MODULE ID

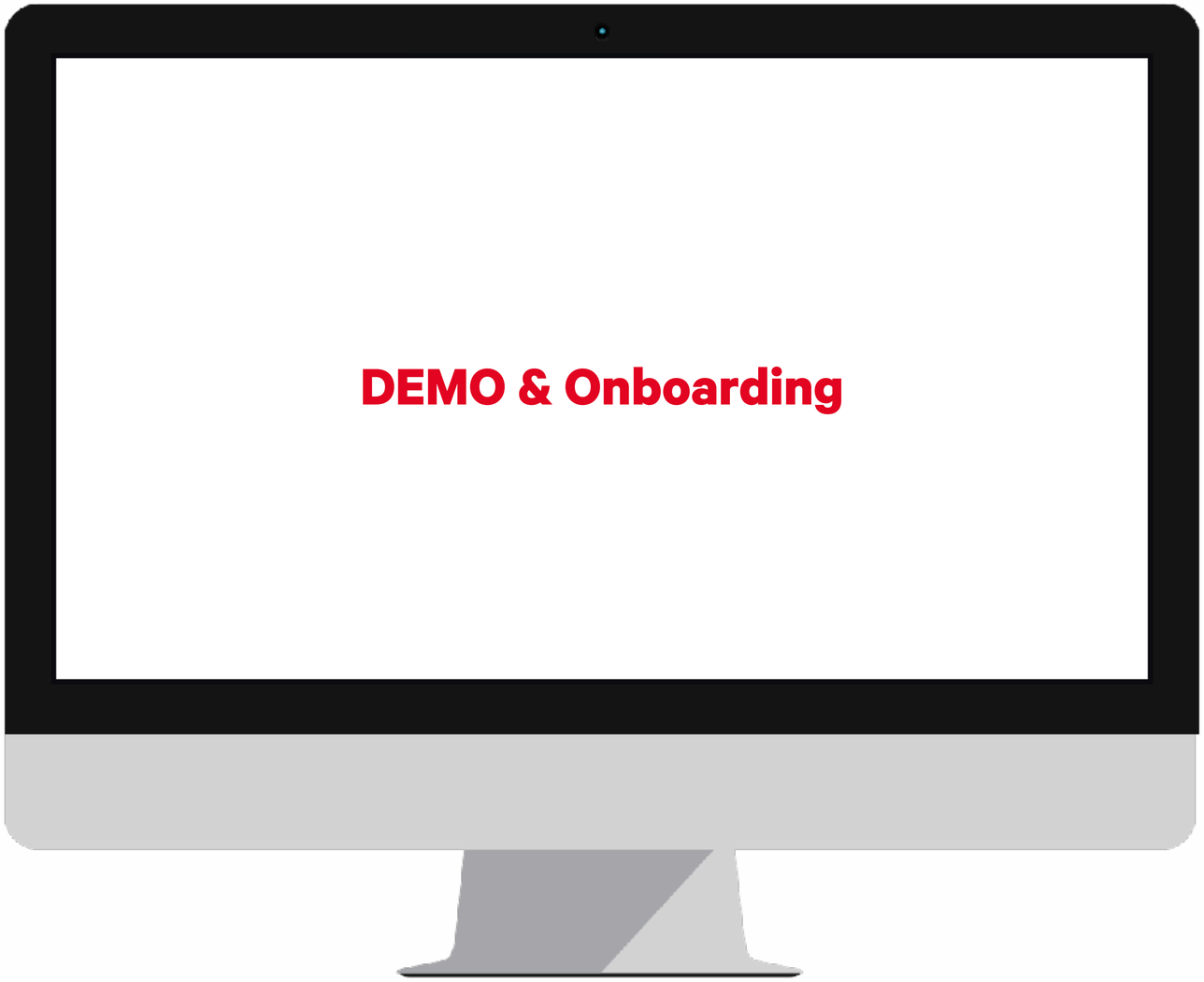
INTRODUCTION INTO CYBER SECURITY FOR IT PROFESSIONALS

Marco

- Equestrian
- Background in software development
- Defensive AppSec research and assessment
- Lecturer (TH-Nürnberg) software security engineering
- Co-author iX publications on SAP security

https://www.linkedin.com/in/marcohammel/

Information



Learning Objectives

- You're able to understand cyber security domains in the context of application security
- You know root causes of security defects in software
- You know the concepts of adversarial frameworks for threat intelligence, threat hunting and emulation
- You can categorise defensive measures by their tactical approach
- You can determine the applicability of deceptive and active countermeasures
- You understand common defensive tools processes and approaches.

MODULE ID

FUNDAMENTALS OF APPLICATION SECURITY

Learning Objectives

- You understand where application security fits into a cyber security domain model
- You can describe the limitations of different security layers
- You know the relevance of input validation and output encoding
- You can assess security traits of simple application workflows
- You understand possible causes of software security defects

Chapters

Application Security in the cyber domain

The dilemma of code security and limitations of security domains and tools

Causes of security defects

Causes of security defects in software development

Input validation

Considerations of securing software by input validation

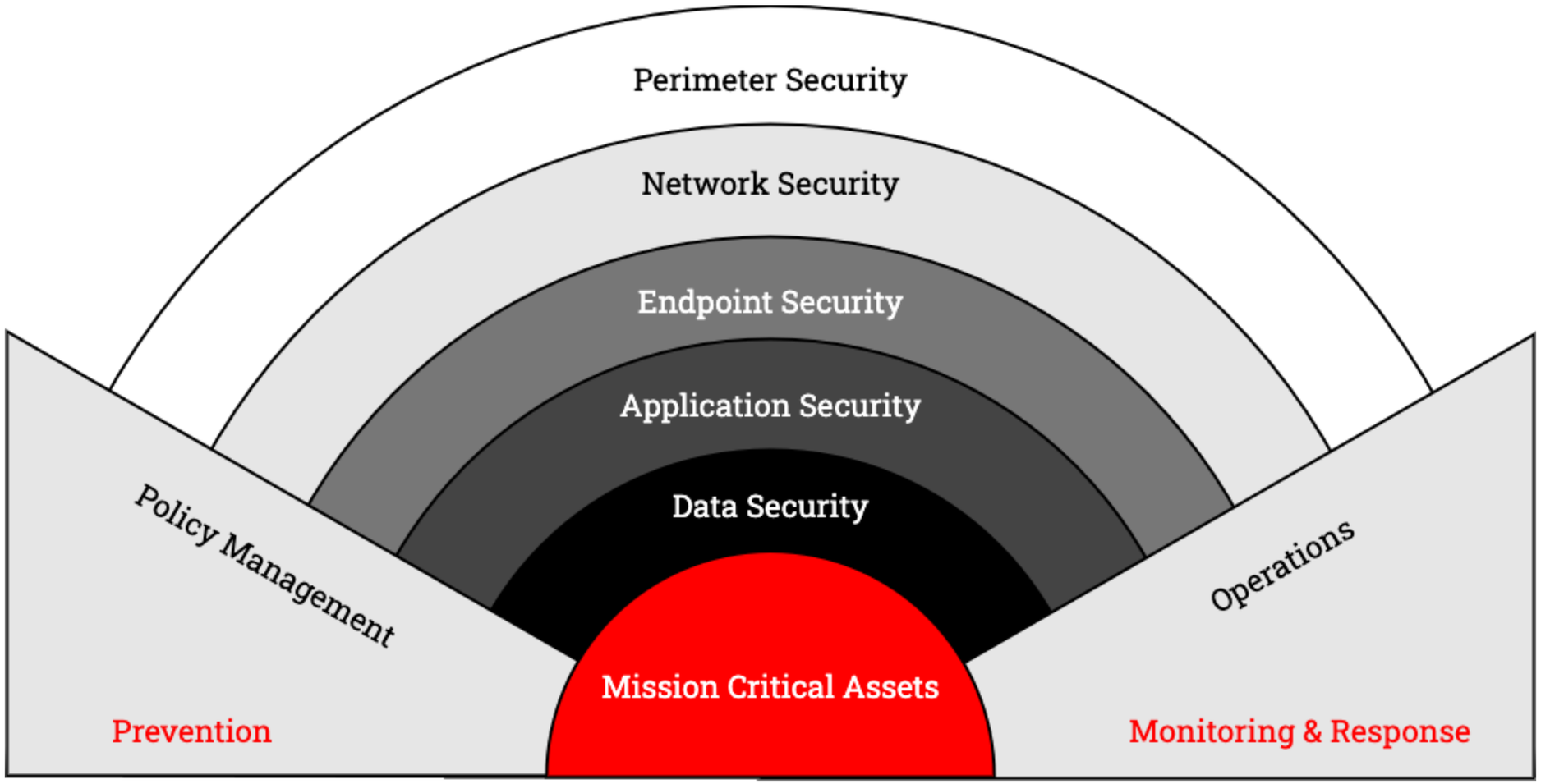
Output encoding

Considerations of securing software by output encoding

Conclusion

APPLICATION SECURITY IN THE CYBER DOMAIN

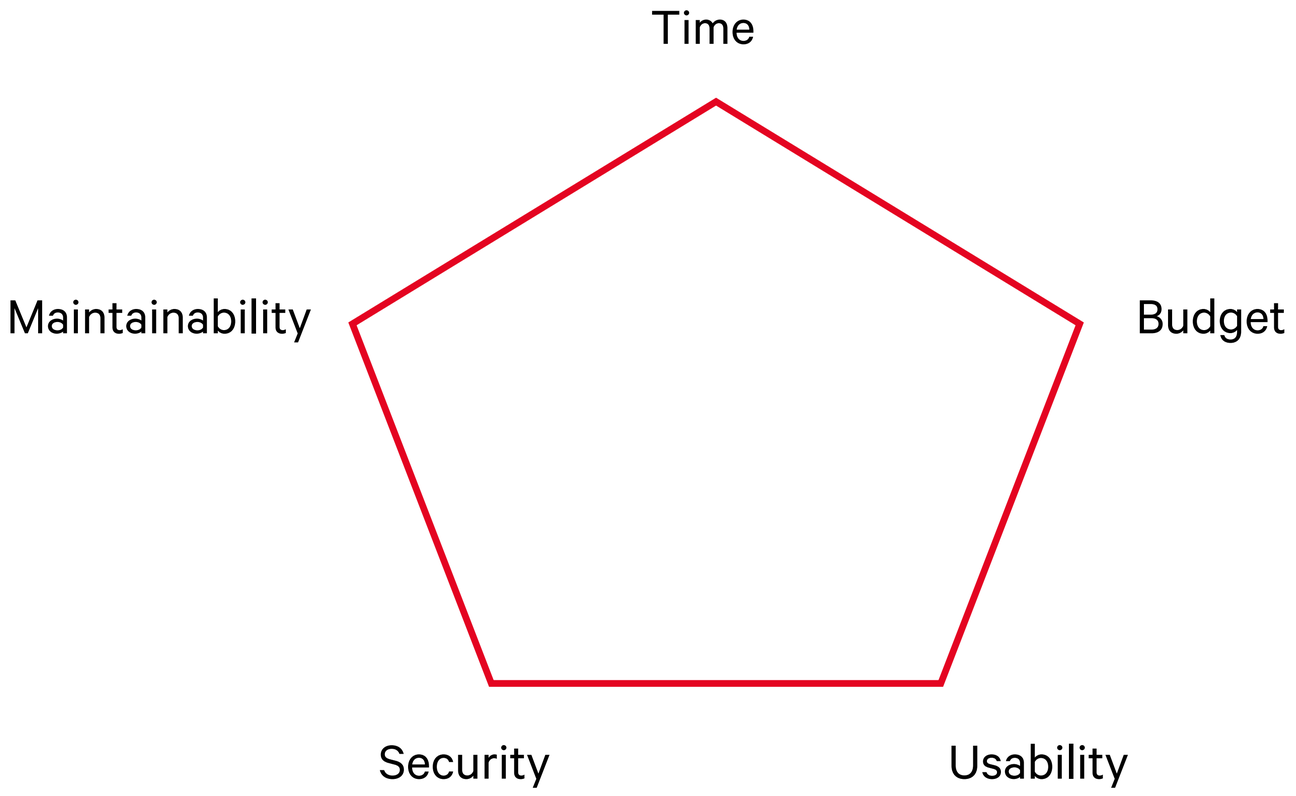
DOMAINS OF PROTECTION



Nothrop Grumman Security Fan

SECURITY AREAS OF ACTION

DILEMMA OF SECURING SOFTWARE



LIMITATIONS OF SECURITY LAYERS

- Firewalls don't make applications secure —> but limit access
- Intrusion prevention systems don't make applications secure —> but might detect attack patterns
- Encryption doesn't make applications secure —> but support confidentiality & integrity of data in transfer & storage
- Access control doesn't make applications secure —> but reduce the attack surface
- Reverse proxies don't make applications secure —> but limiting access of clients
- Web Application Firewalls don't make applications secure —> but might detect and prevent suspicious use when trained
- Scanners are insufficient to detect all vulnerabilities —> because they don’t understand the business context

CAUSES OF SECURITY DEFECTS

ROOT CAUSE OF SECURITY DEFECTS

Security defects can be introduced at various points in the software development process

SPECIFICATION

Missing requirements

DESIGN

Inappropriate architecture / design

IMPLEMENTATION

Implementation flaws

TEST

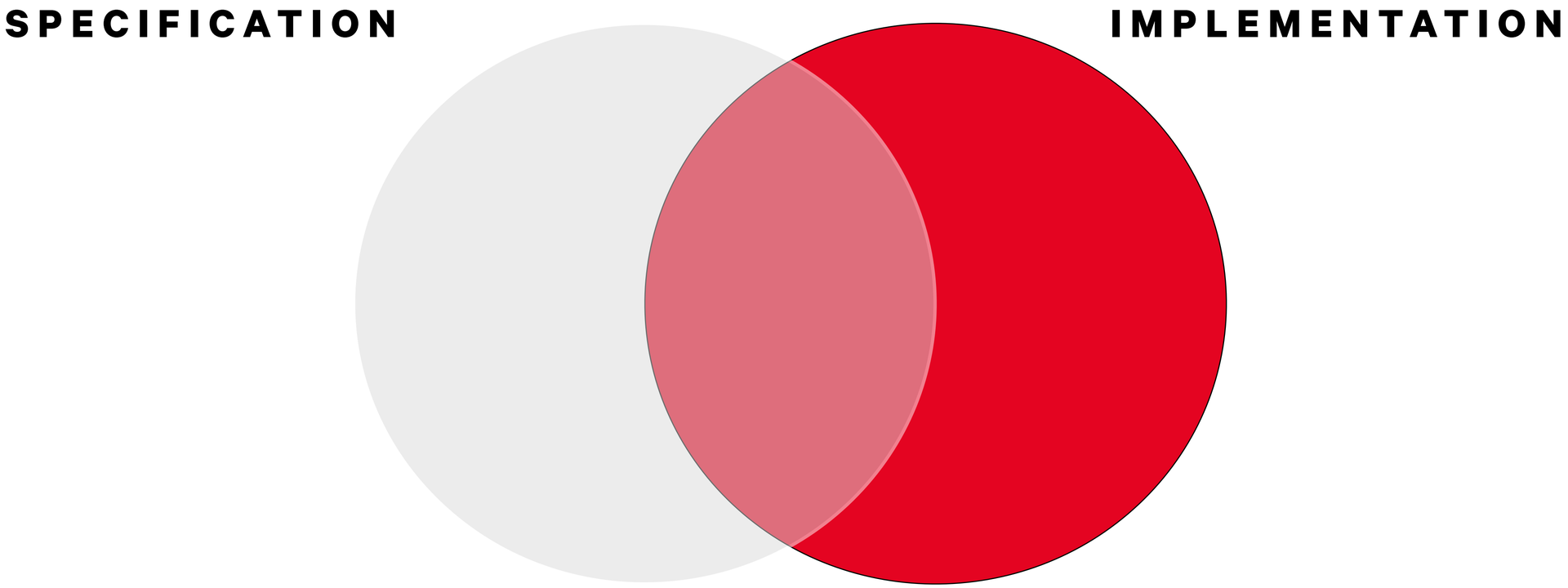
Inappropriate security testing

Mostly False Implicit Assumption

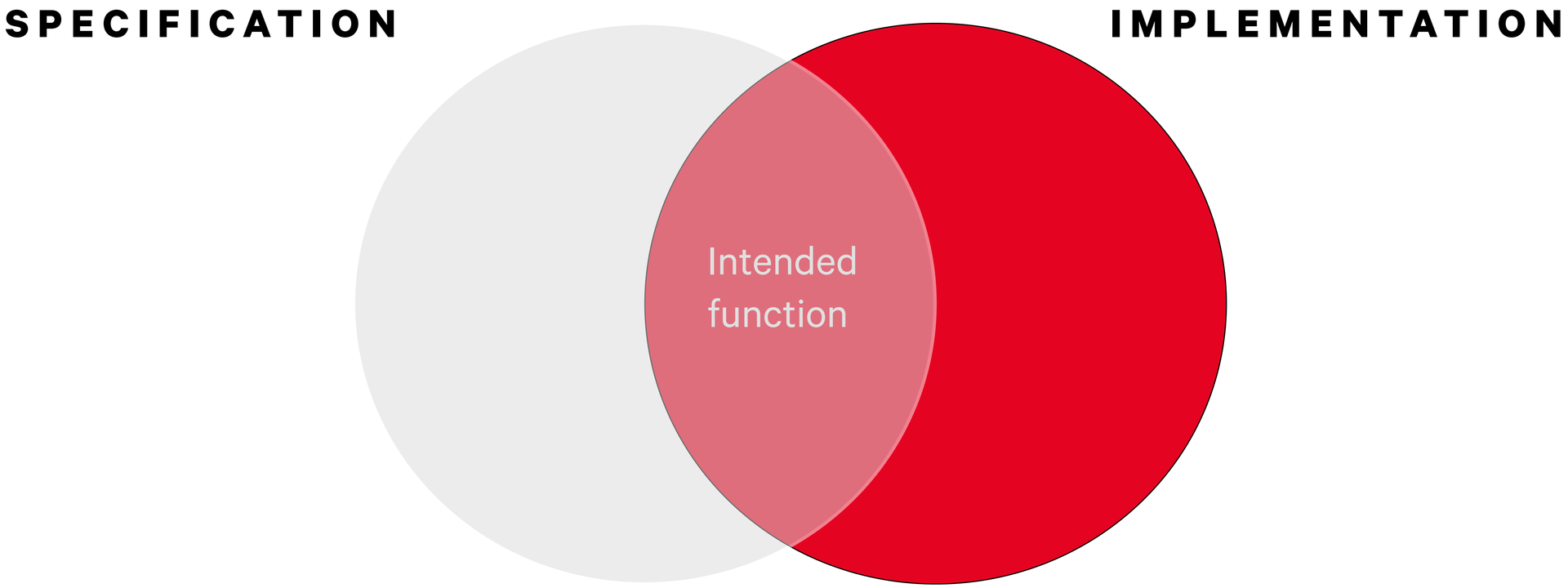
ROOT CAUSES OF SECURITY DEFECTS

SPECIFICATION

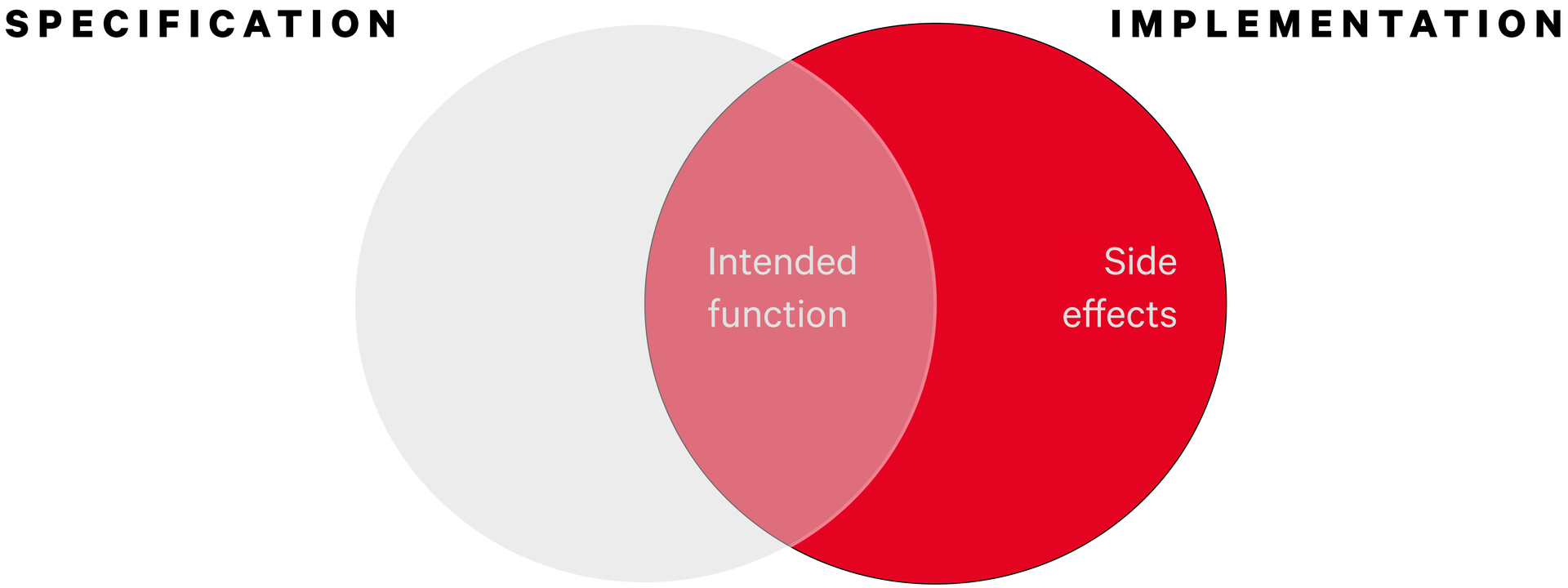
ROOT CAUSES OF SECURITY DEFECTS



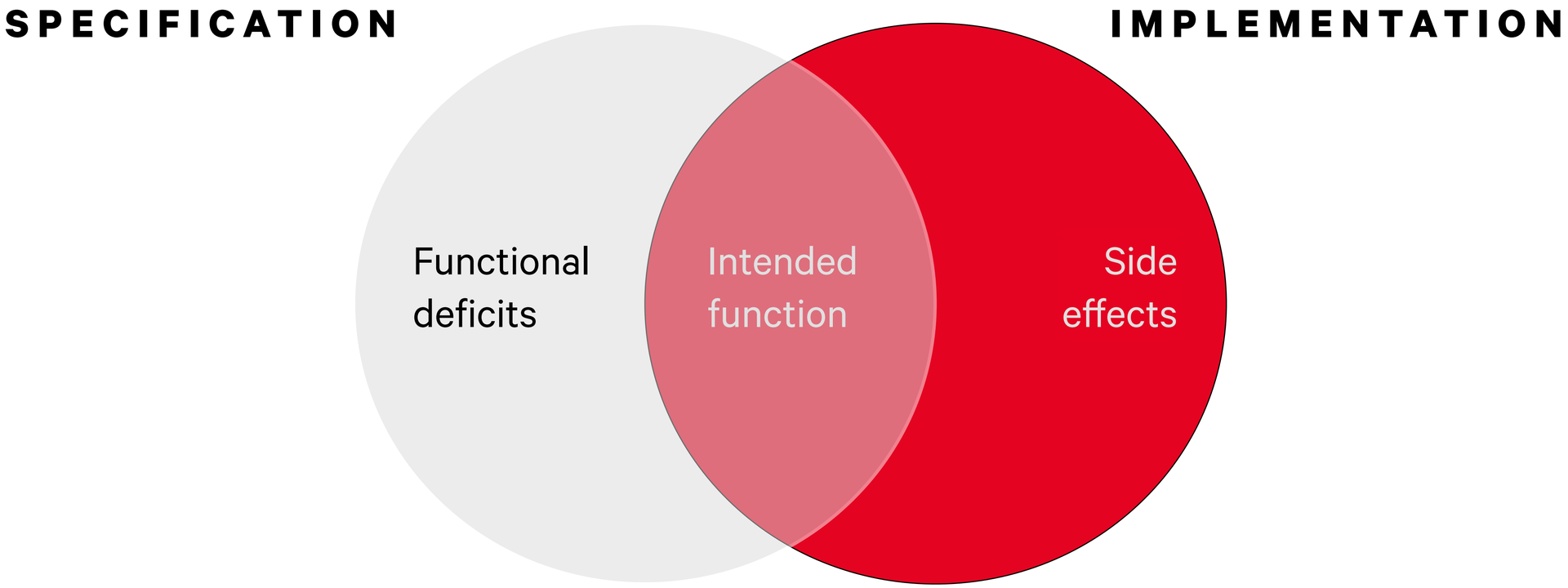
ROOT CAUSES OF SECURITY DEFECTS



ROOT CAUSES OF SECURITY DEFECTS



ROOT CAUSES OF SECURITY DEFECTS



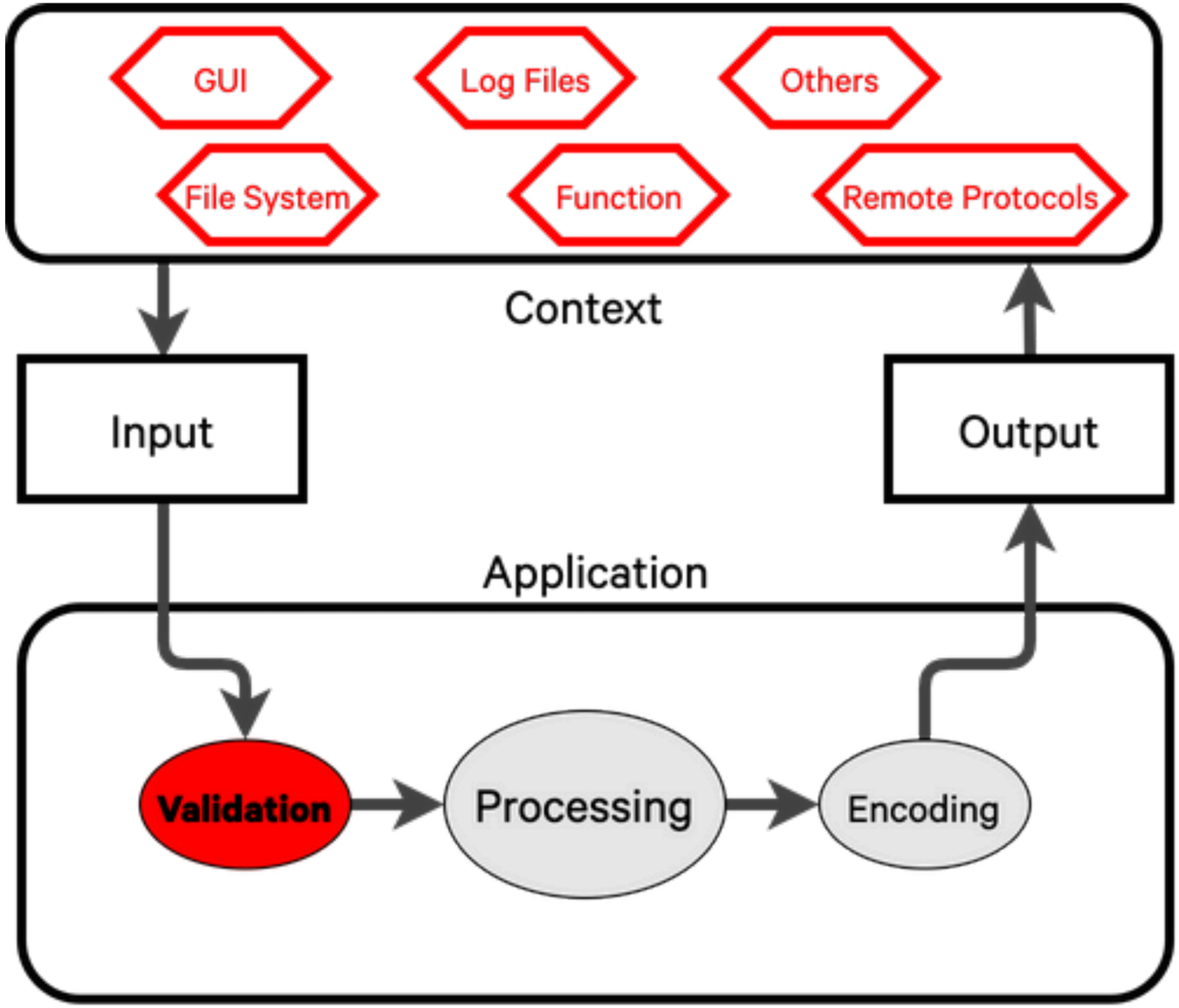
INPUT VALIDATION

PRIAM

KING OF TROY

„We should have done input validation“

BOUNCER
HOW INPUT VALIDATION SHOULD LOOK LIKE
HOW IT ACTUALLY LOOKS LIKE
imgflip.com

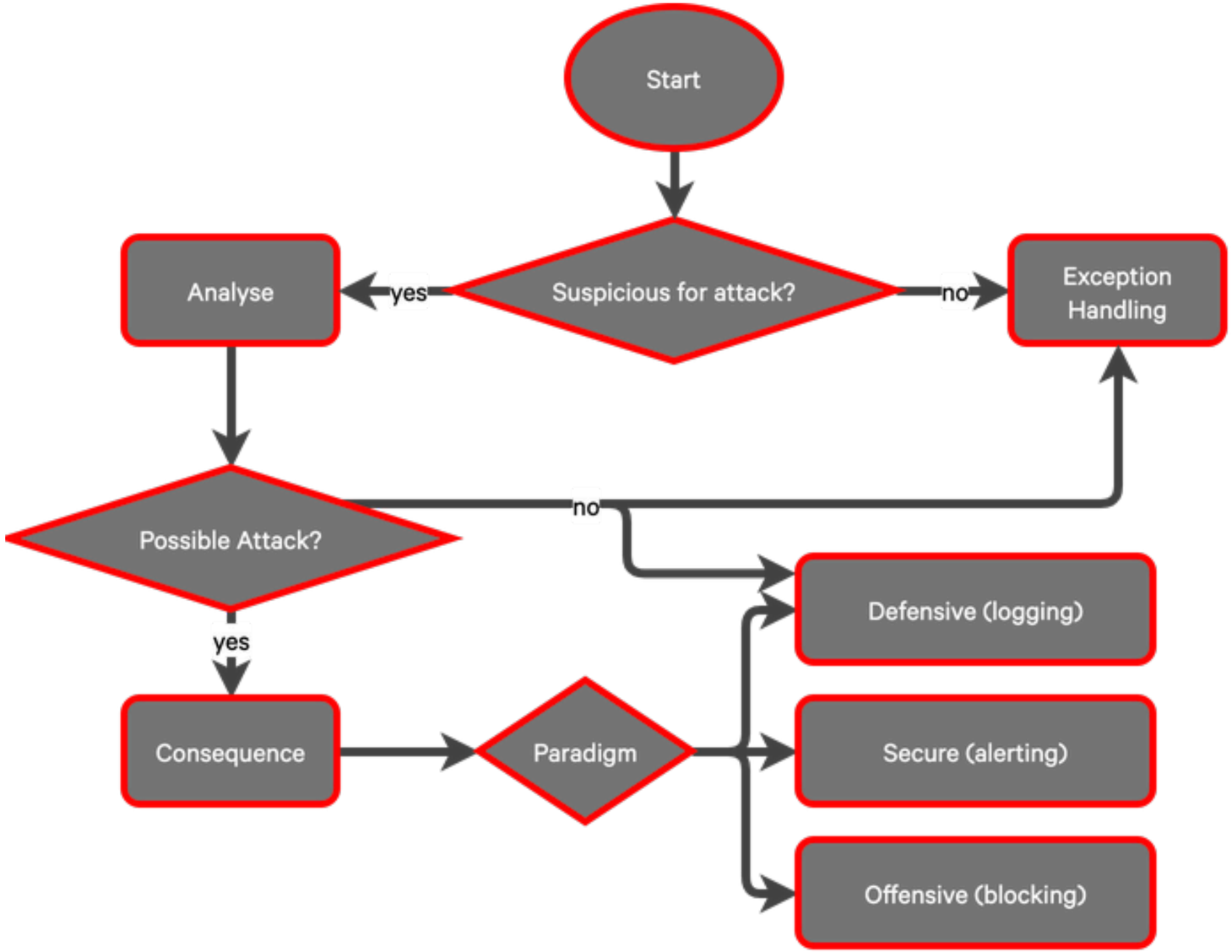

GUI
Log Files
Others
File System
Function
Remote Protocols
Context
Input
Output
Application
Validation
Processing
Encoding

A GENERAL APPROACH

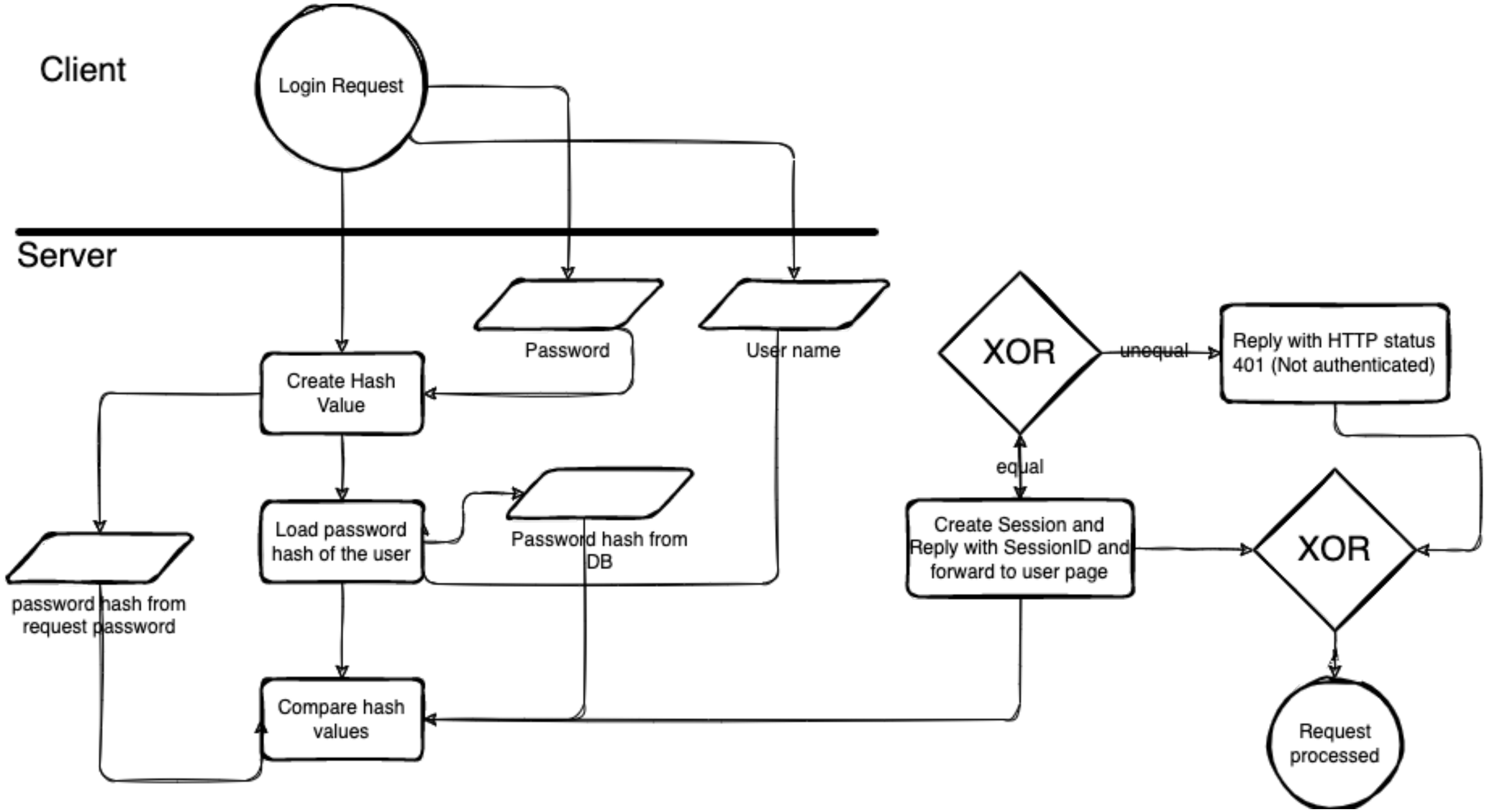
1. Discover input sources and input
2. Make assumptions about the input explicit
3. Validate the input
4. Decide on validation results

1. Existence / length
2. Canonice
3. Check type
4. Check value range
5. Filter
   1. Blacklist
   2. Whitelist

TAKING CONSEQUENCES



- Which input validation is missing in the following implementation of a login routine?
- How can we fix the implementation of the login routine?
- What kind of paradigm do you find appropriate here and why?


Client
Login Request
Server
Password
User name
Create Hash Value
password hash from request password
Load password hash of the user
Password hash from DB
Compare hash values
XOR
unequal
Reply with HTTP status 401 (Not authenticated)
equal
Create Session and Reply with SessionID and forward to user page
XOR
Request processed

REASONS FOR CANONISATION

Valid representation of **<** character in HTML

%3C
&lt
<
&LT
<
&#60
&#060
&#0060
&#00060
&#000060
&#0000060
<
<
<
<
<
<
&#x3c
&#x03c
&#x003c
&#x0003c
&#x00003c
&#x000003c
<
<
<
<
<
<
&#X3c
&#X03c
&#X003c
&#X0003c
&#X00003c
&#X000003c
<
<
<
<
<
<
&#x3C
&#x03C
&#x003C
&#x0003C
&#x00003C
&#x000003C
&#x000003C
<
<
<
<
<
<
&#X3C
&#X03C
&#X003C
&#X0003C
&#X00003C
&#X000003C
<
<
<
<
<
<
\x3c
\x3C
\u003c
\u003C

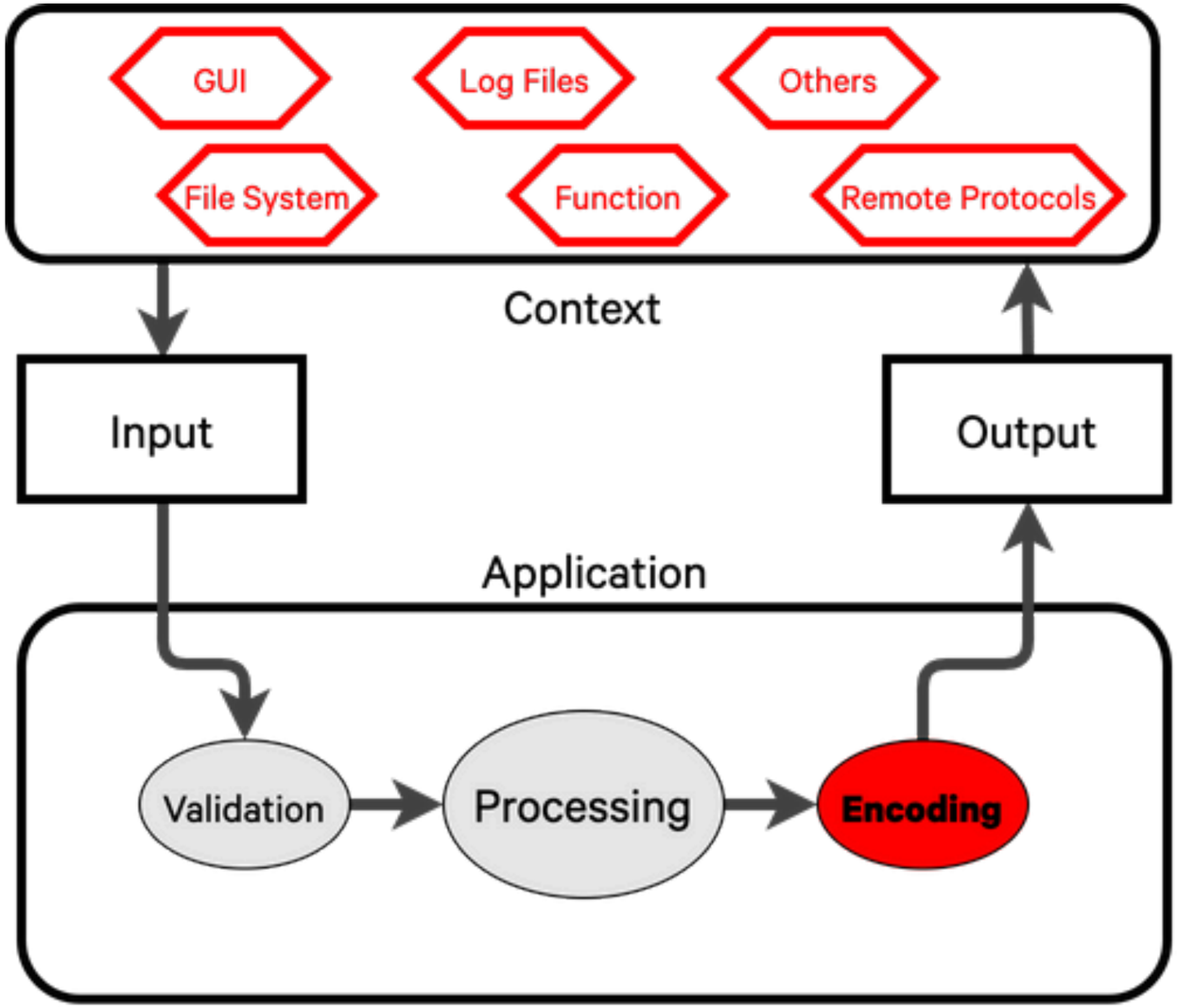
ENCODINGS ON TOP

Encoding	Encoded Text
clear	Demo Text<TAG attr='value' />
URL	%22Demo%20Text%22%3cTAG%20attr='value'%20/%3e
URL-Hex	%22%44%65%6d%6f%20%54%65%78%74%22%3c ...
URL-Unicode	%u0022%u0044%u0065%u006d ... %u003c ...
HTML-Named	&quotDemo Text&quot&ltTAG attr&equals'value' &sol&gt
HTML-Decimal	&#34&#68&#101&#109&#111&#32 ... &#60 ...
HTML-Hex	&#x22&#x44&#x65&#x6d&#x6f&#x20 ... &#x3c ...
HTML-Hex long	&#x0022&#x0044&#x0065&#x006d ... &#x003c ...
JS escaped	\"Demo Text\"<TAG attr=\'value\' />
XML escaped	"Demo Text"<TAG attr='value' />

CHAPTER TITLE

FUZZING THE GOLDEN TICKET

OUTPUT ENCODING


GUI
Log Files
Others
File System
Function
Remote Protocols
Context
Input
Output
Application
Validation
Processing
Encoding

DRIVER

STUCK IN A DEAD END

„But the navigation system said …“

FREE BEER
imgflip.com

WHAT NEEDS TO BE ENCODED

Command signatures and special characters
which will have command-like effects for the parser.

- Code: <script>... <script>
- In band singled commands: DROP TABLE
- characters like: ; , space, return

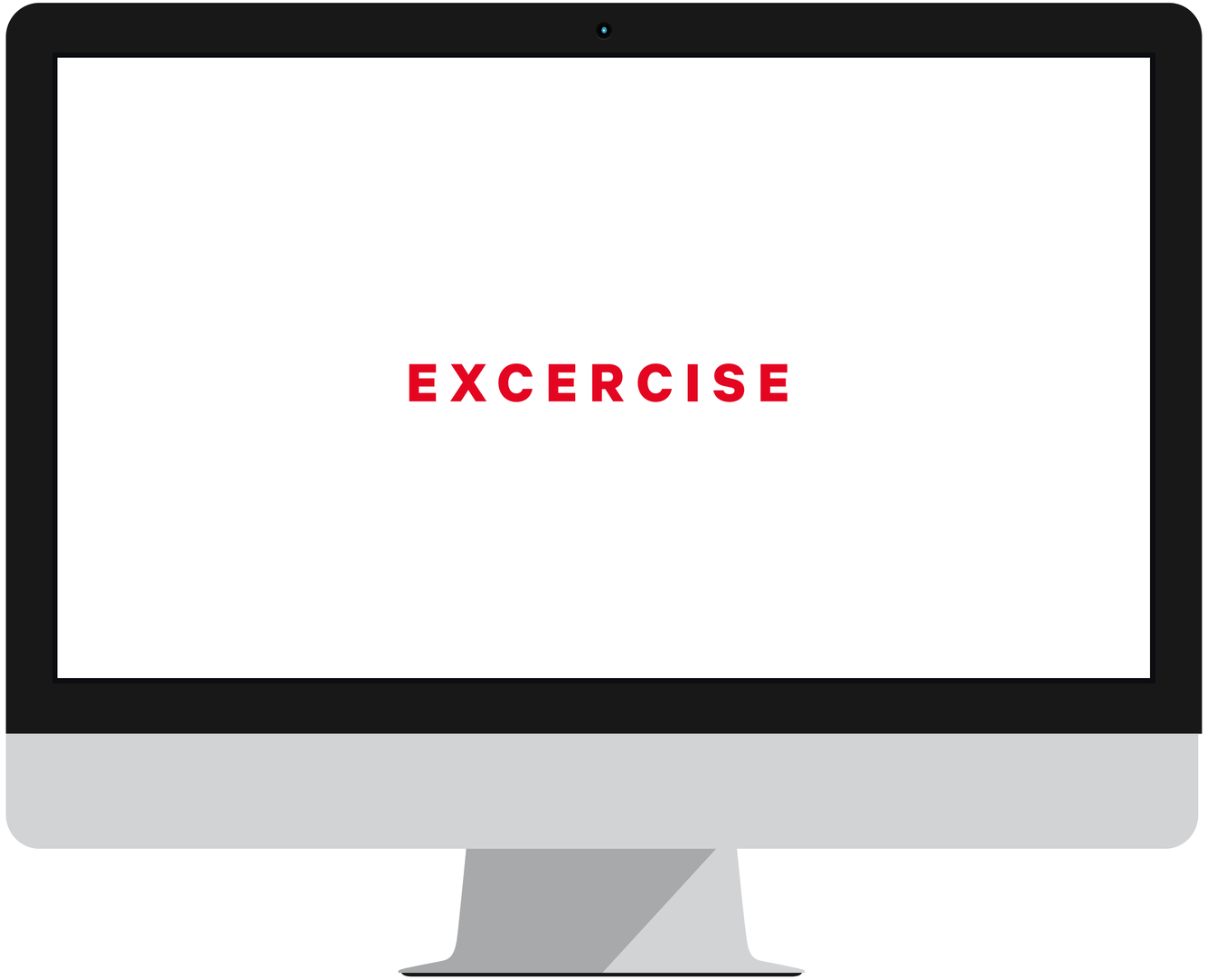
A GENERAL APPROACH

1. Discover output target
2. Make assumptions about the output processing explicit
3. Encode output accordingly
4. Ensure decoding is working properly

1. If appropriate validate for attack patterns
2. Decide on validation
3. Encode close to context transition

CHAPTER TITLE

WHY FILTERS ARE BAD FOR OUTPUT



CONCLUSION

TO TAKE AWAY

- Establish a code security policy
- Derive technology specific security guidelines for developers and testers
- Developers need appropriate requirements to create secure code. Enforce security engineering and design in the development process
- Also check the code security of external providers
- Establish and automate code quality and security tests across the software pipeline

END

UNDERSTANDING THE ADVERSARY

Learning Objectives

- Understand how the MITRE Attack framework can be used as a mid-level approach to attack simulation and response.
- Determine actual techniques by examples of security events.
- Determine possible adversary tactics based on examples.

Fundamentals of the Cyber Kill Chain

Introduction to the cyber kill chain

What is the cyber kill chain, and why do we use it?

Introduction to Threat Intelligence

What is threat intelligence and what can you get from it?

The MITRE ATT&CK framework

An introdcution into MITRE ATT&CK as a midlevel framework to operationalise security

Operationalizing MITRE ATT&CK

On overview of the options to use and start with MITRE ATT&CK

Conclusion

INTRODUCTION TO THE CYBER KILL CHAIN

Cyber Kill Chain

- Derived from military operations
- First introduced by Lockheed Martin in 2011
- Extended and united with the MITRE ATT&CK framework

- Benefits:
- Positioning security controls based on the framework

This Photo by Unknown Author is licensed under CC BY-ND

Lockheed Martin Kill Chain

INTRODUCTION TO THREAT INTELLIGENCE

Threat Intelligence

- Hardens cyber defenses through:
  - Adversarial data about tactics, techniques and procedures
    - Malware hashes
    - Known malicious domains / Ips
    - Known exploitation campaigns
    - …

This Photo by Unknown Author is licensed under CC BY-NC

Threat Intelligence Sources / Protocols / Tools

STIX

Structured Threat Information eXpression. The name is explicit: it is a standard for expressing information about computer threats in a structured and unambiguous way. Based on JSON

TAXII

Trusted Automated Exchange of Intelligence Information, is an intelligence exchange protocol over HTTPS. The standard defines a set of requirements for clients/servers and a REST API

MITRE CRITS

CRITs is an open source malware and threat repository that leverages other open source software to create a unified tool for analysts and security experts engaged in threat defense

THE MITRE ATT&CK FRAMEWORK

MITRE ATT&CK Framework

ATT&CK – Adversarial Tactics, Techniques, and Common Knowledge

Focuses on TTPs (Tactics, Techniques, and Procedures)

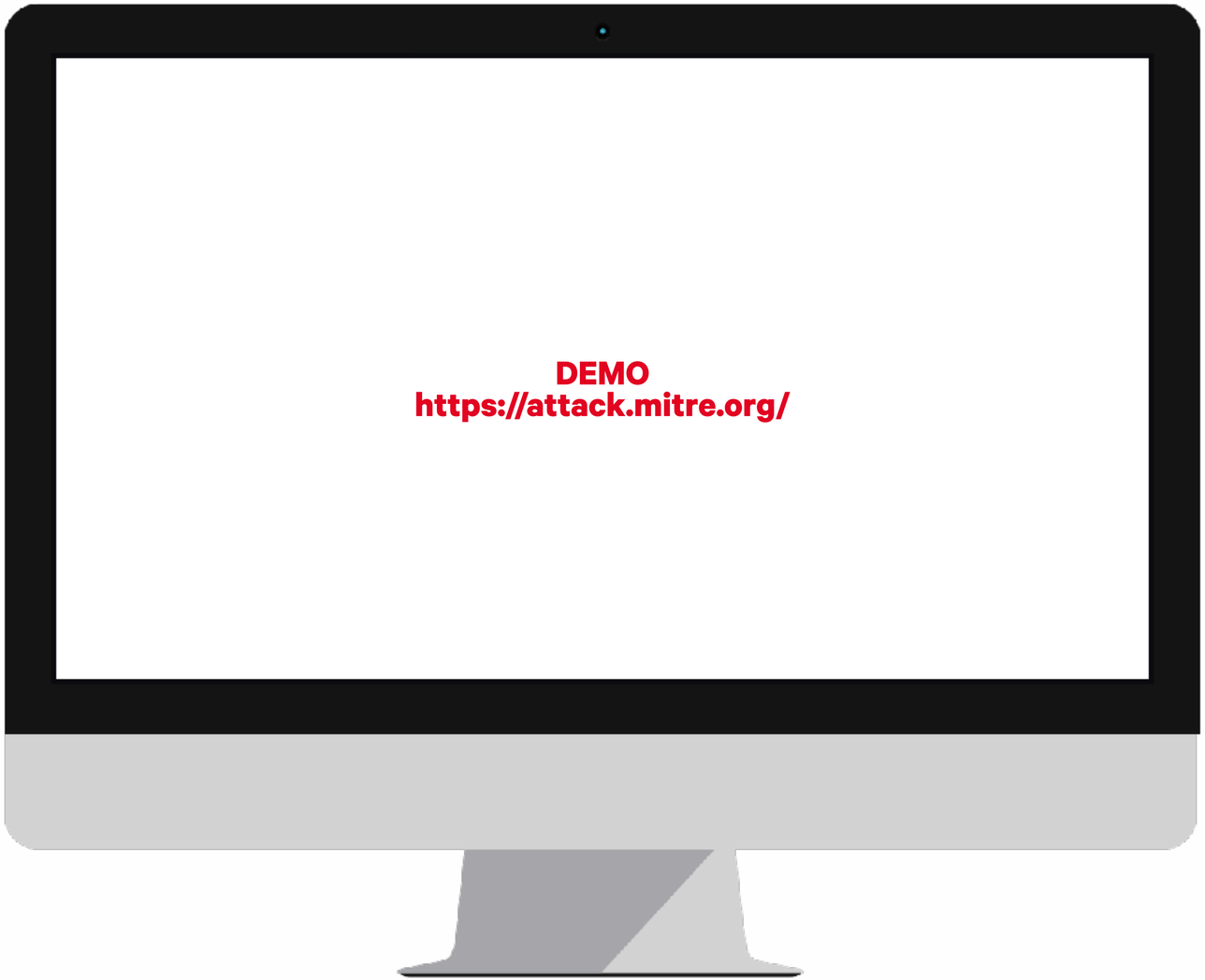
Helping blue teams focus on threats that exist

- Easier use case creation
- Identification of missing security controls or mechanisms

Red teams can run emulations

Purple teams combine the functions of red and blue to test security defenses

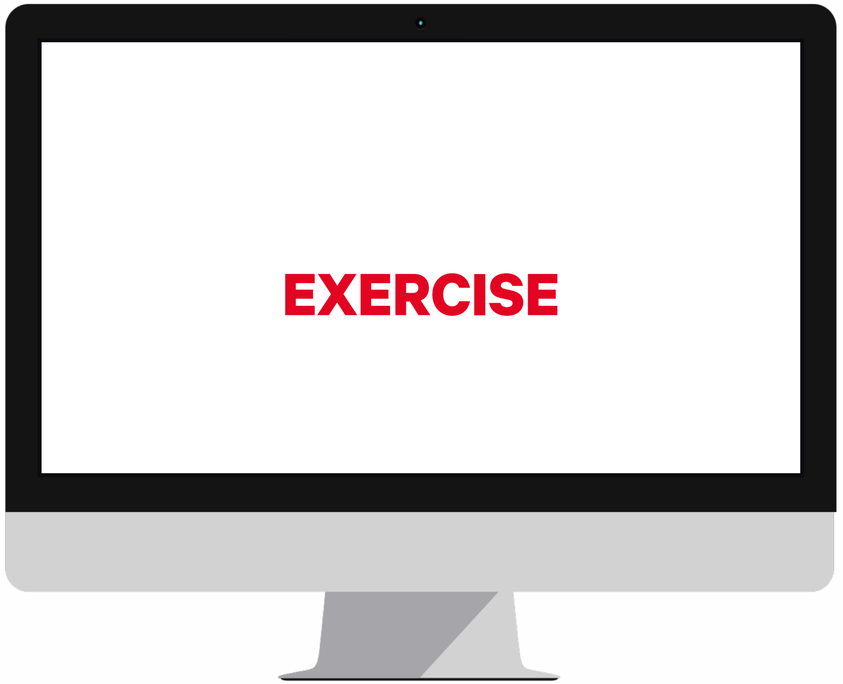
MITRE ATT&CK Framework



Hands-on operational activities

1. Threat Intelligence
2. Detection and Analytics
3. Adversary Emulation and Red Teaming

Threat Intelligence



- We are investigating an incident in the organization and have determined that it is related to a threat group called Fox Kitten. After getting initial access to the network, they were able to use Windows system internal tools (PsExec) to create a domain account to maintain access within the network.

1. Navigate to Threat Groups on the Mitre website (https://attack.mitre.org/groups/)
2. Search for the Threat Group in the scenario
3. Find the software they used to maintain access and list four techniques the tool can be used for
4. Preview the ATT&CK navigator to determine for which tactics the tool can be useful for

OPERATIONALIZING MITRE ATT&CK

Emulation Process:

Select
- Select a technique from the

Choose
- Choose how to conduct

Test
- Test the procedure against

Analyze
- Analyze detection and

Improve
- Improve defenses based on

Emulation Tools and Libraries

- AtomicAtomic Red
- CALDERA by MITRE
- MITRE Engenuity's Adversary emulation library

This Photo by Unknown Author is licensed under CC BY-NC

Ways to apply the MITRE ATT&CK

- Threat Intelligence
- Threat Hunting
- Automated testing and audit
- Compliance and regulatory mapping
- Risk management and strategy
- Training and exercises
- Security solution prioritization and evaluation
- Security pipeline validation

This Photo by Unknown Author is licensed under CC BY-SA-NC

CONCLUSION

Final Remarks

- **Know your enemies**

  Cyber attacks are real and you should organize your defense against real world attacks

- **Emulation as an approach to create visibility**

  Emulating an attacker can be easy. Understand what's important for you to see and verify if you do

- **You control MITRE ATT&CK**

  It's a best practice approach to provide you guidance on the way. It's not meant to tick all the boxes

- **It doesn't cost a fortune**

  Gathering threat intelligence can start without subscribing to a commercial service.

END

COUNTERMEASURES AND DECEPTION FOR THE DEFENDER

Learning Objectives

- Learn the difference between active and passive defence and prevention
- Learn the general concept of the OODA loop and how it works as a model to defend against attack strategies
- Understand the concept of endpoint detection & response (EDR)
- Understand the general concept of threat intelligence
- Learn the basic concepts and benefits of SOAR (Security Orchestration, Automation and Response).
- Follow the full lifecycle of an incident response plan to create an incident response plan and/or activity based on a successful attack scenario.

Chapters

Tactics of the Defender

Overview of defensive tactics for active and passive defense

The Defender's OODA Loops

An introduction to the OODA loop as a counter strategy to the cyber kill chain

The Defender's Toolbox

Overview of endpoint detection and response (EDR) as part of SOAR

Conclusion

TACTICS OF THE DEFENDER

Passive Defence & Prevention

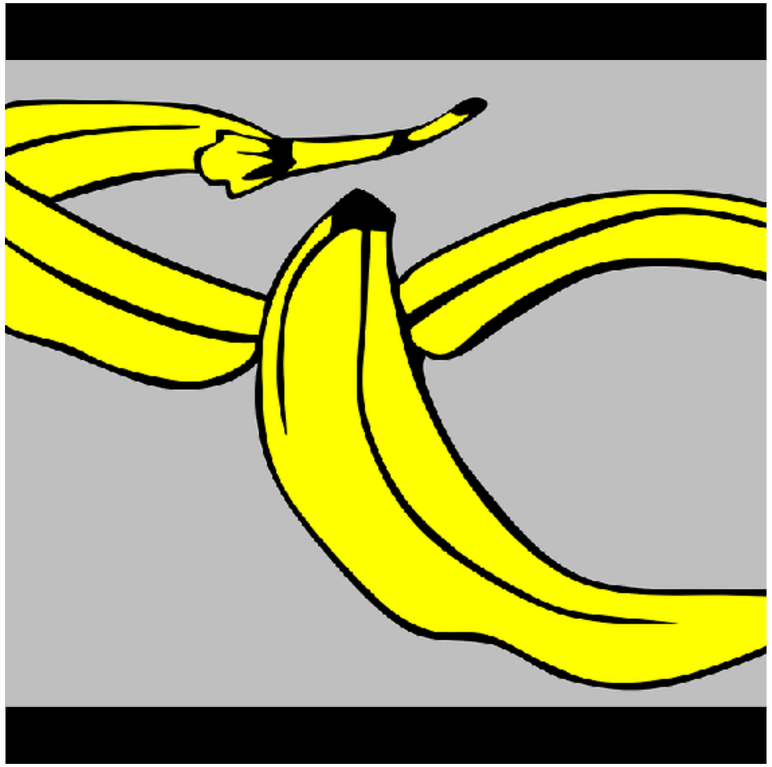
Measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative (i.e., hope for the best)

- Network Access Management
- Device Management
- Identity Management
- Deny- Allowlisting
- Vulnerability & Patchmanagement
- Hardening
- Lockpolicies
- …

Active Defensive and Offensive Countermeasures

- The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy
- Proactive, anticipatory, and reactionary actions against aggressors
- The adversaries are already breached the gates…
- Offensive countermeasures employ offensive techniques as aggressors attack with a defensive posture

Offensive Countermeasures - Cyber Deception



Deliberate and calculated process of deceiving attackers in an effort to wage a better defense

- Slow them down, confuse them, deceive them … make them work harder – Serves to significantly increase your chances of detection
- Designed to make $\text{Detection}_t + \text{Reaction}_t < \text{Attack}_t$ ($D_t + R_t < A_t$)
- It doesn't replace other efforts or layers of defense
- It should complement and feed the other layers

- Militaries have employed deception strategies since the beginning of time. Why don't we?

Brian Krebs

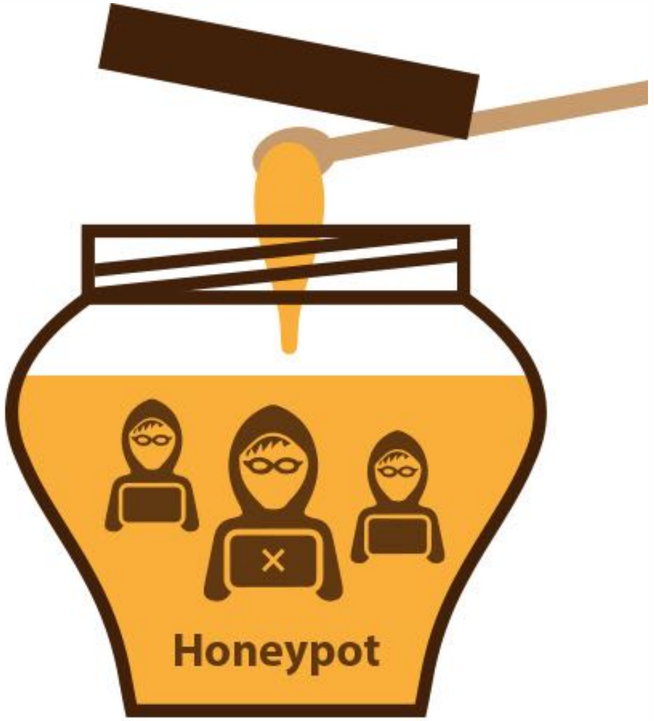
“Deception Technologies are nice, but advisable only if your organization is already doing 99% of the rest”

“There is an apparent lack of the use of deception technology”

Jeff Moss

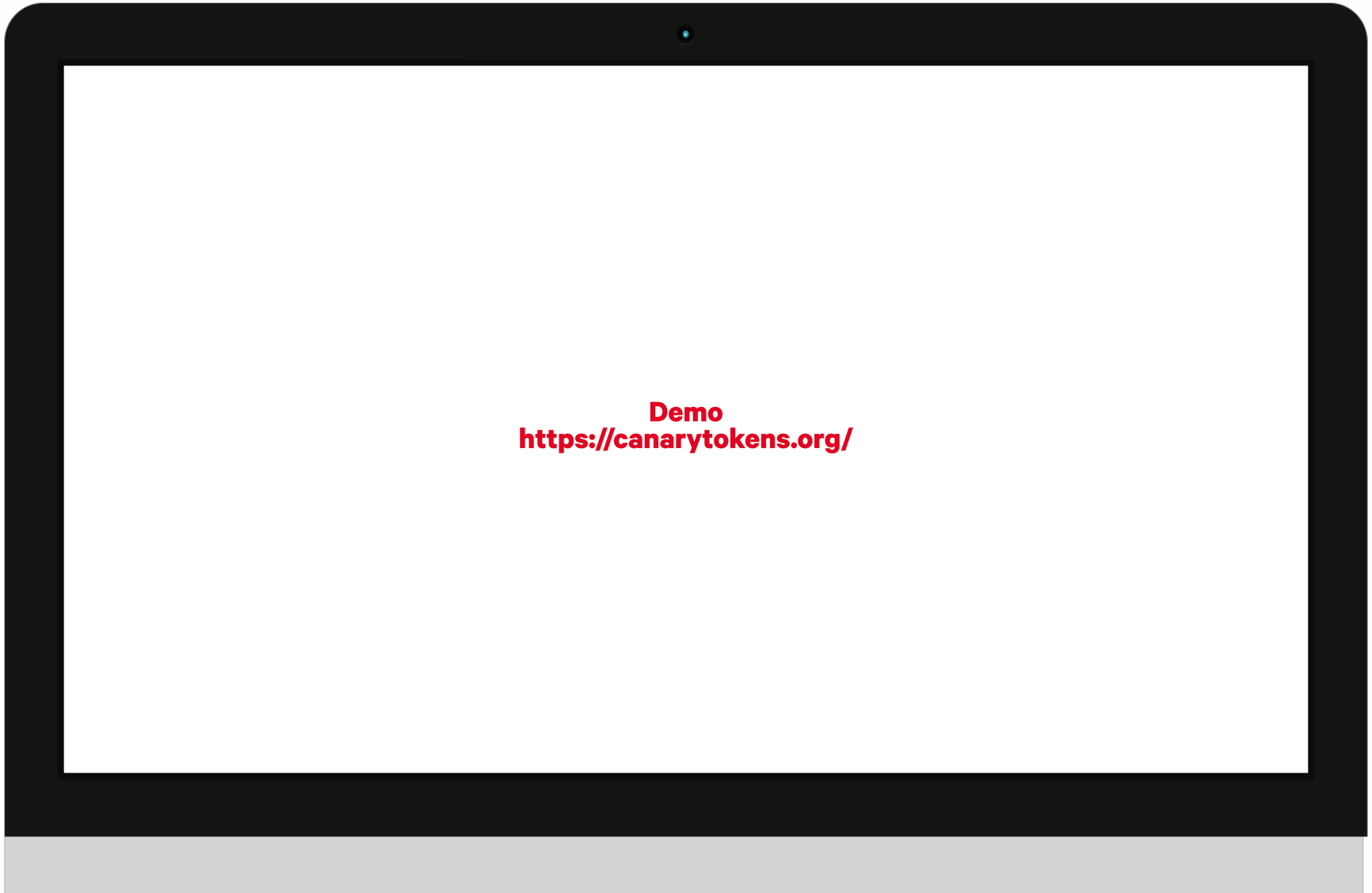
Offensive Countermeasures - Cyber Deception

- Honey Ports / Services / Pots / Nets
- Honey Docs / User
- Counter Attacks
  - Malware
  - …
- Attribution
  - Canary Tokens
  - Internal Threat Intelligence



Some Ideas Already?

Canary Tokes



NVIDIA Counter Hack

Nvidia hacked by ransomware group, steals its stolen data back

by Chadley Kemp

Sources suggest that Nvidia launched a cyber attack on hacker group Lapsu$ after the hackers stole 1TB of proprietary data.

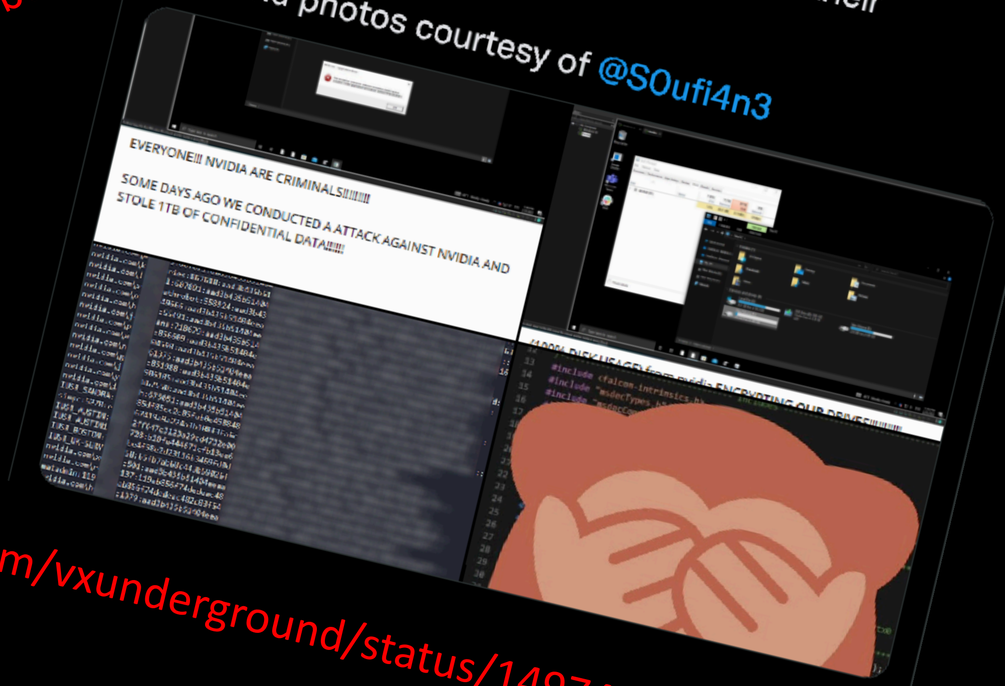
https://www.ginx.tv/en/video-games/nvidia-hacked-ransomware-steals-data-back

vx-underground
@vxunderground

LAPSU$ extortion group, a group operating out of South America, claim to have breached NVIDIA and exfiltrated over 1TB of proprietary data.

LAPSU$ claims NVIDIA performed a hack back and states NVIDIA has successful ransomed their machines

Intel and photos courtesy of @S0ufi4n3



https://twitter.com/vxunderground/status/1497484483494354946

Offensive Countermeasures – Legal Perspective

This Photo is licensed under CC BY-ND

A few simple tips go a long way…

- Don’t put malware where it is publicly accessible
- Prevent collateral damage
- Make the attackers come to you first
- Use warning banners and Terms of Use (TOU)
  - Warn of “evil” things on the network
  - Consult with a lawyer

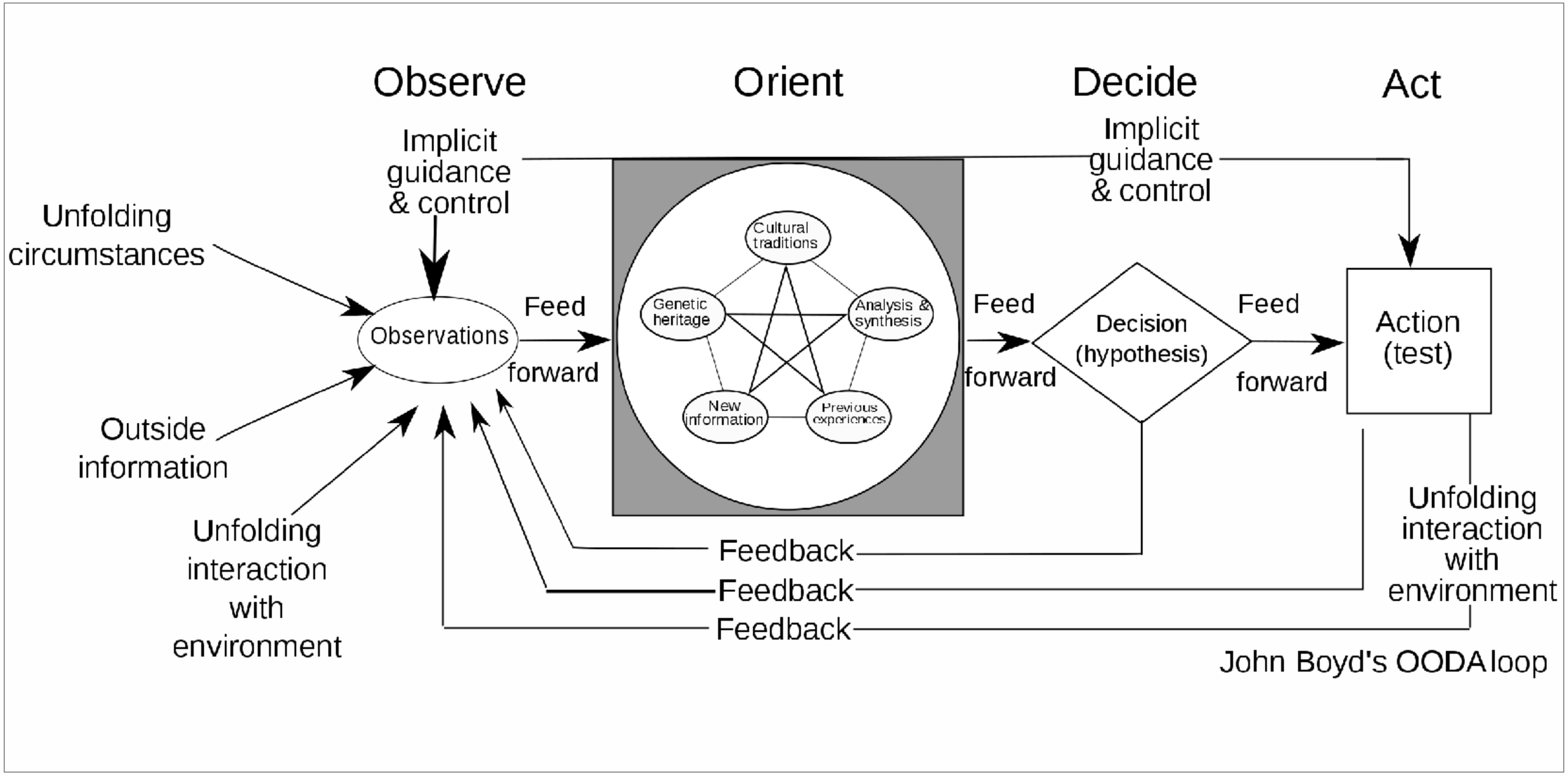
THE OODA LOOP

The Cyber OODA Loop

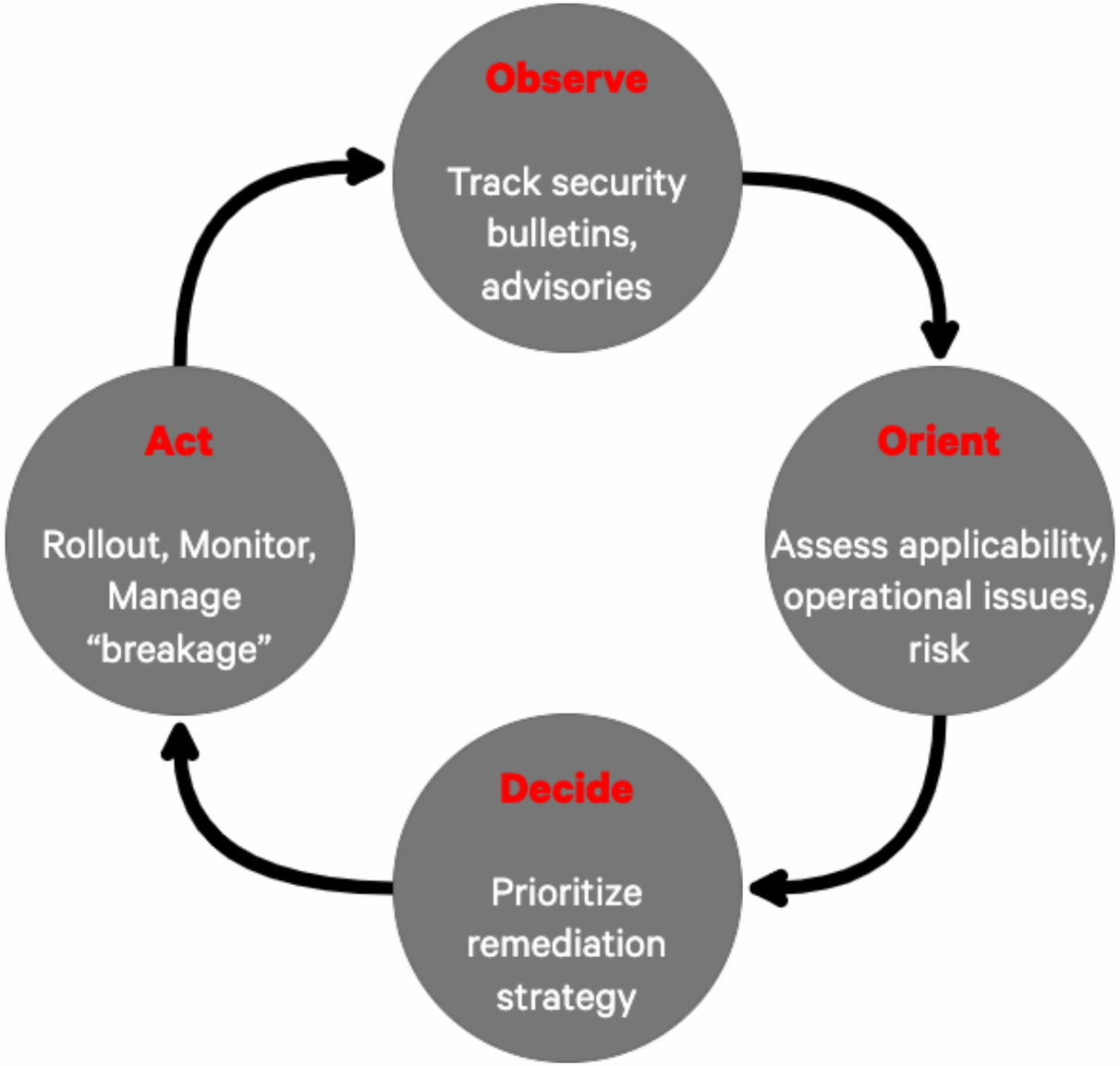
How Your Attacker Should Help You Design Your Defense Because:

$$Risk = f\{\frac{Vulnerability,\ Threat, Consequence}{countermeasures}\}$$

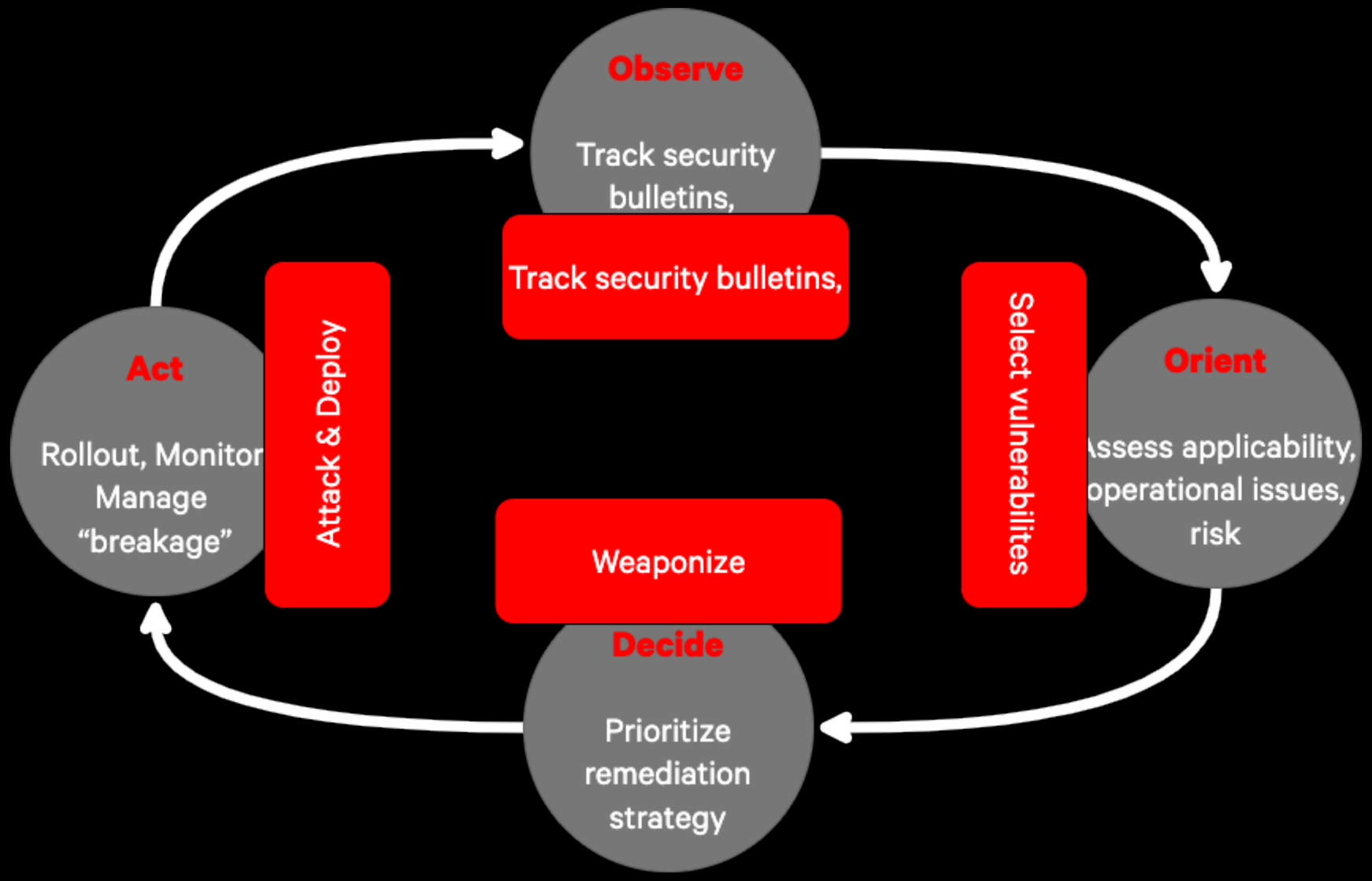
The General OODA Loop



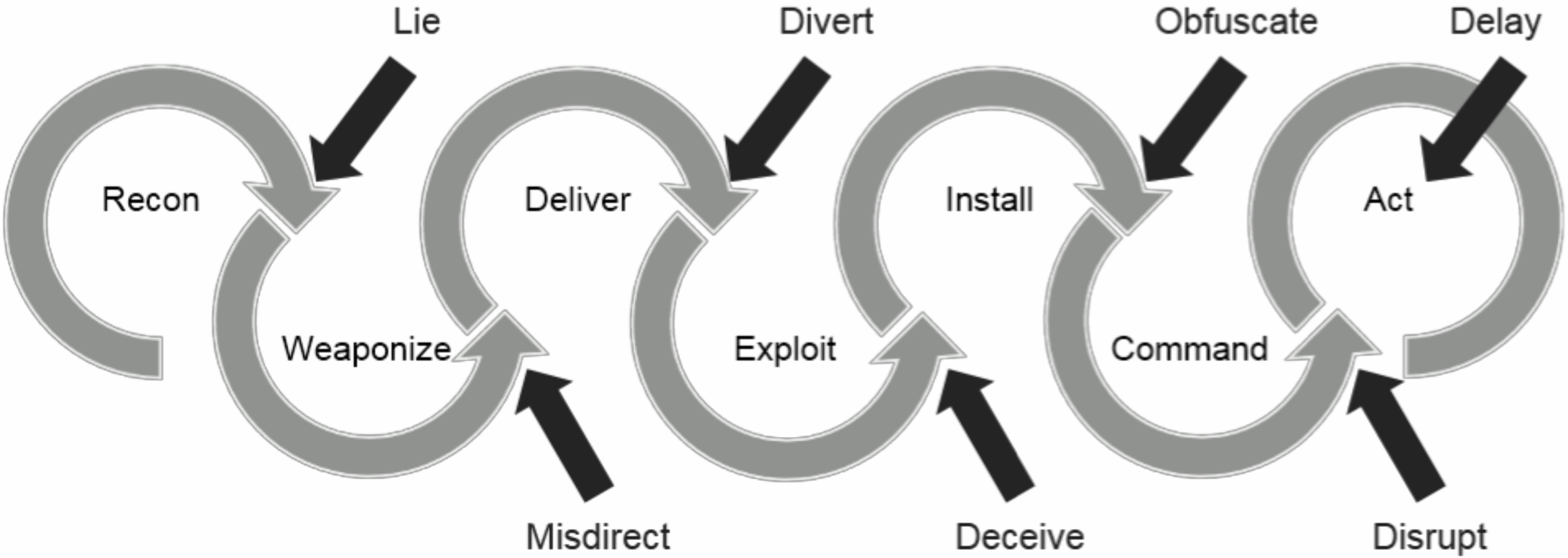
Patching Loop



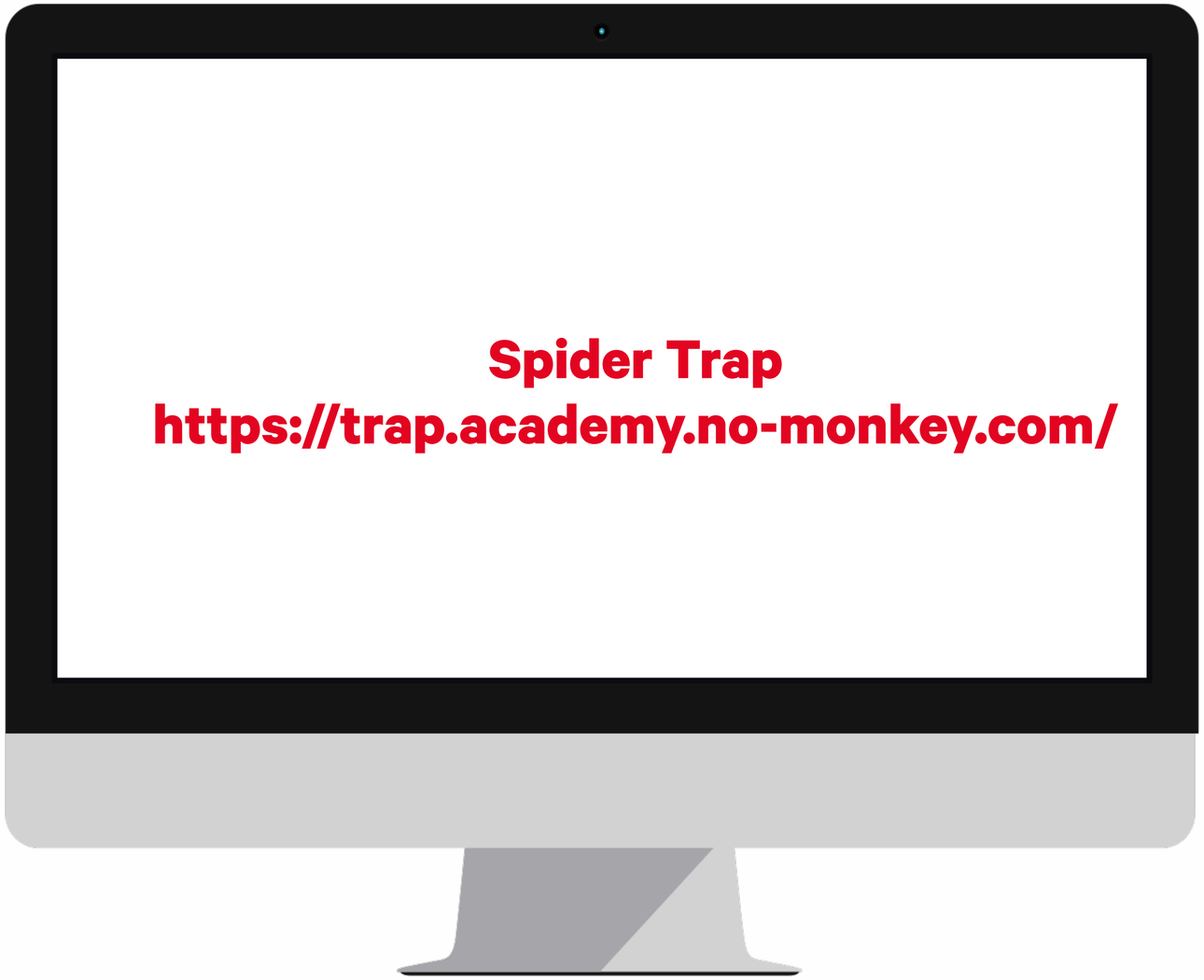
Patching Loop – Attacker Perspective



Breaking the Attacker's OODA



Demo

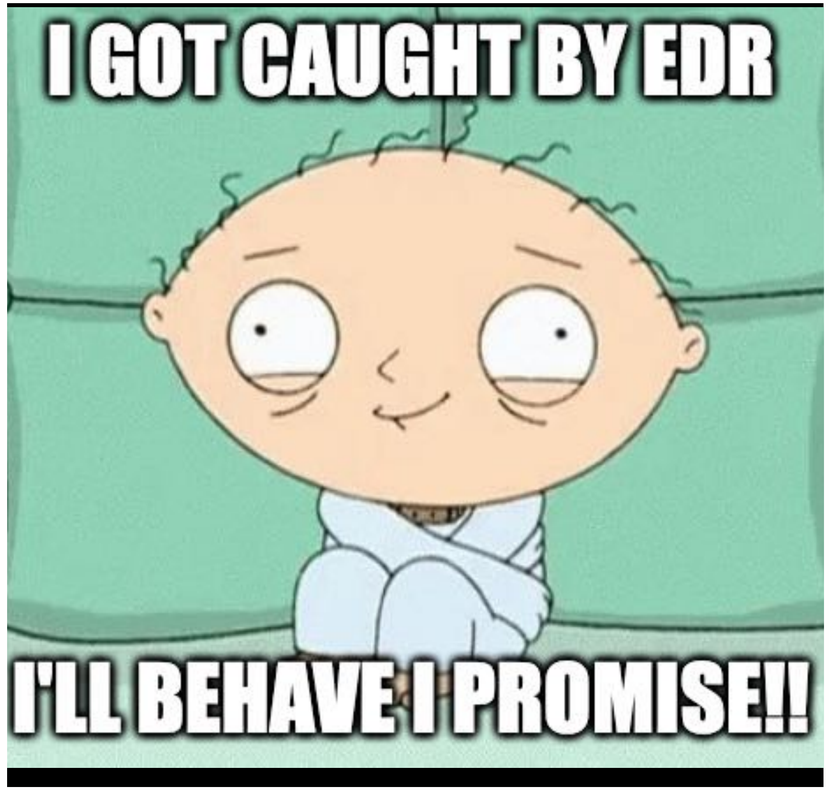


THE DEFENDER’S TOOLBOX

Why Endpoint Detection & Response

Because incident response becomes very difficult without it.
EDR is more about capabilities then tools

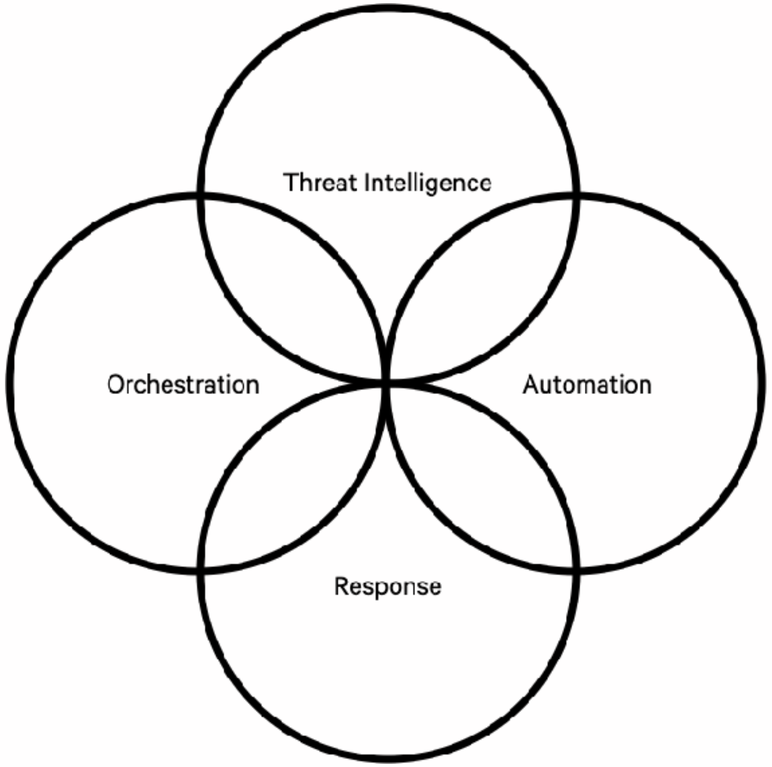
- Quickly getting information from multiple sources
- Correlating events from different endpoints and providing threat intelligence
- Combining malware signature-based and behavioural detection with user behaviour evaluation
- Blocking attempts for lateral movement



What about eXtended Detection and Response (XDR)?

Comparing EDR Solutions

Why Security Orchestration, Automation and Response?



Because without it, incident response doesn't scale and becomes too slow. SOAR is more about capabilities then tools

- Making security information from different sources relatable and digestible
- Reduce security operations fatigue by automating the boring things
- Defines a process to incorporate the creation of playbooks

Why is this not SIEM?

Breakdown - Why SOAR

Security Orchestration

- Security information from different sources is not normalized
- IT landscape becomes heterogenous and grows
- Operations doesn’t know which assets are the most important for the business

Automation & Response

- Reduce response time by use of playbooks and automation of activities
- Reduce mitigation time by automating repetitive work
- Automate detection based on orchestrated security information.

CONCLUSION

Final Remarks

- **Think like an attacker**
  They are humans. Understand what they're afraid of, what demotivates them and makes their lives harder
- **Containment requires coordination**
  There is no single activity to contain a breach in your network. Understand and align communication between each other
- **It's not rocket science**
  You're already doing a lot. Use and test all tactics applicable to your environment.
- **Active defense is for the small business too**
  If you can't afford running or paying a SOC it might be the only way to recognize if somebody is really after you.

END