A Common Network



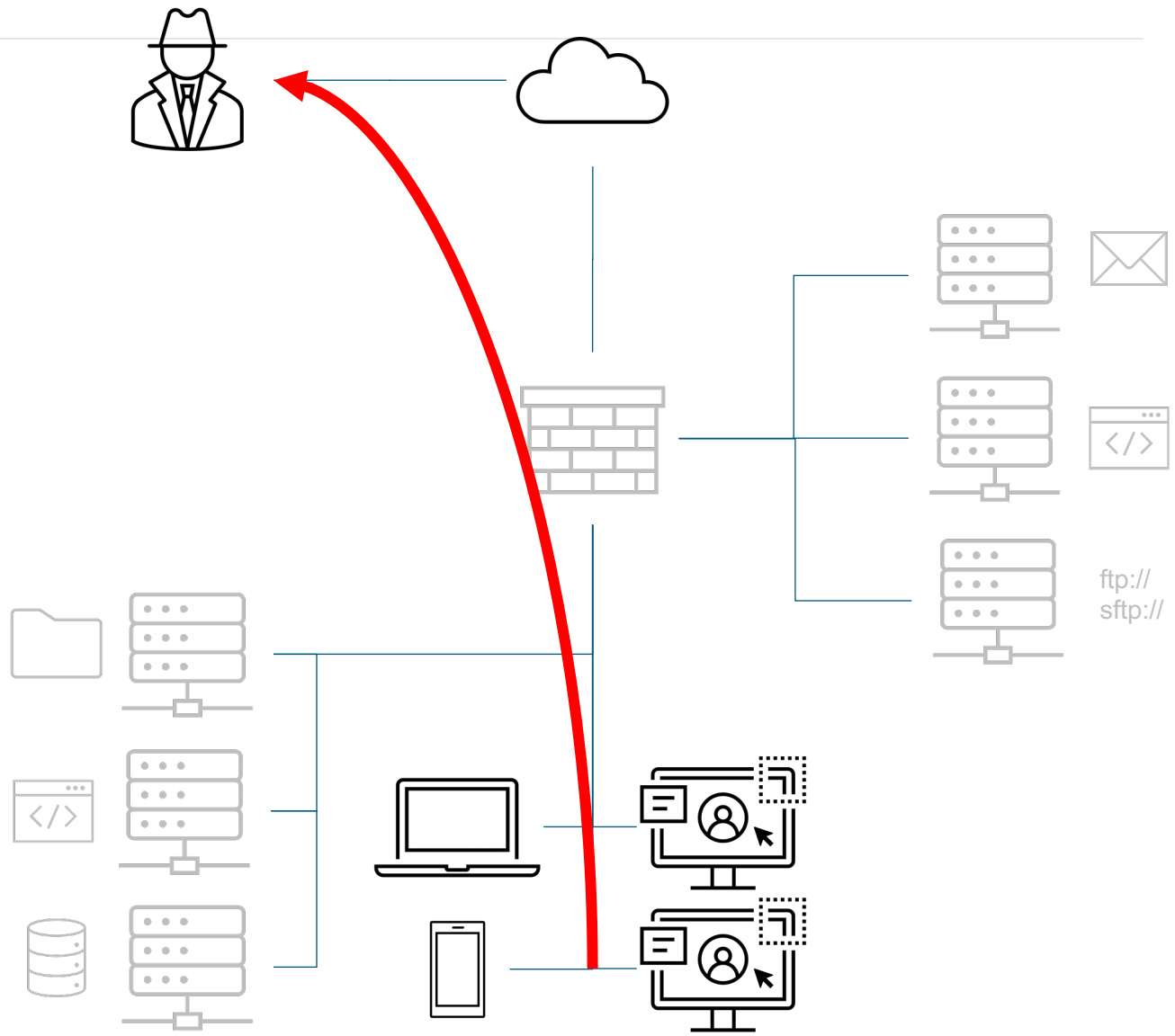
Prioritize by Common Attack Paths (1)

- **Internet Accessible Systems First**
  - 1. Network & Security Appliances
  - 2. Web Servers
  - 3. Web Apps
  - 4. Host OS
- **Reasoning**
  - Attackers can directly access these systems – No dependencies
  - Some lack normal detective controls. (ie. Your firewall does not have EDR)
  - Many will be “critical” to business ops, and have “risk accepted” vulns.



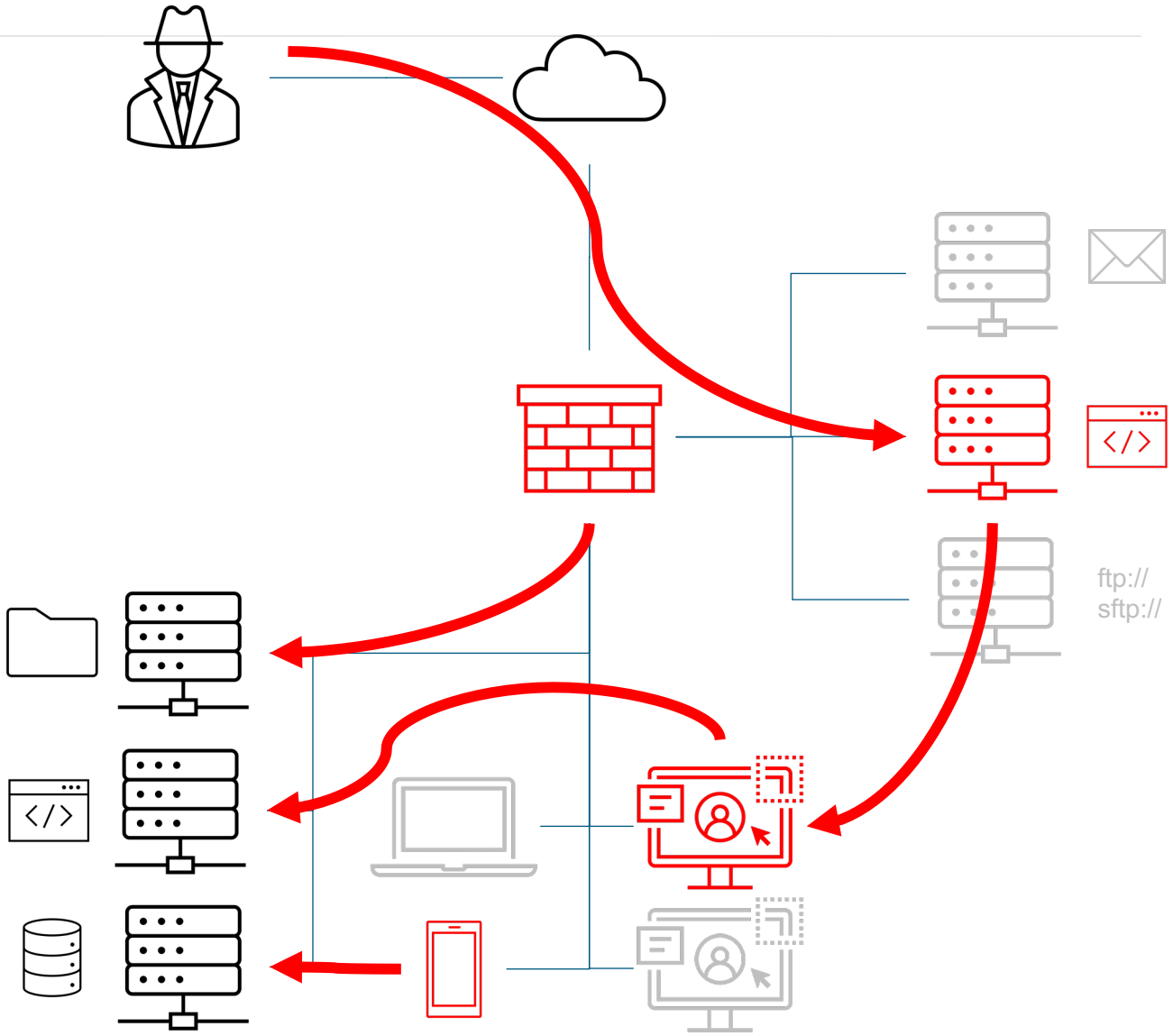
Prioritize by Common Attack Paths (2)

- **Clients & Client Software**
  - 1. MS Office, Adobe PDF Products
  - 2. Browsers
  - 3. Mobile Apps
  - 4. Host OS and Mobile Devices
- **Reasoning**
  - Users' systems have broad access to the internet
  - Client software *is designed* to download executable code from arbitrary places on the internet…and *run it*.
  - Users don't have to do *anything* wrong to be compromised



Prioritize by Common Attack Paths (3)

- **Internal Servers & Software**
  - 1. Database Servers
  - 2. Applications
  - 3. File Servers
  - 4. IoT Devices
- **Reasoning**
  - Internal severs are usually the *goal* – it's where the data is stored
  - Attackers gain access through Internet facing systems or clients, then pivot to internal systems
  - Often the last "stop" for the attacker



Defensive Technique #2

Logging Strategies

Strategies

Tell stories with your logs

More log sources

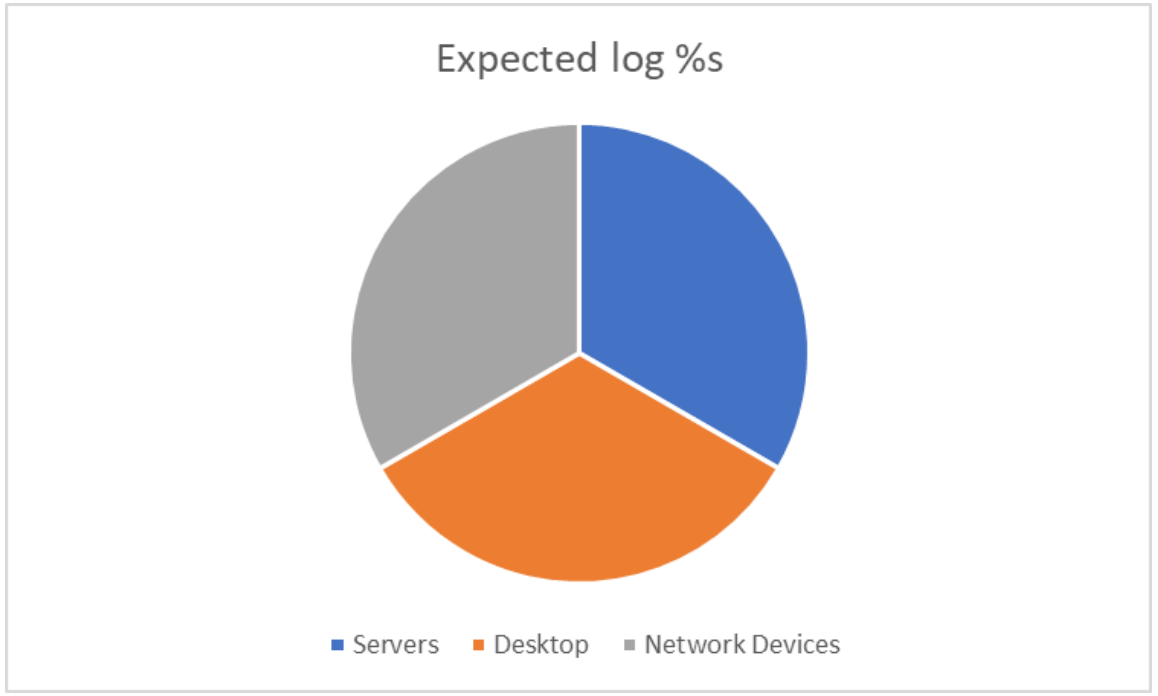
Where possible decrease retention

Tactics

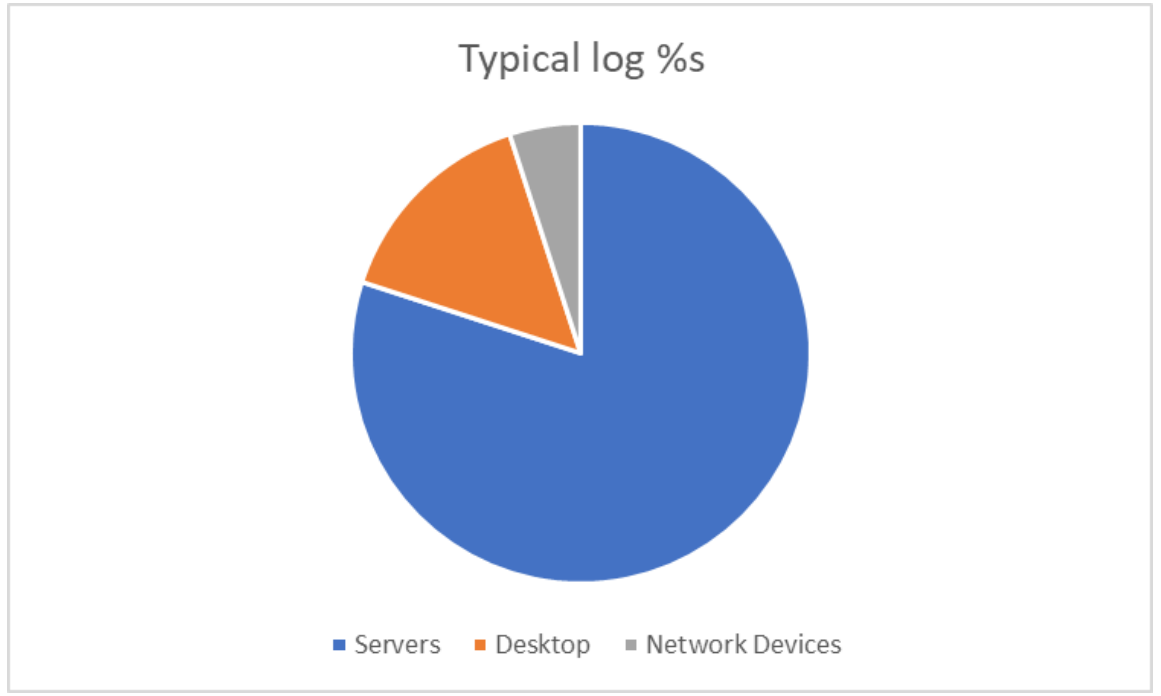
- Desktops generate fewer logs than servers.
- All log sources can be filtered.
- Remove fields from logs if they don't help.

Expectation vs. Reality (sending logs)

Source	% of volume
Servers	33%
Desktops	33%
Network devices	33%



Source	% of volume
Servers	80%
Desktops	15%
Network devices	5%



Defensive Technique #3

Outbound Traffic

Control & Monitor Outbound Traffic

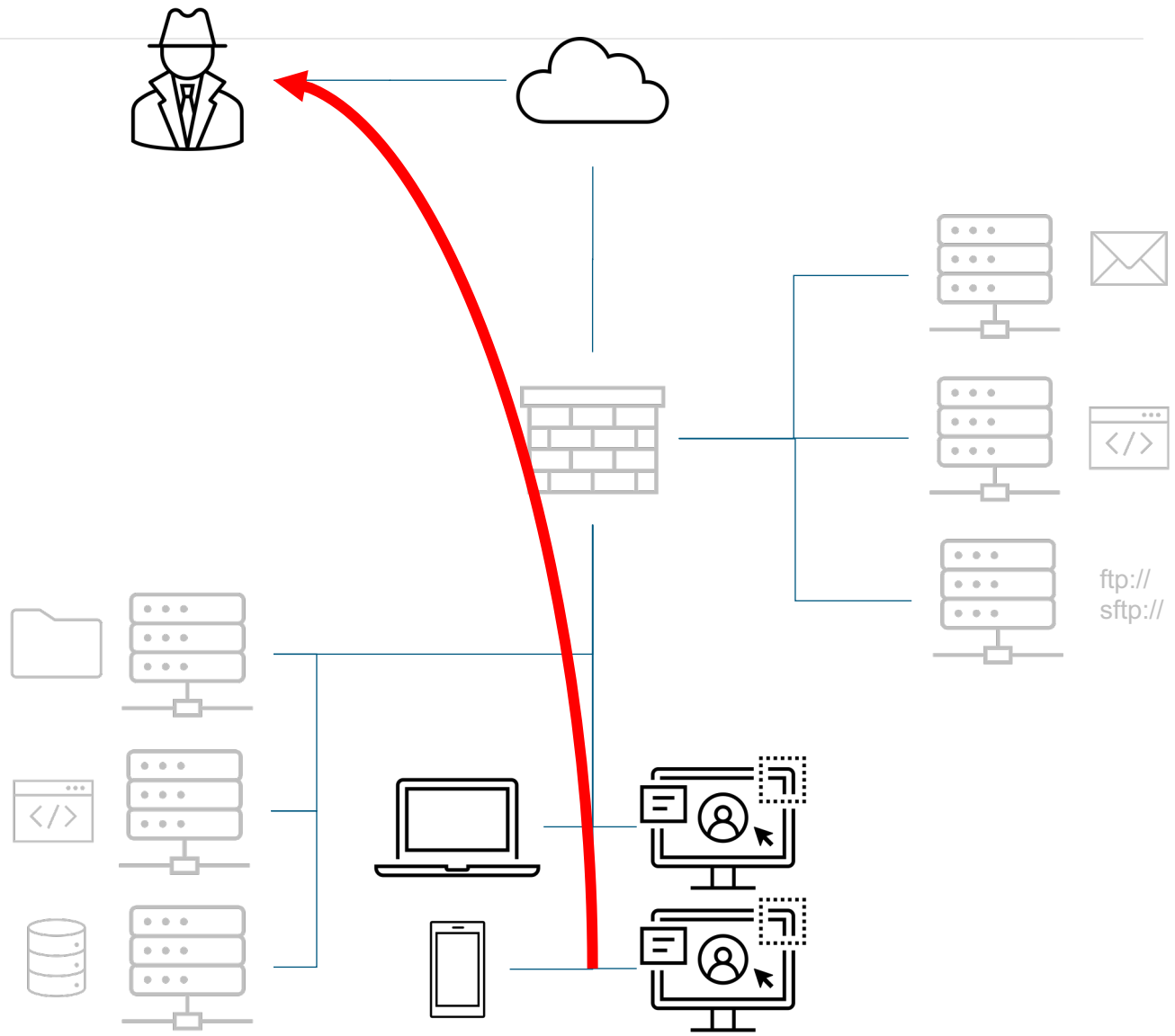
Attackers depend on internet traffic to deliver exploits, payloads, and command and control messages – *find it and take it away*

How to Do It

- Firewall rules
- Web Content Filtering
- DNS Content Filtering
- Network Monitoring Tools

Outbound Traffic Controls

- **Firewall Rules**
  - Deny traffic to or from unnecessary IP ranges (Consider RIRTools)
  - Limit traffic to *required* connections
  - Egress rules are *critical*
- **Web Content Control**
  - Next Gen firewalls, Web Proxies, etc. have databases of categorized domains
  - Block uncategorized domains
  - Block unnecessary web traffic to reduce noise
  - Block specific content types (EXEs, etc)
- **DNS Content Filtering**
  - Similar Web Content Filtering, but only based on domain name resolution
  - Effective alternative if Web filtering isn't an option
- **Network Monitoring Tools**



Defensive Technique #4

Rapid Containment

Learn what you can, then interdict.

When it's time to contain, move fast.

Have WRITTEN pre-authorization to take systems and networks offline as needed.

Conventional Wisdom Isn't always Wise.

- Sometimes you need systems online
- What if you're not allowed to block a system?

Attacks are brittle

Small actions with big impact on attackers.

Look for points of interdiction!

- Firewall rules
- Account lock/disable
- DNS entries
- Routing/network VLAN
- Power off system?

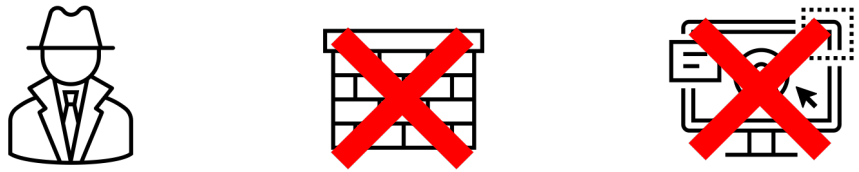
HOMEWORK:
Please get written pre-authorization
(The appendix in the PDF)

Multiple points of Defense

Focus on attacker frustration!

Attackers rely on lots of elements.

Deny one, entire campaign can unravel.



Defensive Technique #5

Application Control

Deny Malware & Limit LOL Attacks

Application Control is amazing... but risky.

Not used enough!

Fear of misconfiguration is real.

Let your systems tell you how to configure

- Know exactly what apps are running.
- Use SRUM-DUMP or tools like it.

Defensive Technique #6

Sustainable Workflow

Perfect is the Enemy of Good

When in crisis mode... any non-breaking improvement... is an improvement.

Small Improvements Over Time

- Find and work easiest issues.
- Make something "less painful"
- Focus on removing noise

SANS | GIAC CERTIFICATIONS

Thank You

Mick Douglas
@BetterSafetyNet
mdouglas@sans.org

Jon Gorenflo
@flakpacket

Mick Douglas

- **SANS Principal Instructor**
  - SEC504
  - SEC555
- **Founder, InfoSec Innovations**
  - Boutique security solutions
    - Defense focus, offensive capability
    - Research forward & specialized services

Jon Gorenflo

- **SANS Certified Instructor**
  - SEC504
  - SEC560
- **Founder, Fundamental Security**
  - Security Consulting Services
    - Penetration Testing
    - Vulnerability Assessments
    - General Security Consulting