Successful Security Operations

Christo Butcher
Executive Consultant
2023-05-04

Christo Butcher

Executive Consultant

20+ years in cyber security
15+ years at Fox-IT

Dabbled in renewable energy, speech recognition, molecular biophysics; but found cyber security the best mix of fun technical innovation and relevance to society

Now focused on helping organizations optimize their security strategy to defend themselves against the real cyber threats they face

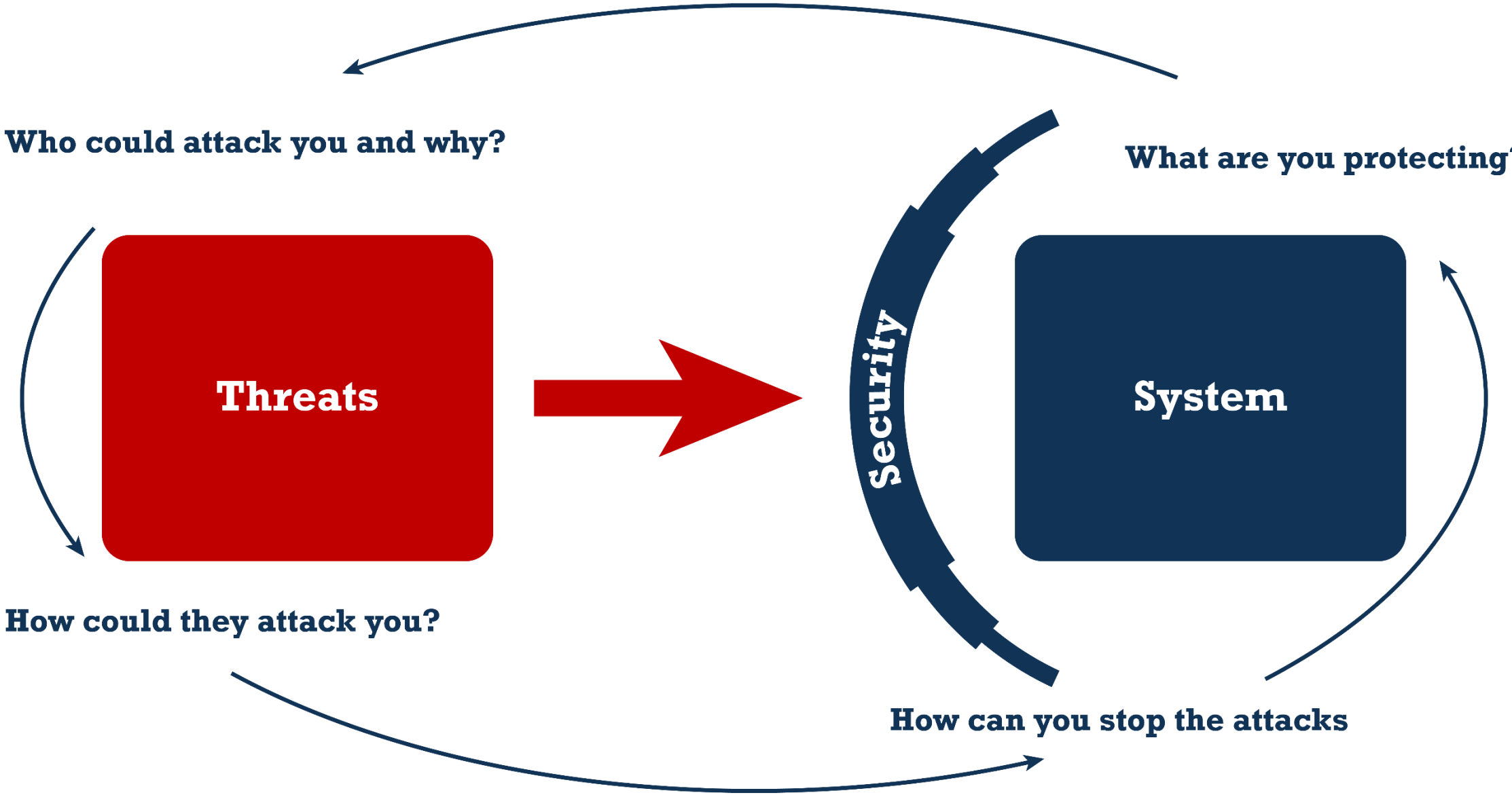

Photo by NIFTYART on Unsplash

Contents

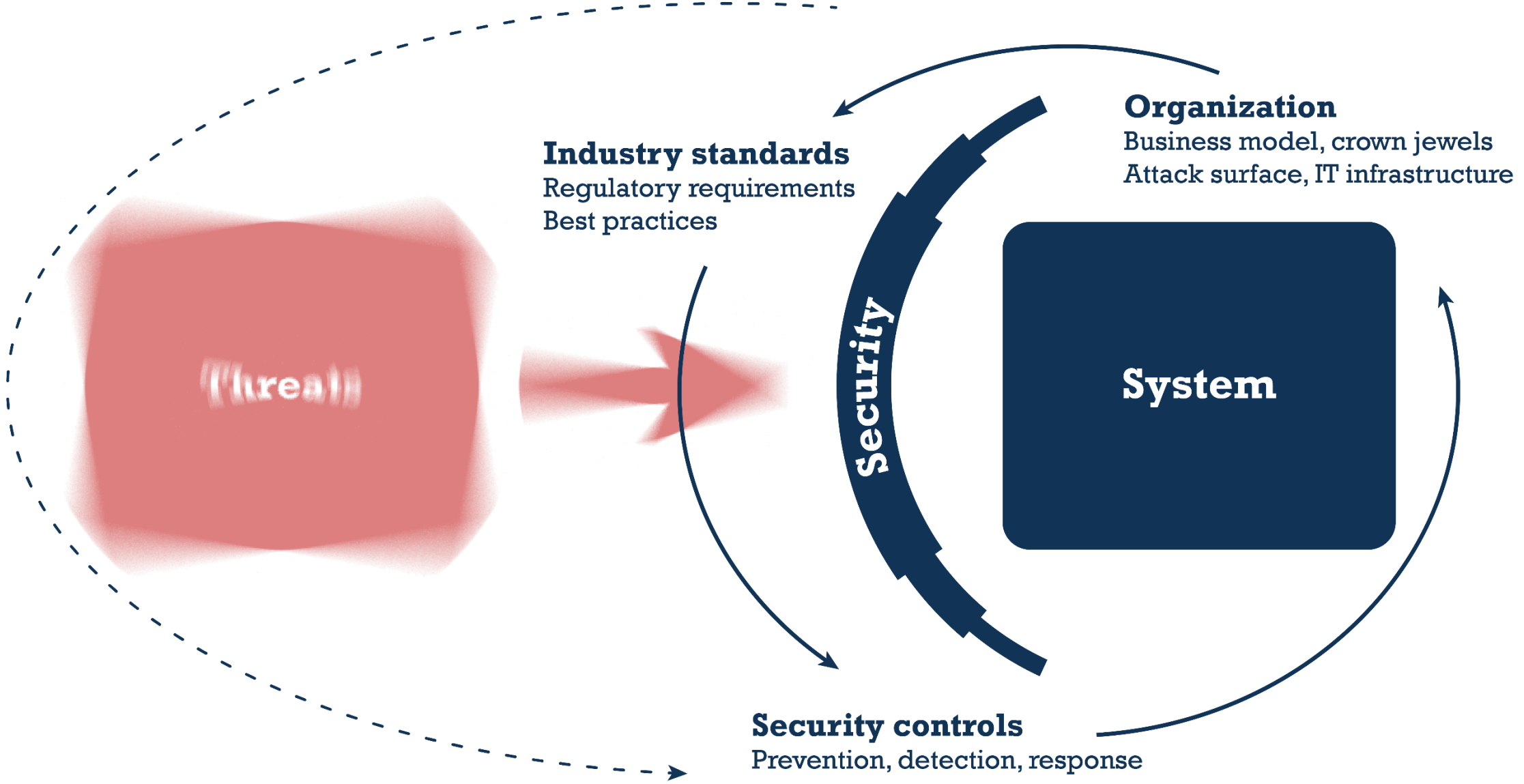
- Security optimization cycle

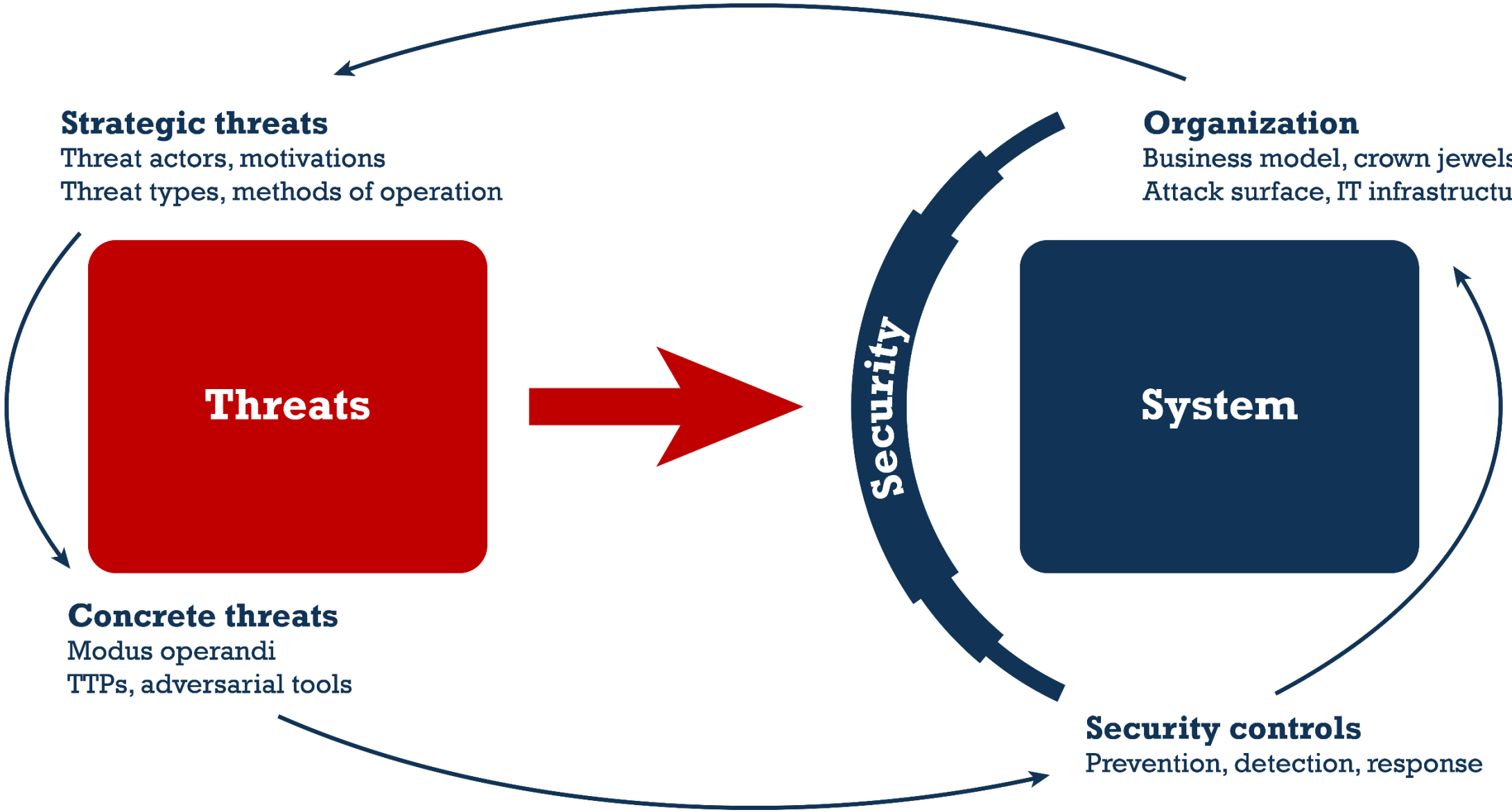
- Prevention
- Response
- Detection

- Conclusion

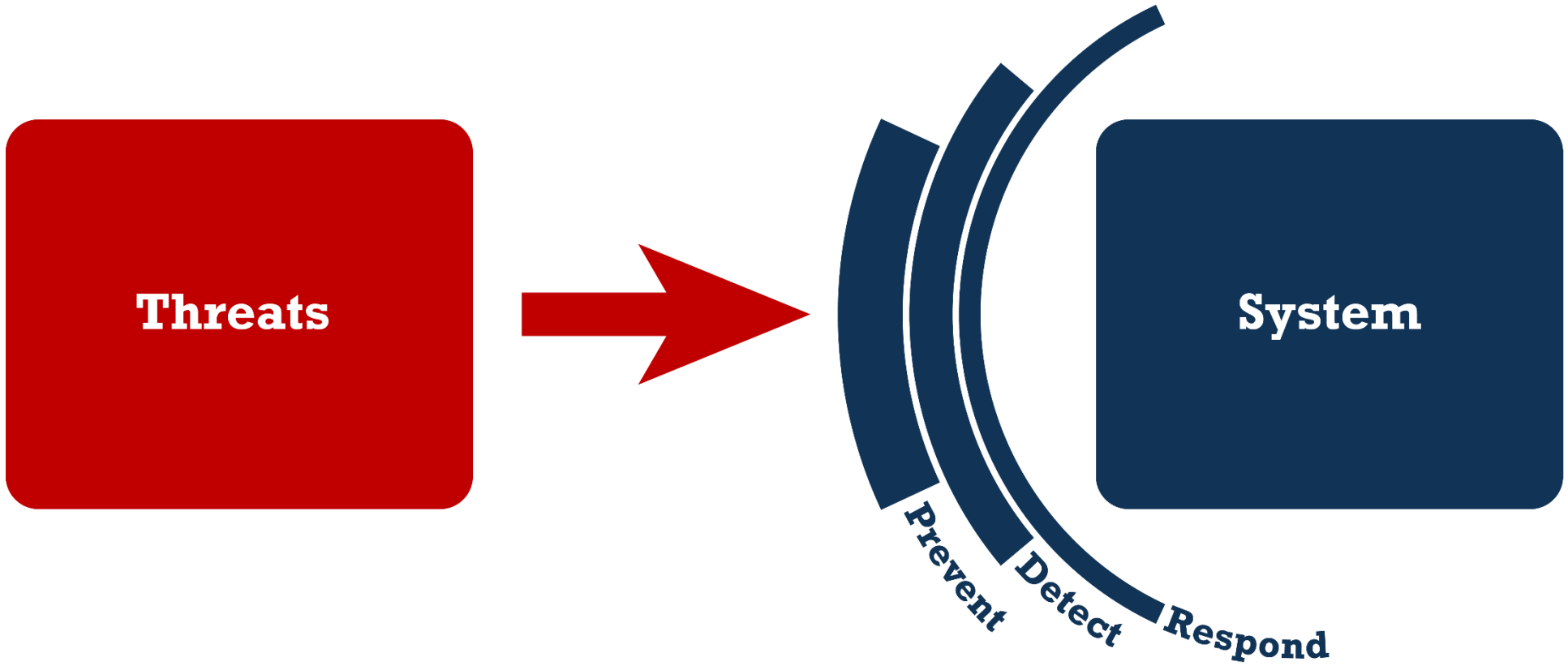


FOX IT
part of nccgroup


Threat
Industry standards
Regulatory requirements
Best practices
Security
Organization
Business model, crown jewels
Attack surface, IT infrastructure
System
Security controls
Prevention, detection, response



FOX IT
part of nccgroup


Threats
Prevent
Detect
Respond
System

» Prevention

- Is important
- Slows down attackers
- But doesn’t stop them if they want to get in

» Keep on preventing

- Prevention is a continuous process, it is never “done”
- What is being protected changes
- The threats it is being protected against change

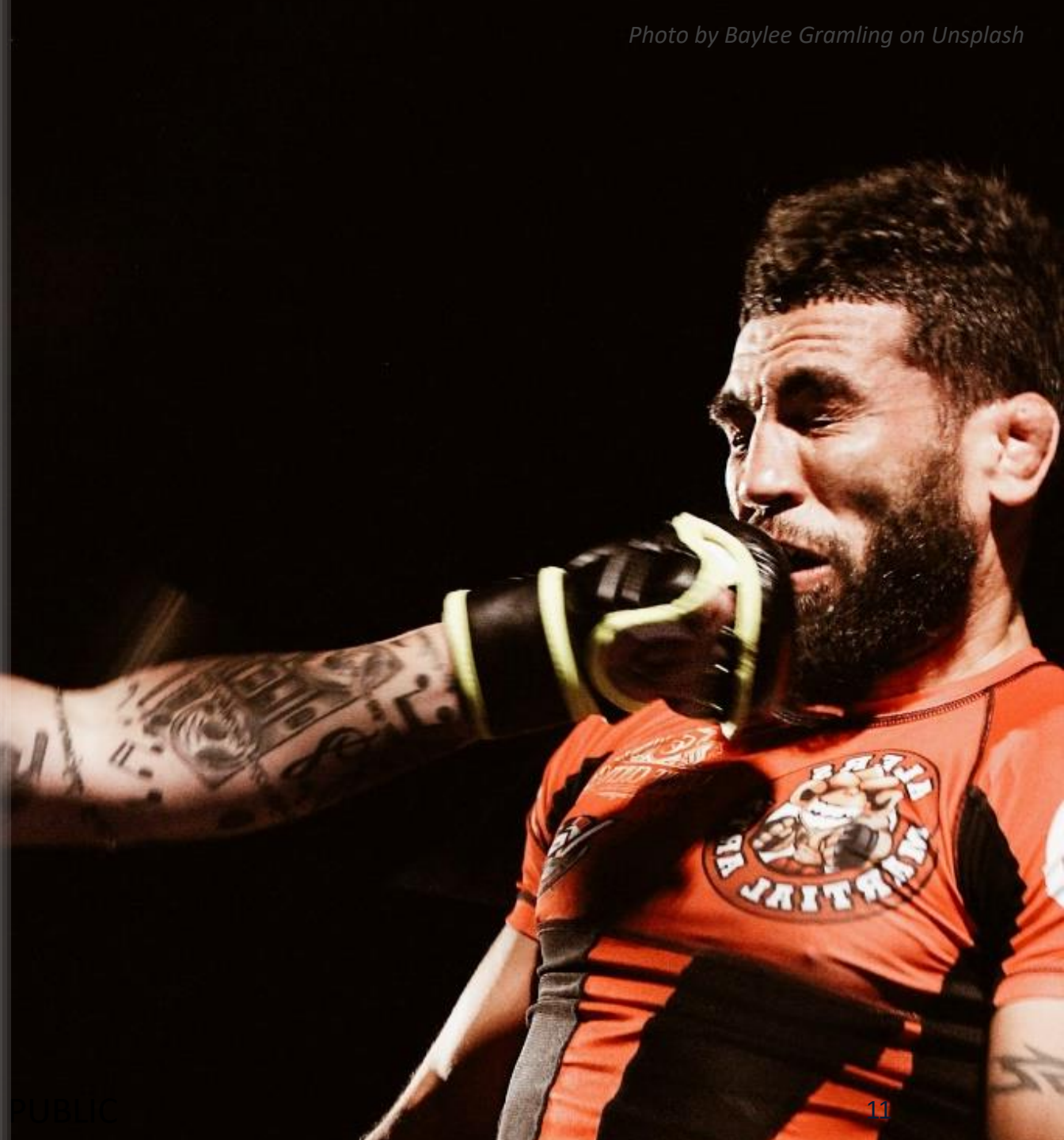
» **Detection**
  - See attackers
  - Even when already breached
  - Enable you to respond rapidly
  - Minimize impact of attacks

» That is why **detection** is now a **standard part** of most defensive strategies

» But detection out-of-the-box is generally not very effective or efficient

Photo by Henry & Co. on Unsplash

- **Response**
  - Respond to problems
  - Attacks, vulnerabilities
  - Act fast
    Limit blast radius
    Minimize impact of attacks
- **Resilience**
  - Proactive response,
    prepare for what could go wrong
- **Multilevel resilience**
  - It’s not IT, it’s the “business”
  - From technical operations
    to management and Board
  - Exercise at all levels
    Make it real, use scenarios



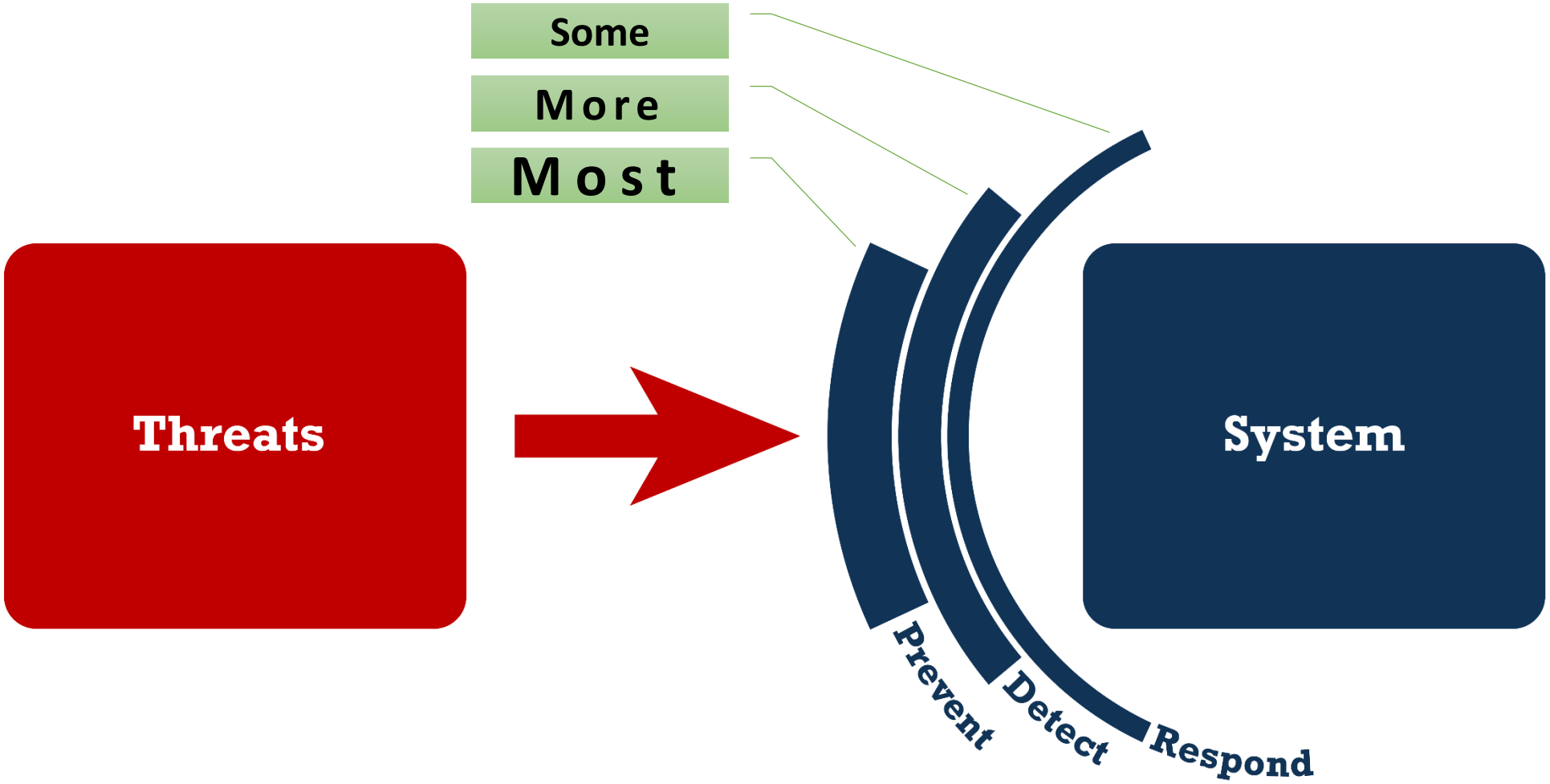
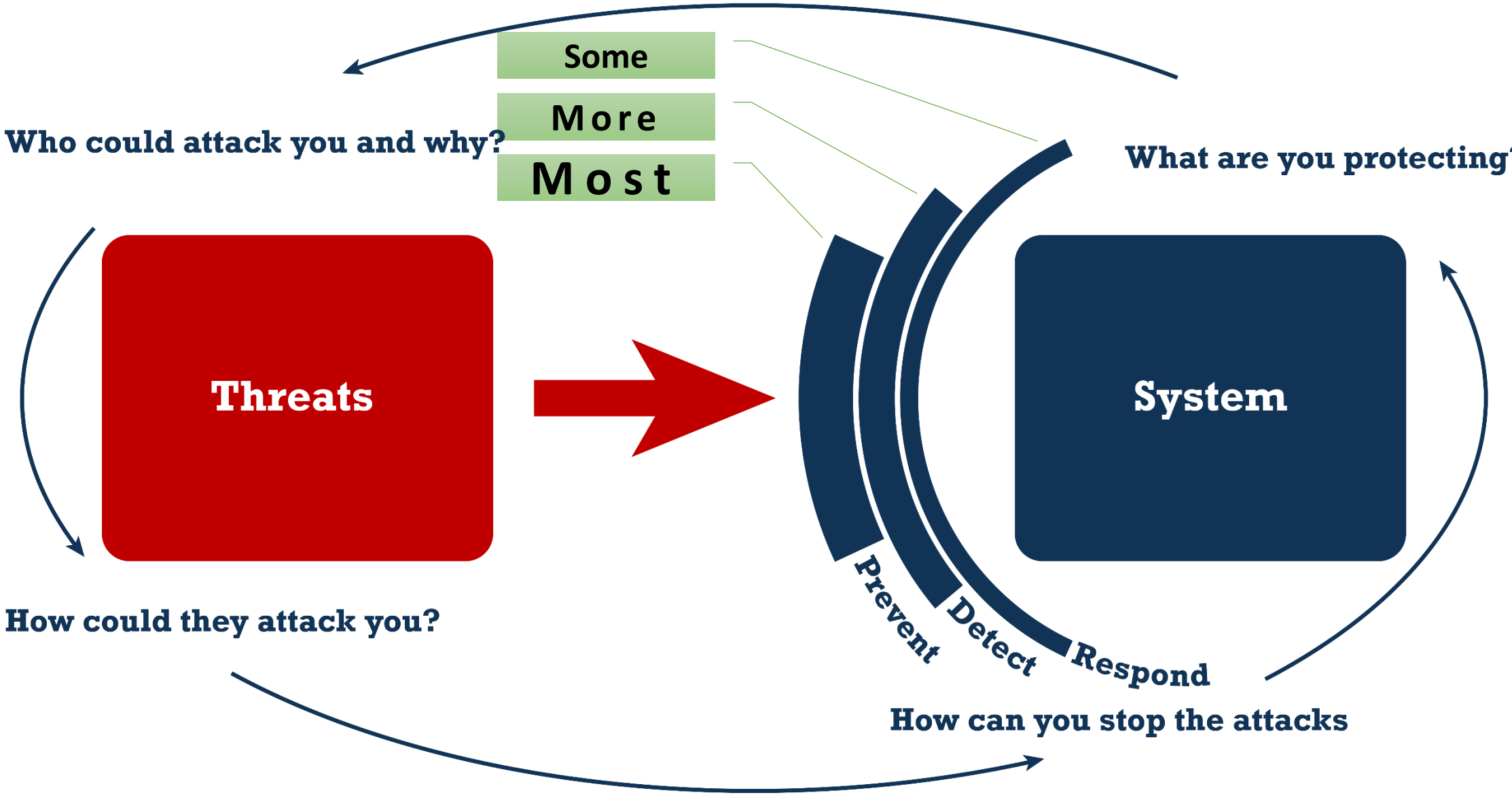
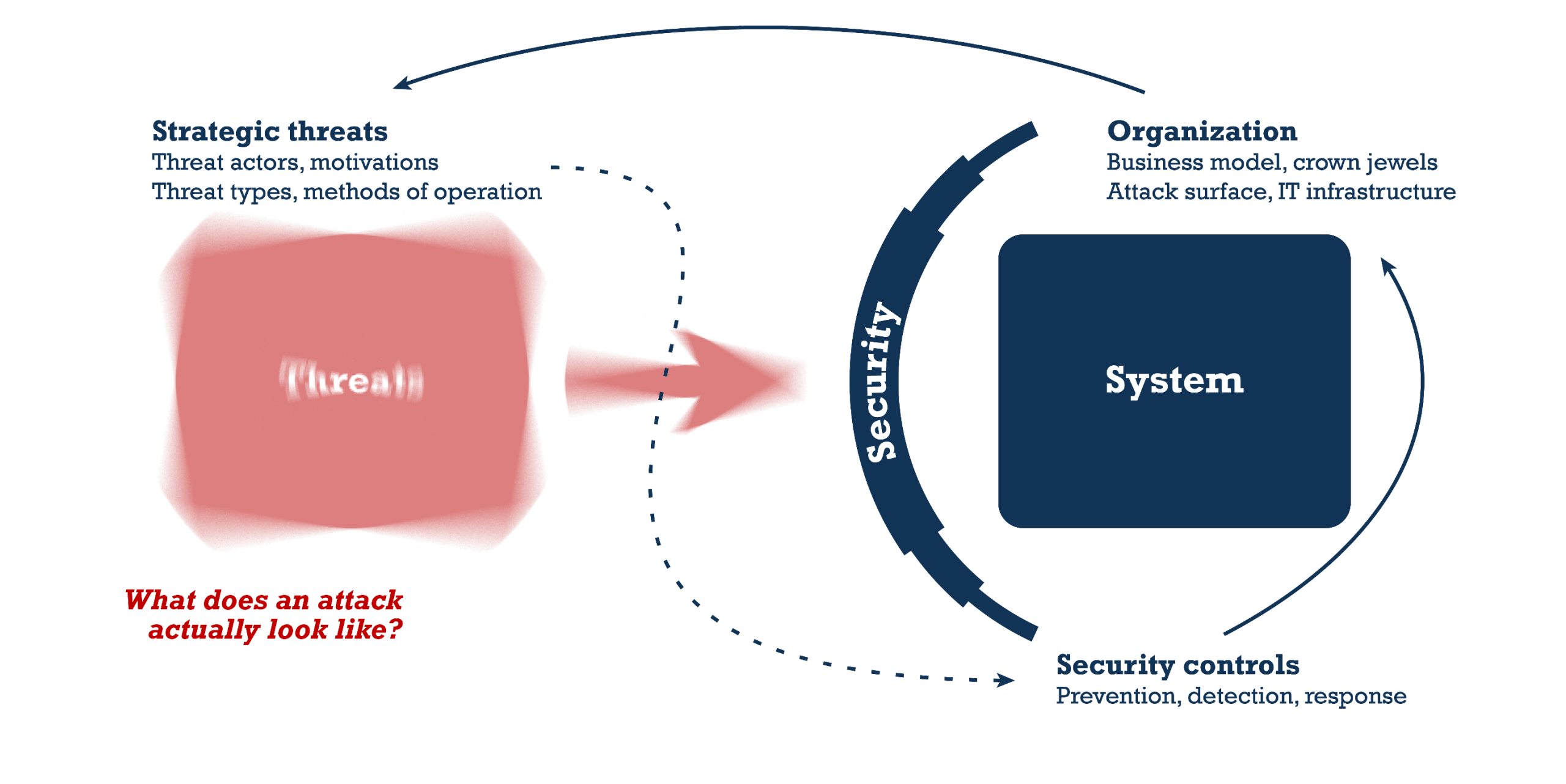

Some
More
Most
Threats
System
Prevent
Detect
Respond

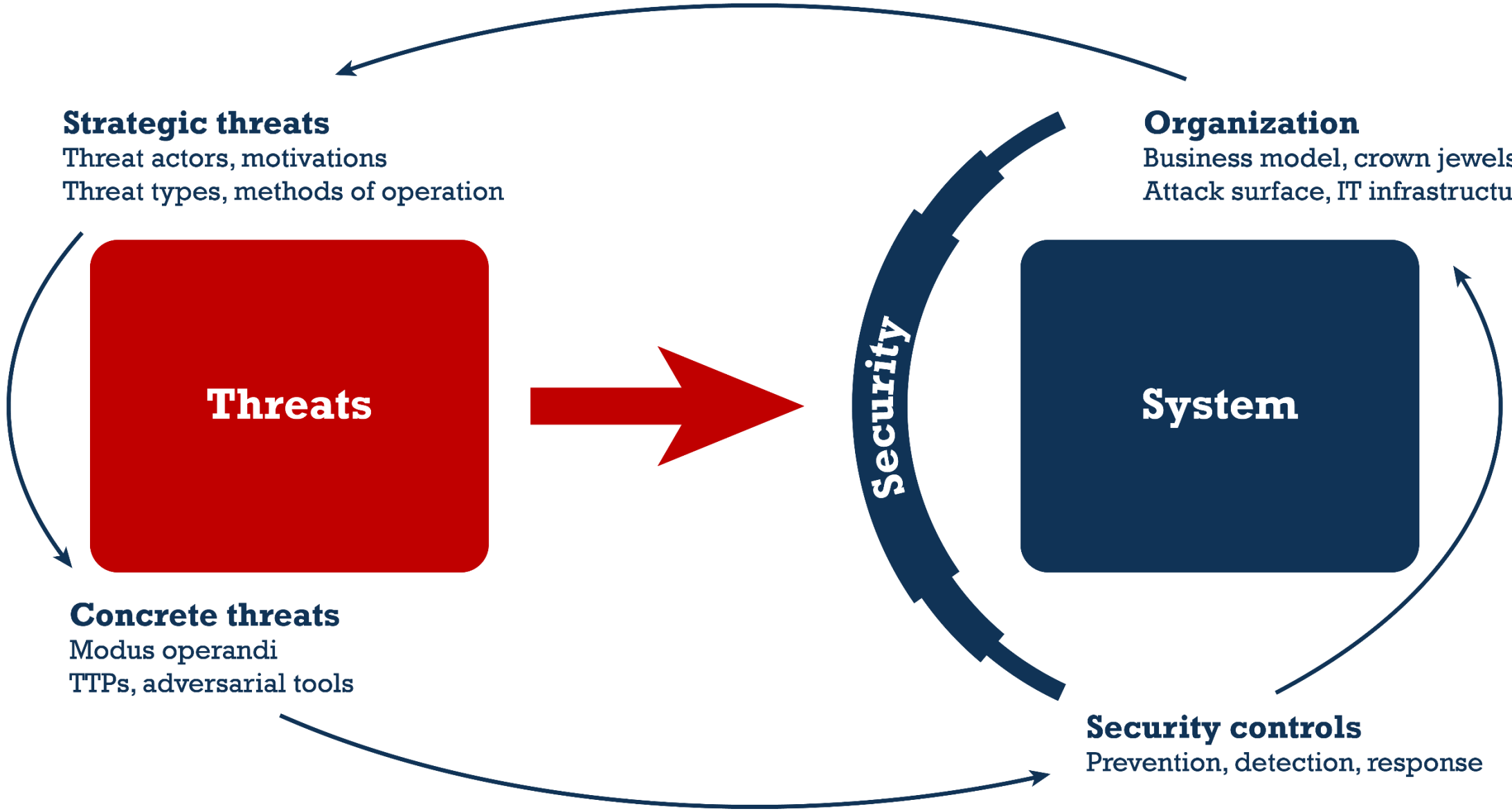

Photo by Marcus Woodbridge on Unsplash

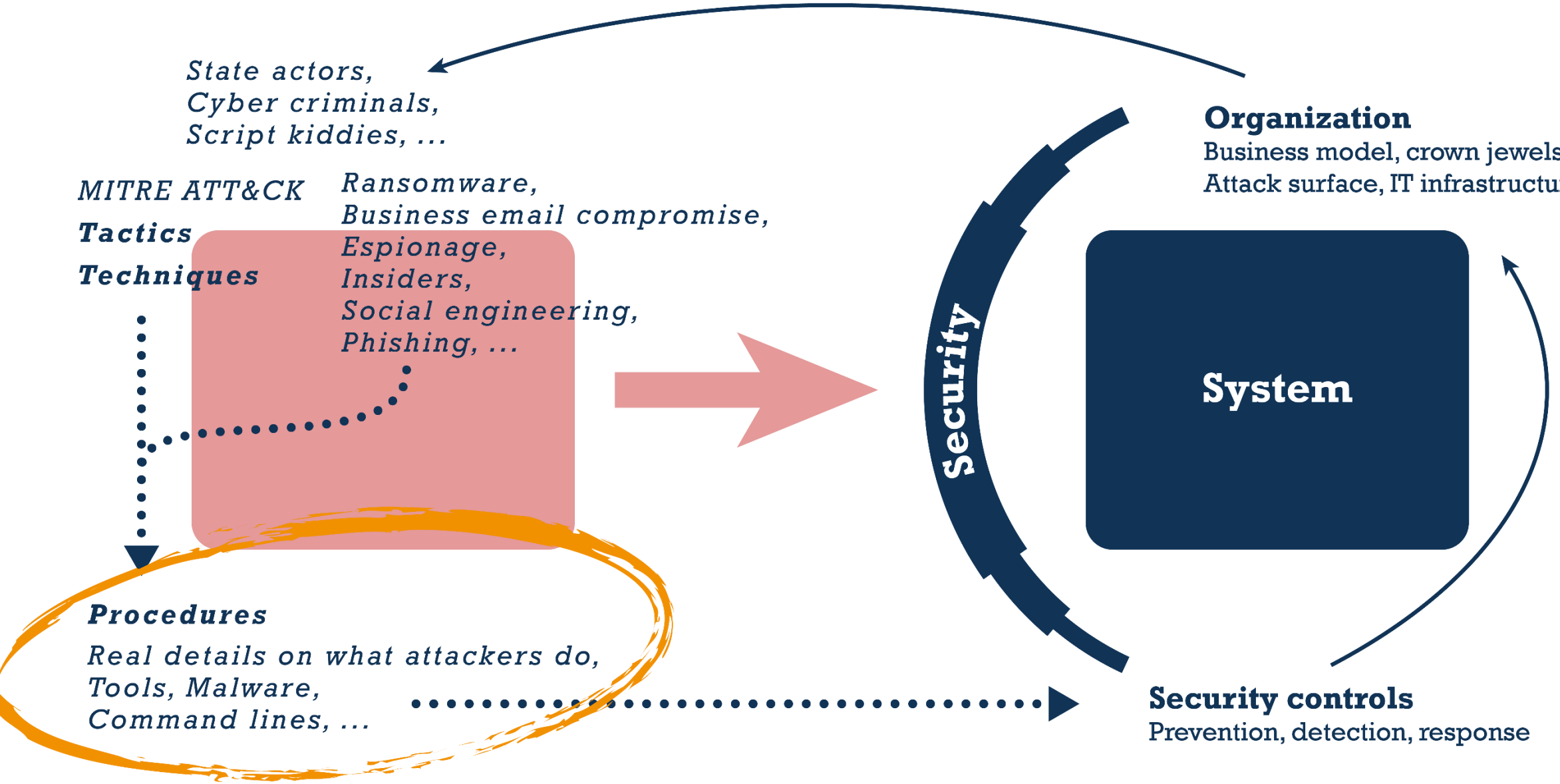


Threats?
Which threats?

FOX IT
part of nccgroup


Strategic threats
Threat actors, motivations
Threat types, methods of operation
Threat
What does an attack actually look like?
Security
Organization
Business model, crown jewels
Attack surface, IT infrastructure
System
Security controls
Prevention, detection, response


Strategic threats
Threat actors, motivations
Threat types, methods of operation
Organization
Business model, crown jewels
Attack surface, IT infrastructure
Threats
Security
System
Concrete threats
Modus operandi
TTPs, adversarial tools
Security controls
Prevention, detection, response


State actors,
Cyber criminals,
Script kiddies, ...
MITRE ATT&CK
Tactics
Techniques
Ransomware,
Business email compromise,
Espionage,
Insiders,
Social engineering,
Phishing, ...
Procedures
Real details on what attackers do,
Tools, Malware,
Command lines, ...
Security
Organization
Business model, crown jewels
Attack surface, IT infrastructure
System
Security controls
Prevention, detection, response

MITRE ATT&CK: Pros and Cons

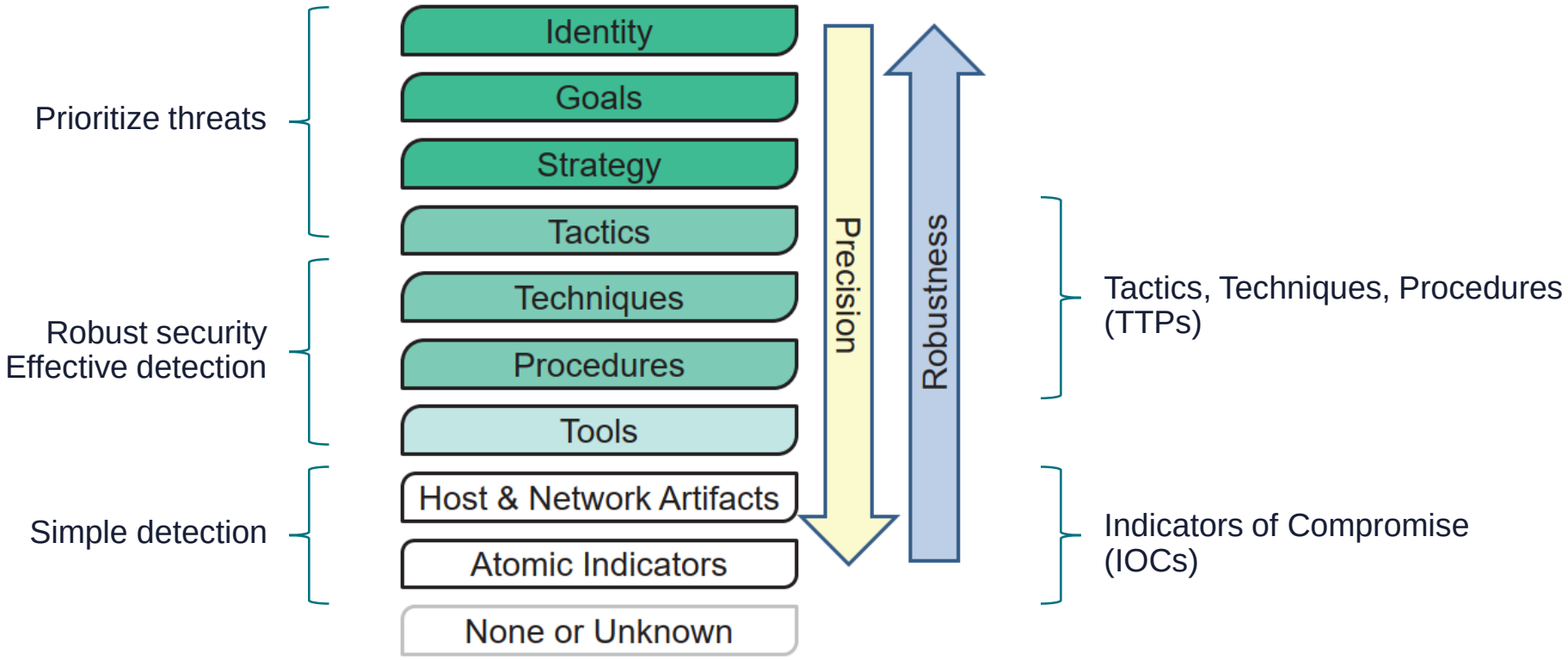
MITRE ATT&CK is **very useful**:

- Give structure to the complex threat landscape
- Provide a common vocabulary for communicating adversarial behavior
- Contain background information on adversaries and their TTPs

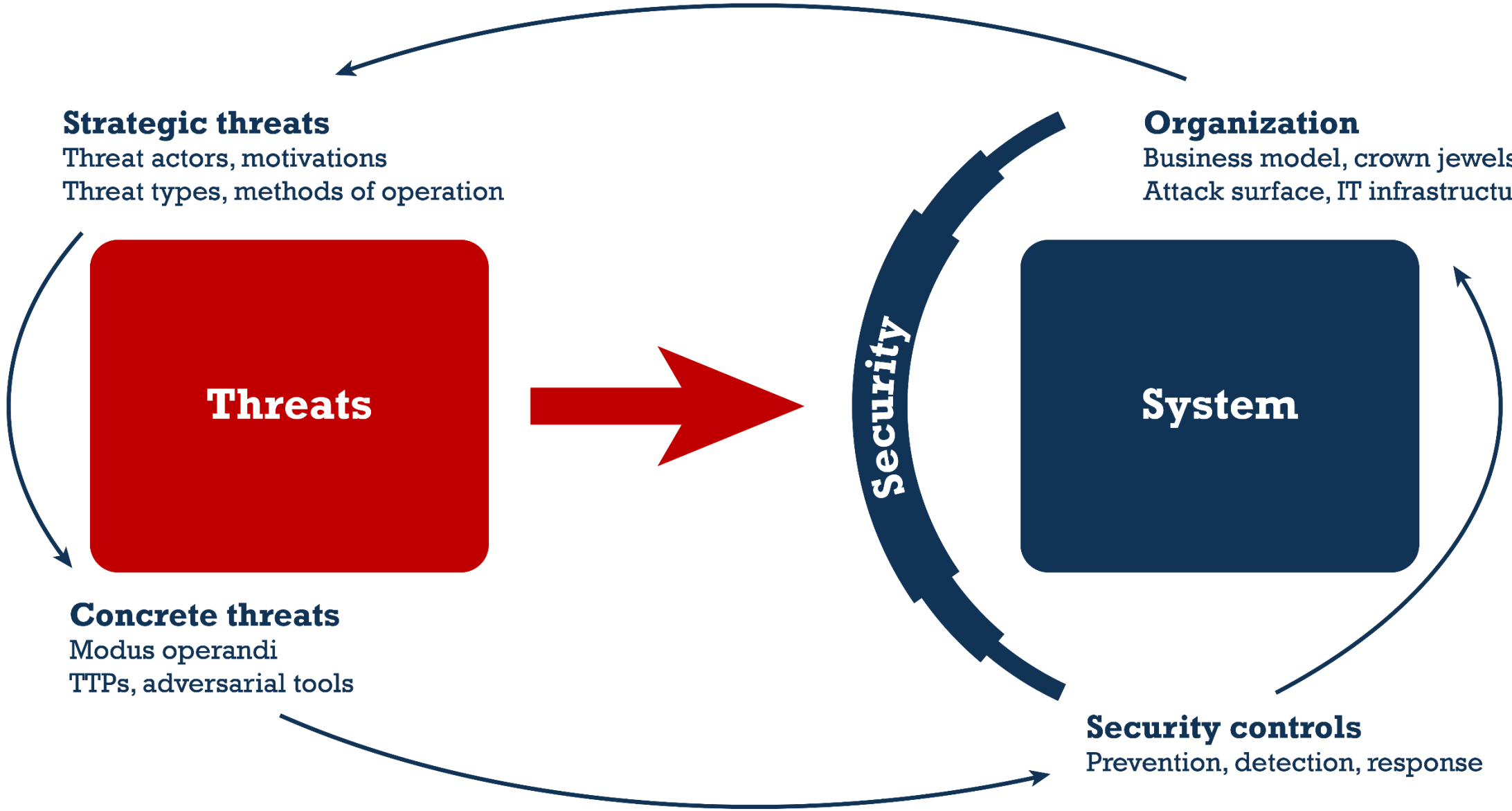
However, it is **not leading**:

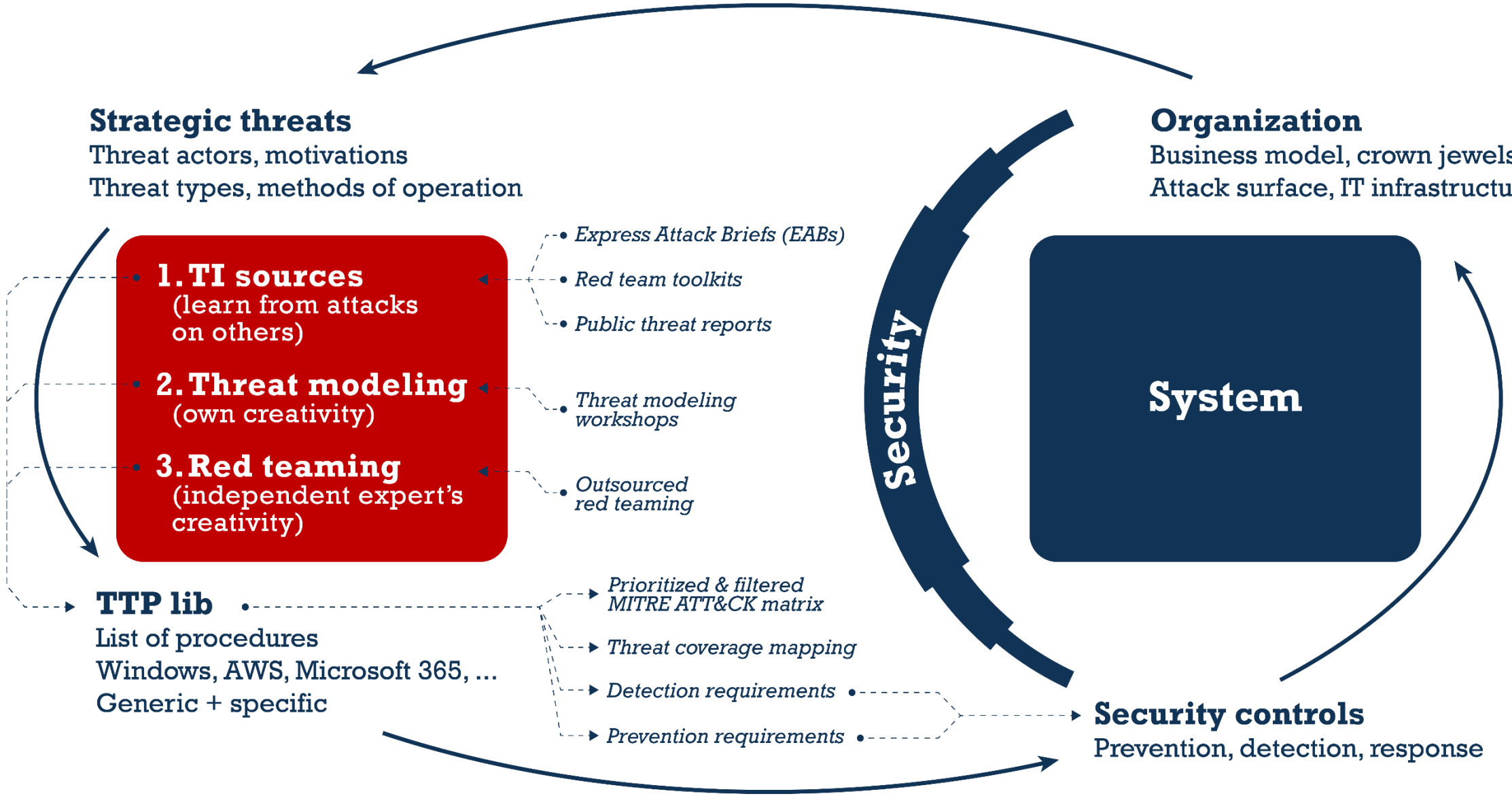
- Trail far behind the state-of-the-art (many months, sometimes years)
- Can give a false sense of security (“coverage” of a technique)
- Are of limited use in prioritizing actual relevance of threats

Threat Intelligence Levels



Semantic Cyberthreat Modelling
by Siri Bromander, A. Jøsang, Martin Eian, 2016


Strategic threats
Threat actors, motivations
Threat types, methods of operation
Organization
Business model, crown jewels
Attack surface, IT infrastructure
Threats
Security
System
Concrete threats
Modus operandi
TTPs, adversarial tools
Security controls
Prevention, detection, response


Strategic threats
Threat actors, motivations
Threat types, methods of operation
1. TI sources
(learn from attacks on others)
2. Threat modeling
(own creativity)
3. Red teaming
(independent expert's creativity)
Express Attack Briefs (EABs)
Red team toolkits
Public threat reports
Threat modeling workshops
Outsourced red teaming
TTP lib
List of procedures
Windows, AWS, Microsoft 365, ...
Generic + specific
Prioritized & filtered MITRE ATT&CK matrix
Threat coverage mapping
Detection requirements
Prevention requirements
Security
Organization
Business model, crown jewels
Attack surface, IT infrastructure
System
Security controls
Prevention, detection, response

Technical threat assessments

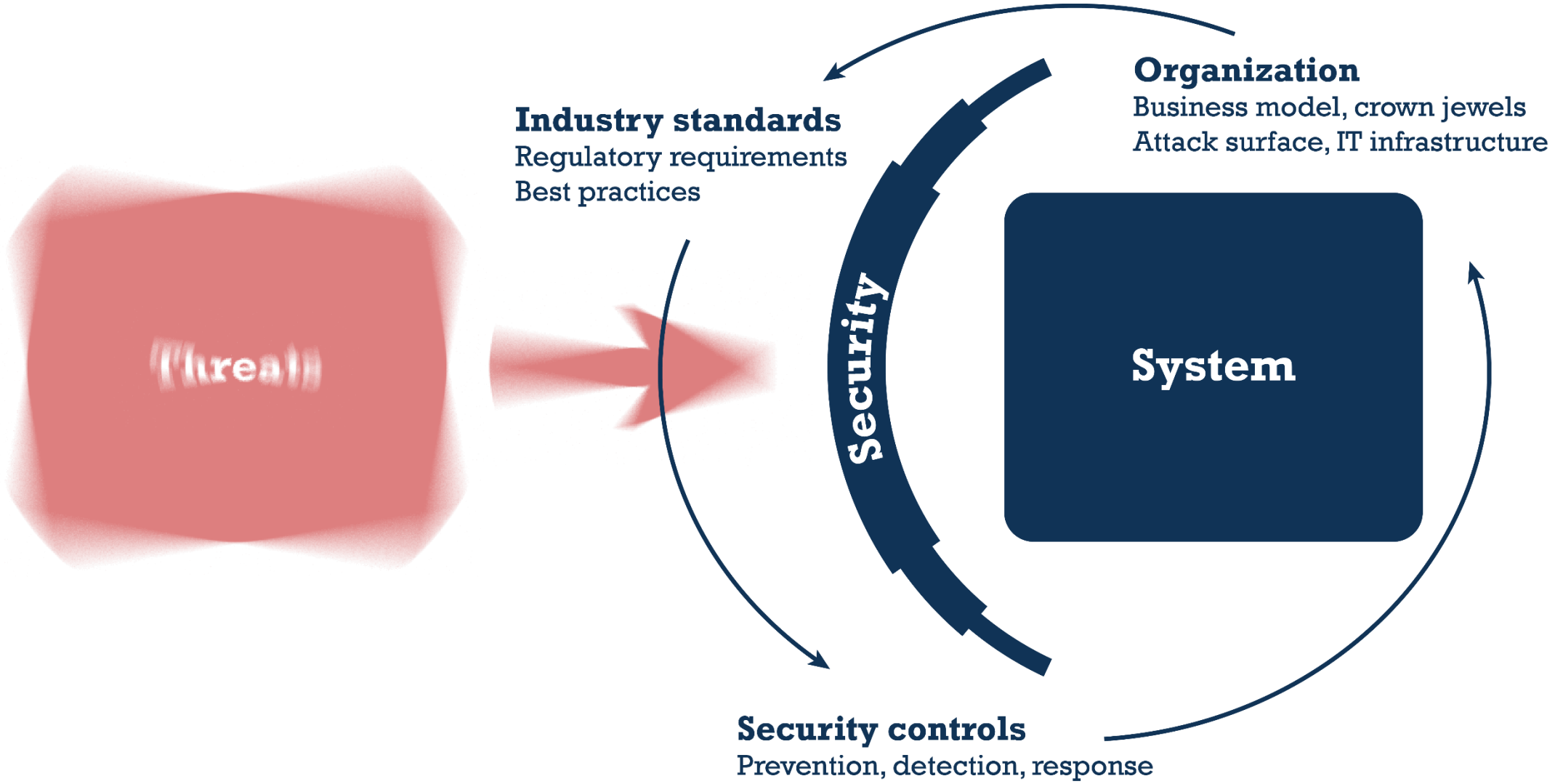
IT environment	Generic	Specific
Enterprise Windows	●	◔
Office 365	●	◔
Cloud SaaS	○	●
Cloud IaaS (AWS, Azure)	◔	◕
Linux servers	◕	◔

Generic TTPs
Incident Response cases, Red Teaming, partner communities, public threat reports

Specific TTPs
Threat modeling workshops, Red Teaming

Prevention

FOX IT
part of nccgroup


Threat
Industry standards
Regulatory requirements
Best practices
Organization
Business model, crown jewels
Attack surface, IT infrastructure
Security
System
Security controls
Prevention, detection, response

CIS Controls™

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.

CIS Controls V7 separates the controls into three distinct categories:

Basic:
Key controls which should be implemented in every organization for essential cyber defense readiness.

Foundational:
Technical best practices provide clear security benefits and are a smart move for any organization to implement.

Organizational:
These controls are more focused on people and processes involved in cybersecurity.

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

> "Start by taking care of the basics: build a solid cybersecurity foundation by implementing the [CIS Controls], especially application white-listing, standard secure configurations, reduction of administrative privileges and a quick patching process."

Zurich Insurance Group
Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures
Switzerland


Photo by Annie Spratt on Unsplash

Response

FOX IT
part of nccgroup

Overview of response-related documentation

Information Security Policy: Overview of information security risks, and guidelines of security controls (availability, confidentiality, integrity)

- Information security goals
- Scope
- Roles and responsibilities
- Compliance | regulation
- Timeline
- Working from home
- Mobile device policy
- Enforcement
- User training
- Contacts
- Passwords/MFA
- Segmentation
- Asset management
- Backup & herstel van IT
- Physical security
- Identity & access management
- Incident response
- Patch Management
- Network security
- Internet usage & Social media

Incident Response Plan: Defines the process of detection, triage, analysis, escalation and follow-up

- Who performs the (technical security) monitoring
- Where do alerts come from
- Who analyzes these alerts
- How is the (potential) impact determined (impact and escalation criteria)
- Who will be informed
- Who is responsible for the follow-up
- When is escalation
- Where does the registration take place

- ***Disaster Recovery Plan / IT Recovery Plan***: Plans and preparation to support a fast IT recovery during a (cyber) crisis
- Detailed description of how to act to restore the affected business process or IT asset as quickly and efficiently as possible.
- To be drawn up by administrator / responsible of the IT
  - RTO = Recovery Time Objective
    - What is the acceptable downtime of the systems?
    - Related to Business Continuity Plan
  - RPO = Recovery Point Objective
    - What is the accepted loss of data?

Crisis Management Plan: Defines who is doing what during a (cyber) crisis

- Escalation criteria: what is an (imminent) crisis, incl. scenarios
- Escalation process & contact details
- Composition of team(s)
- Tasks and responsibilities (by role)
- Communication & Spokesperson
- Rules of thumb and points of attention
- Completion
- Evaluation

Business Continuity Plan: Ensure the business continues during a (cyber) crisis

- Is closely related and dependent on IT recovery!
- Definition of processes & dependent assets.
- Scenarios where assets are unavailable that cause workarounds to be set up.
- Preparations to ensure the implementation of workarounds.
-


Photo by Yulia Matvienko on Unsplash

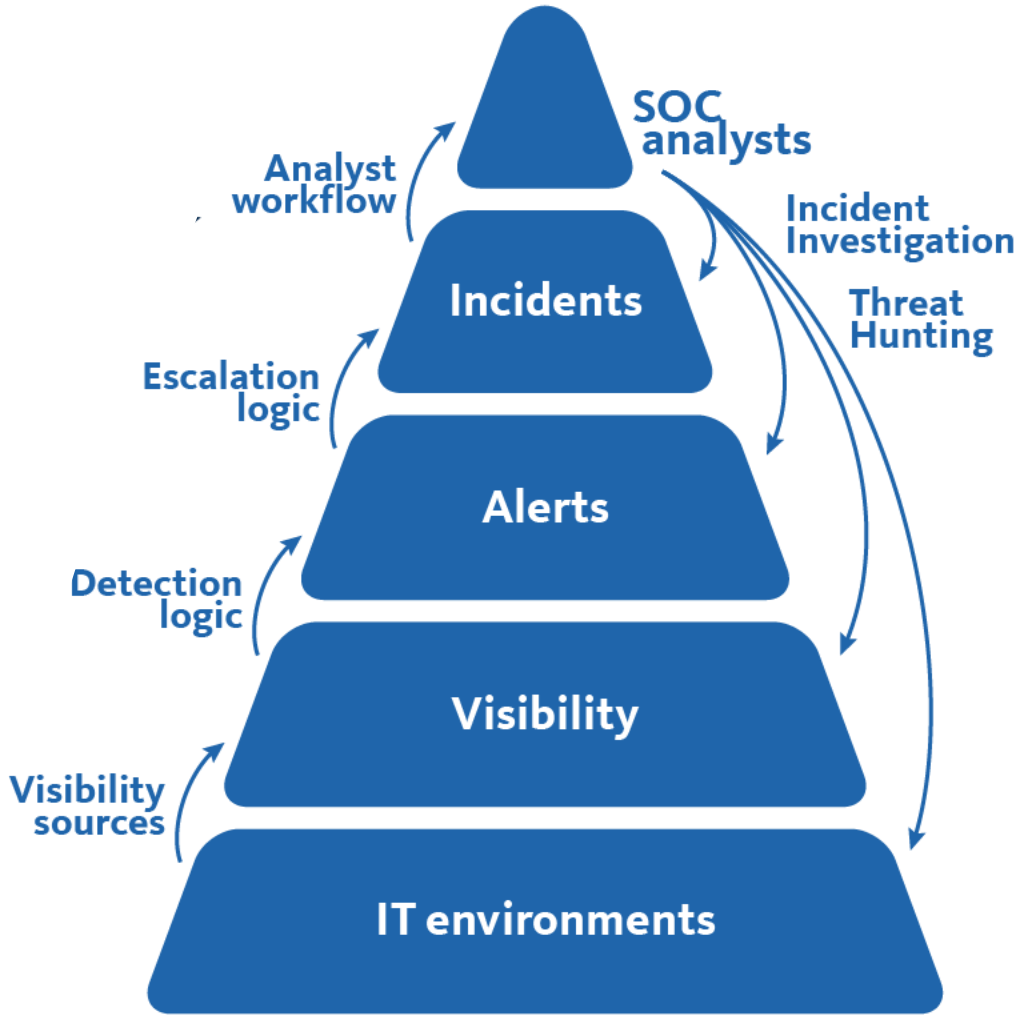

Photo by Alora Griffiths on Unsplash

Detection must be engineered

FOX IT
part of nccgroup

?

Threats


SOC analysts
Analyst workflow
Incident Investigation
Incidents
Threat Hunting
Escalation logic
Alerts
Detection logic
Visibility
Visibility sources
IT environments

» **Not detecting attacks**
- Coverage of IT estate limited
- Visibility with insufficient detail
- Detection outdated

» **Too many alerts**
- High cost
- Alert fatigue
- Unseen true–positives between false–positives

More Detection

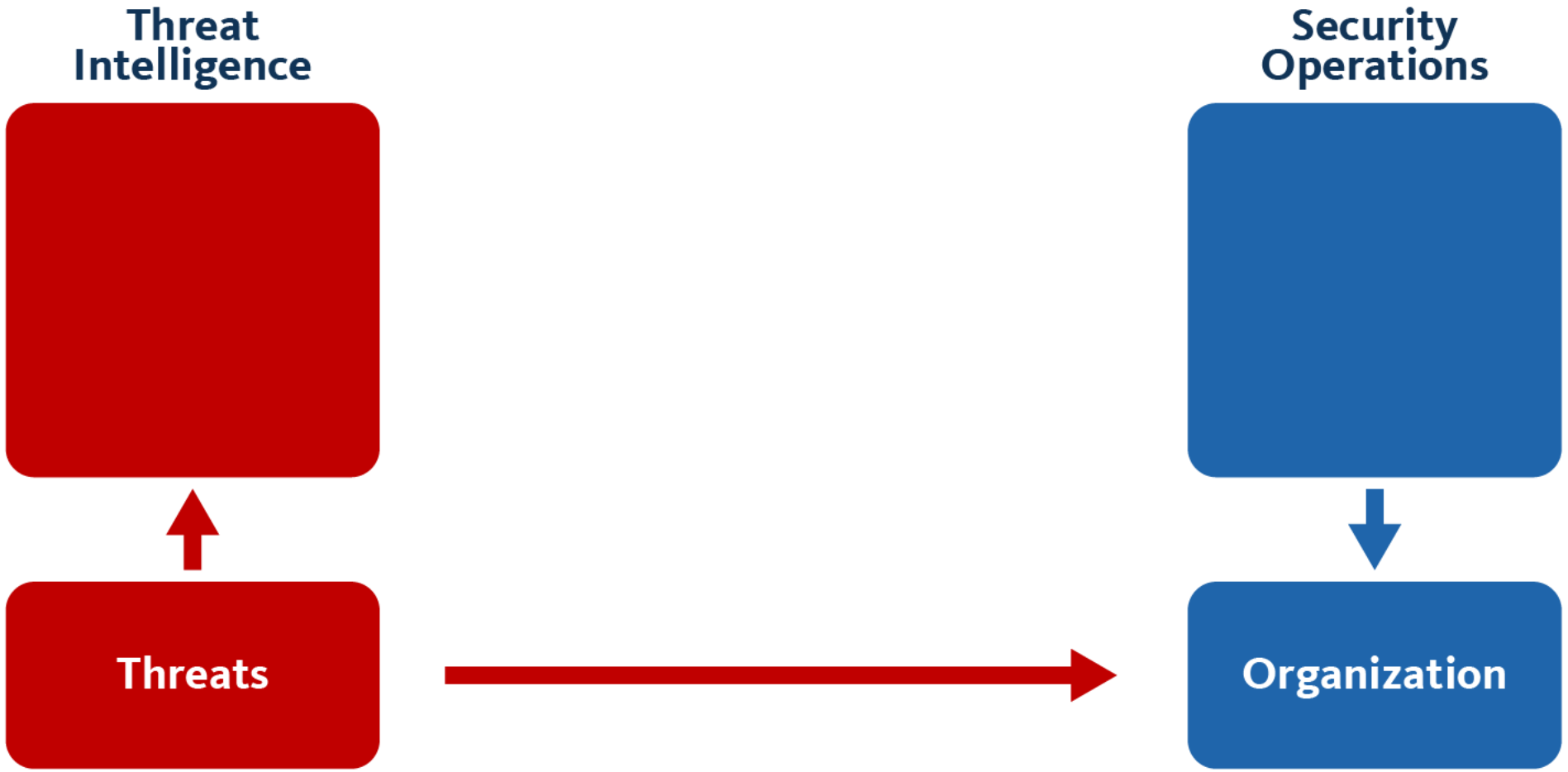
Less Detection

Low Quality

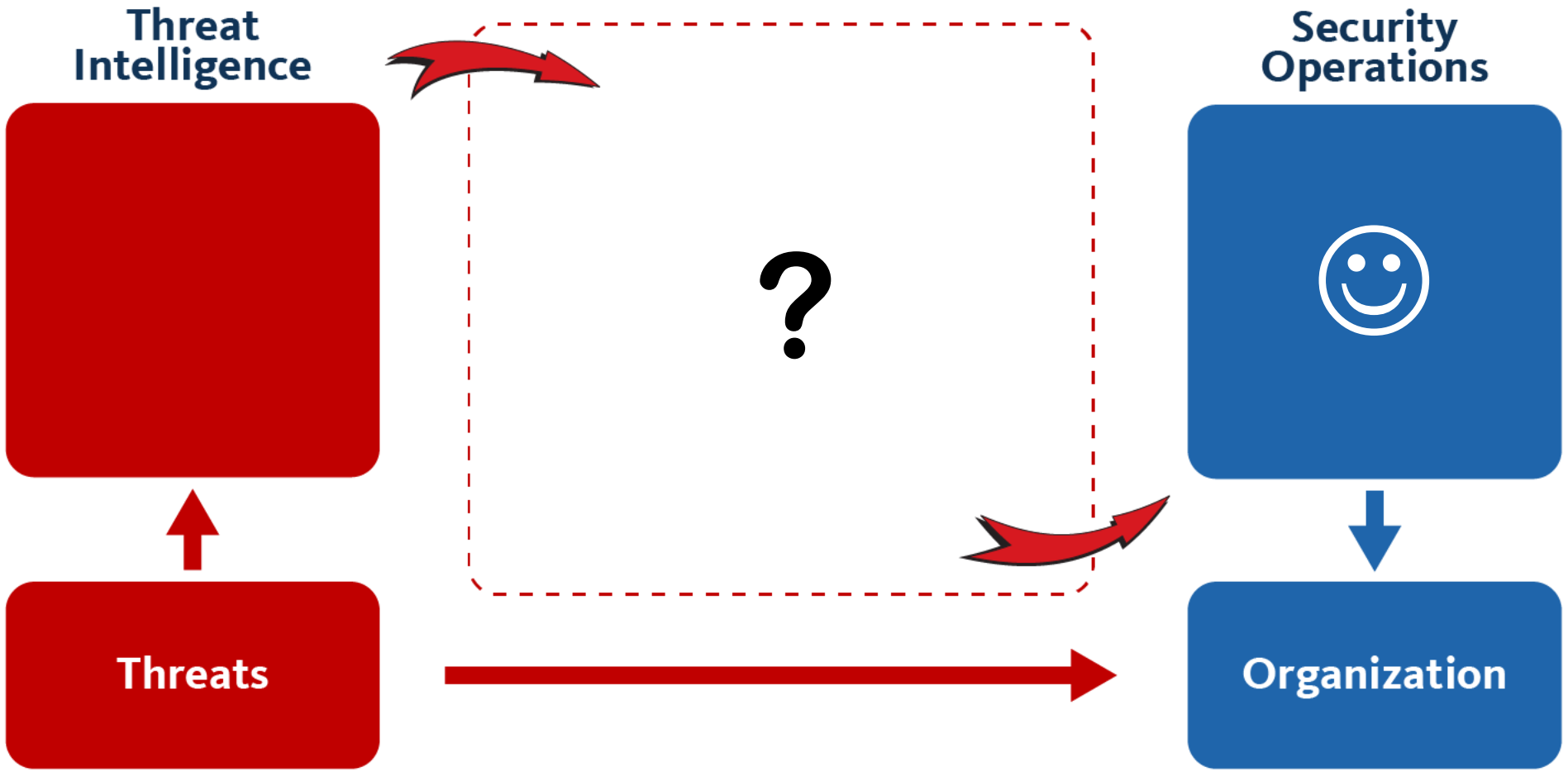
What is Quality?

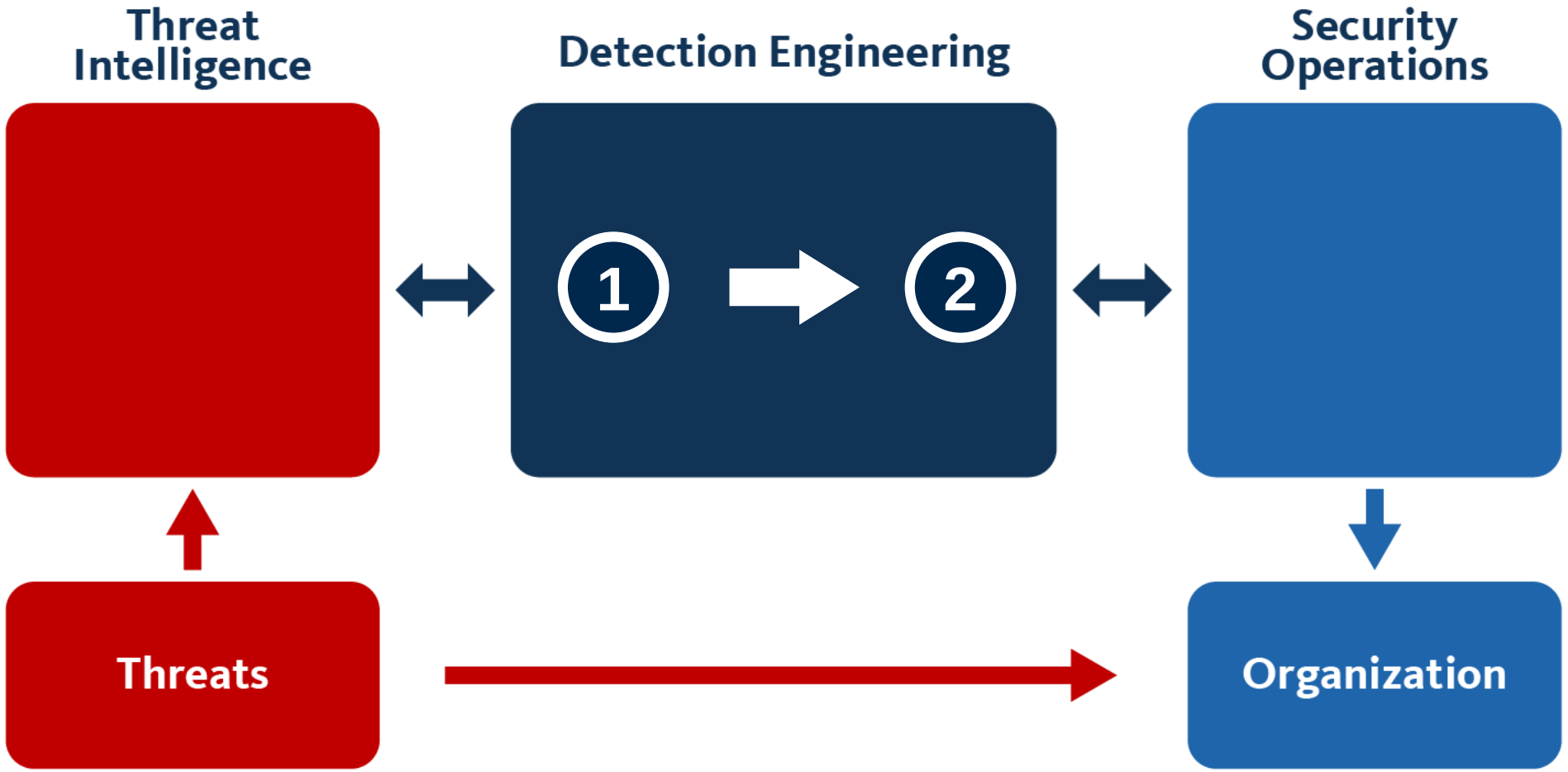
Low Quality

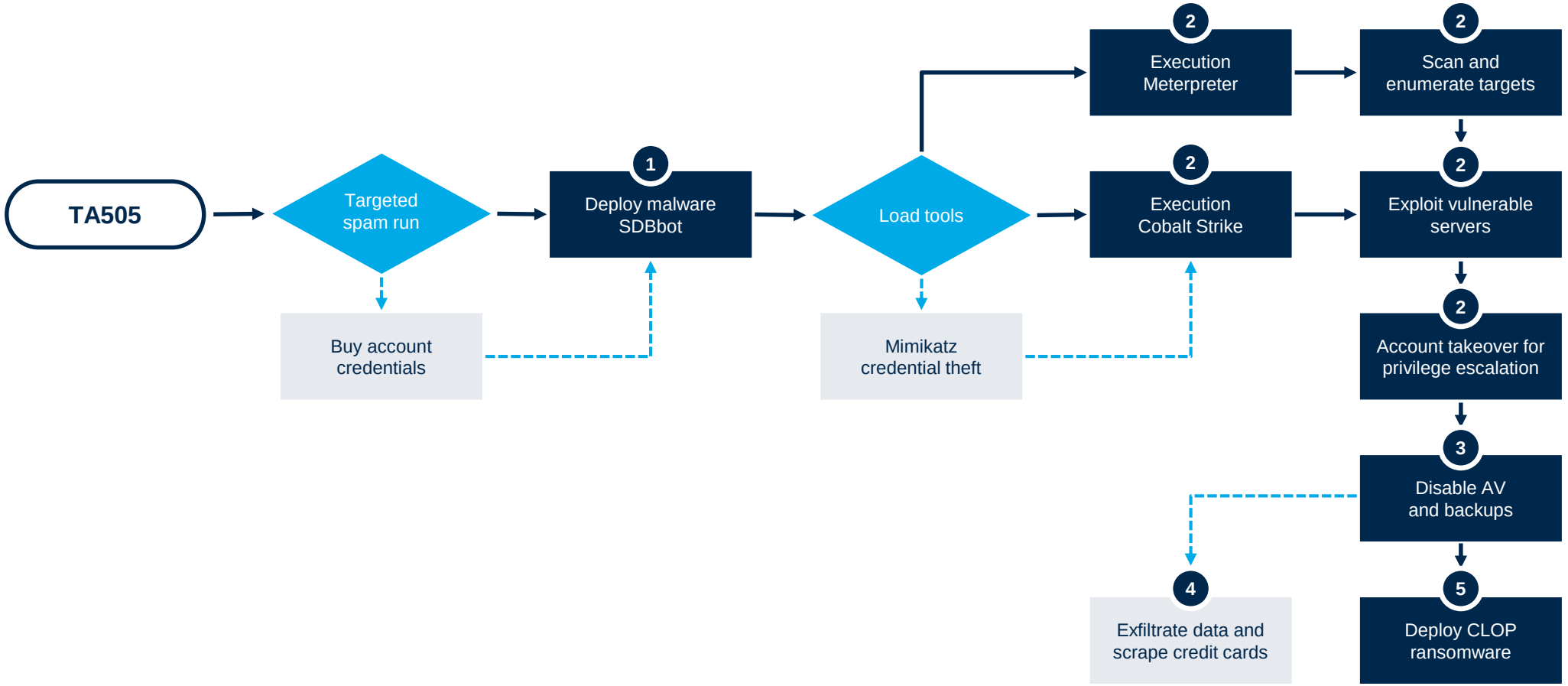
Photo by Eugene Triguba on Unsplash


Threat Intelligence
Security Operations
Threats
Organization

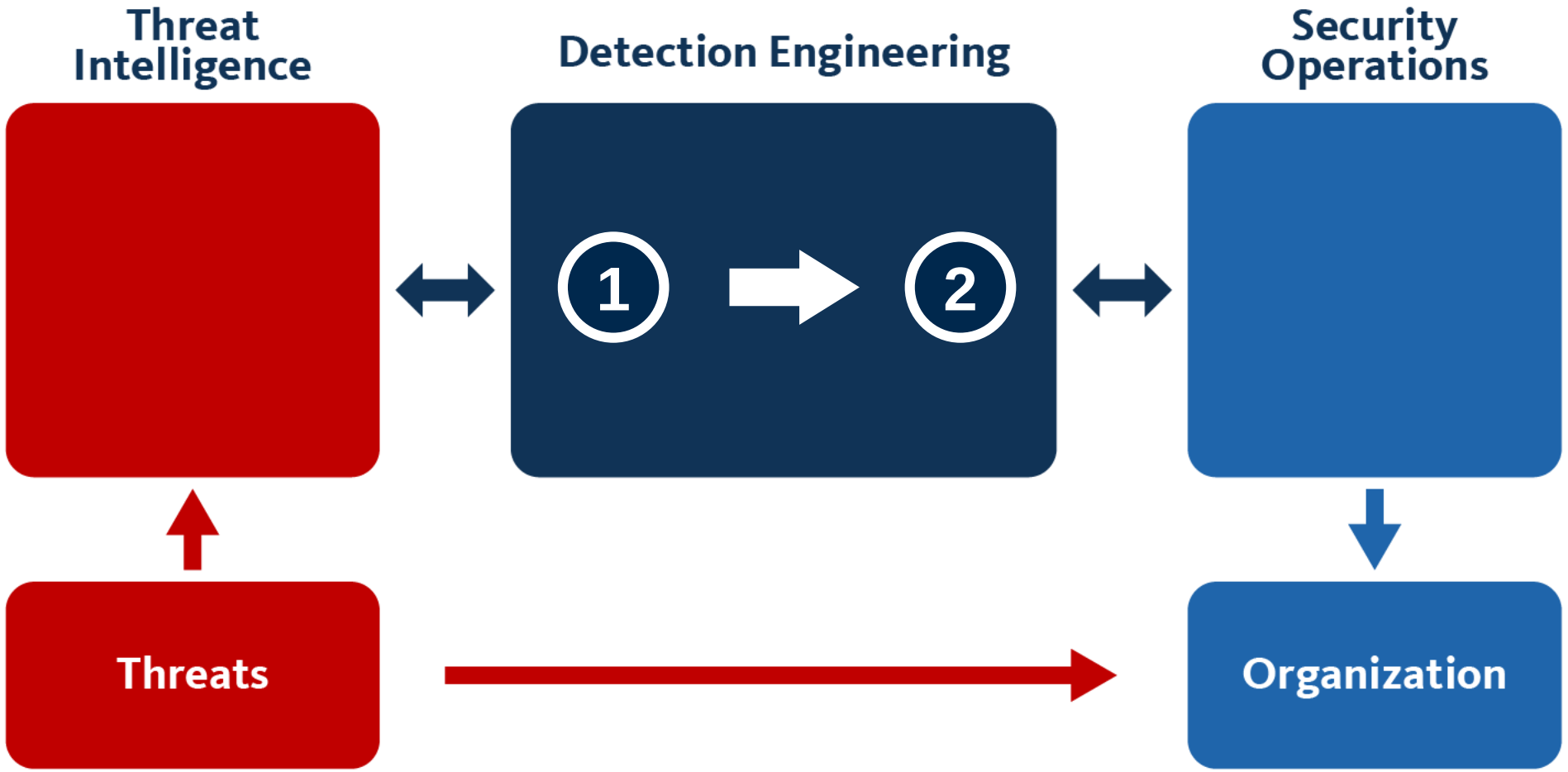
FOX IT part of nccgroup

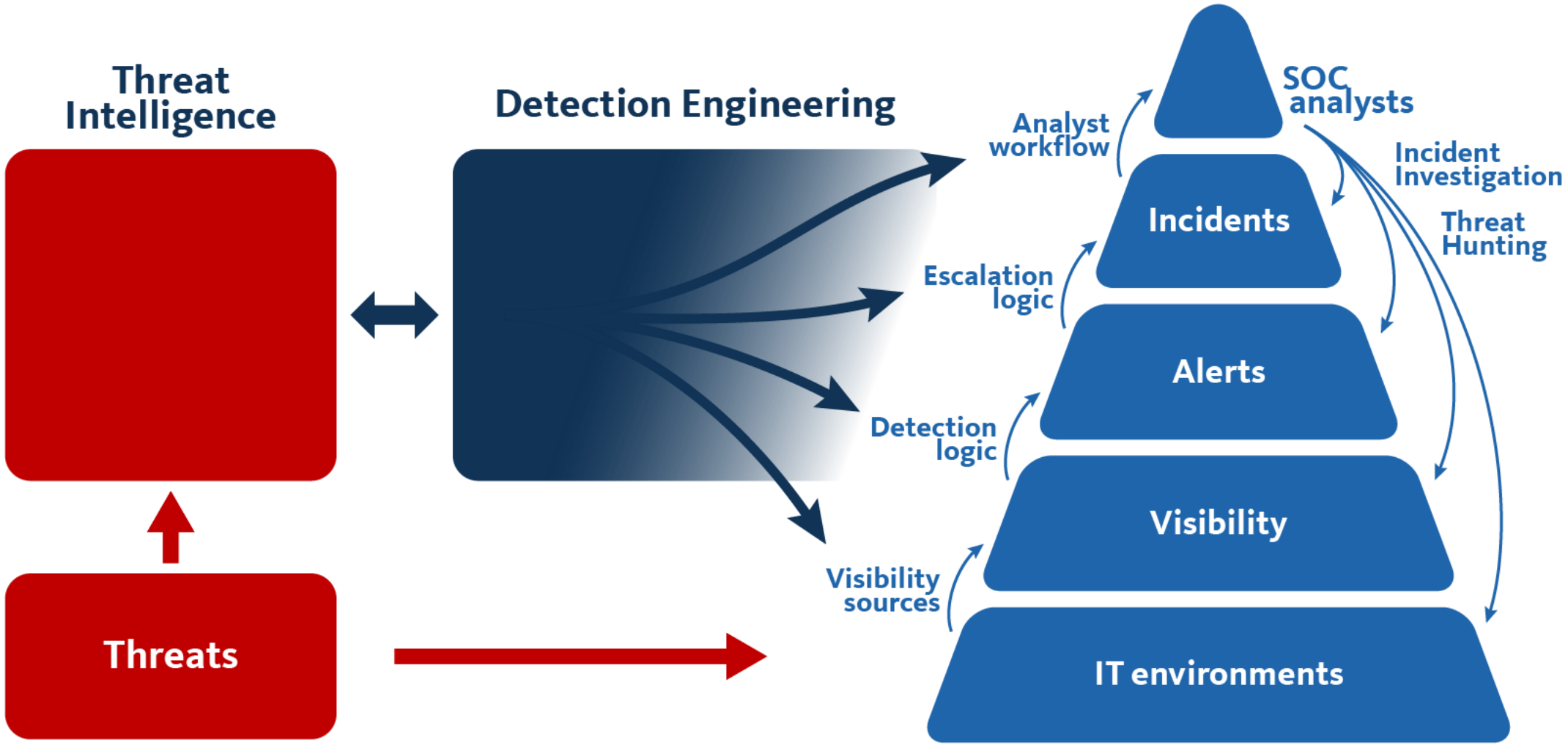

Threat Intelligence
Security Operations
?
Threats
Organization

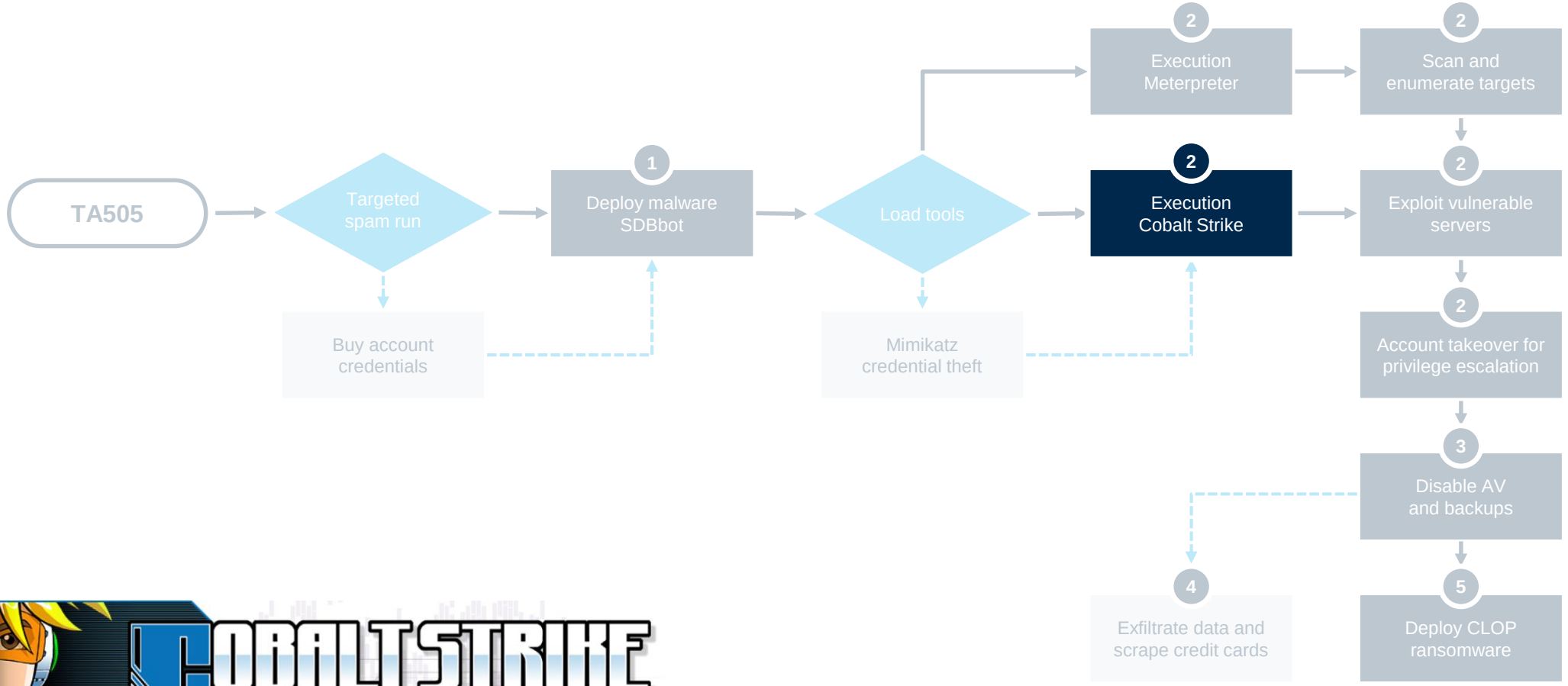

Threat Intelligence
Detection Engineering
Security Operations
1
2
Threats
Organization



FOX IT part of nccgroup


Threat Intelligence
Detection Engineering
Security Operations
1
2
Threats
Organization

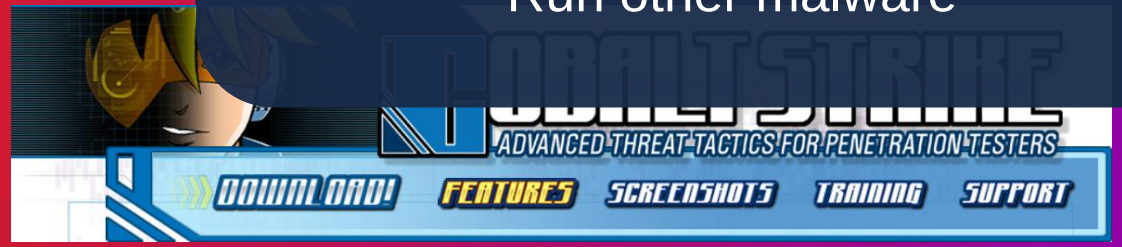

Threat Intelligence
Detection Engineering
Threats
SOC analysts
Analyst workflow
Incident Investigation
Threat Hunting
Incidents
Escalation logic
Alerts
Detection logic
Visibility
Visibility sources
IT environments



https://www.cobaltstrike.com/

› Cobalt Strike
- Commercial software that hackers use to take over target environments
- Used by both legitimate penetration testers and malicious actors, including APTs

› Feature rich
- Take screenshots, log keystrokes
- Lateral movement
- Run other malware



https://www.cobaltstrike.com/

› Create lab environment
- Realistic enough to test relevant Cobalt Strike features
- Separate lab or in actual environment

› Run attack scenario
- Emulate adversarial usage
- Use features, e.g. privilege escalation, persistence, lateral movement

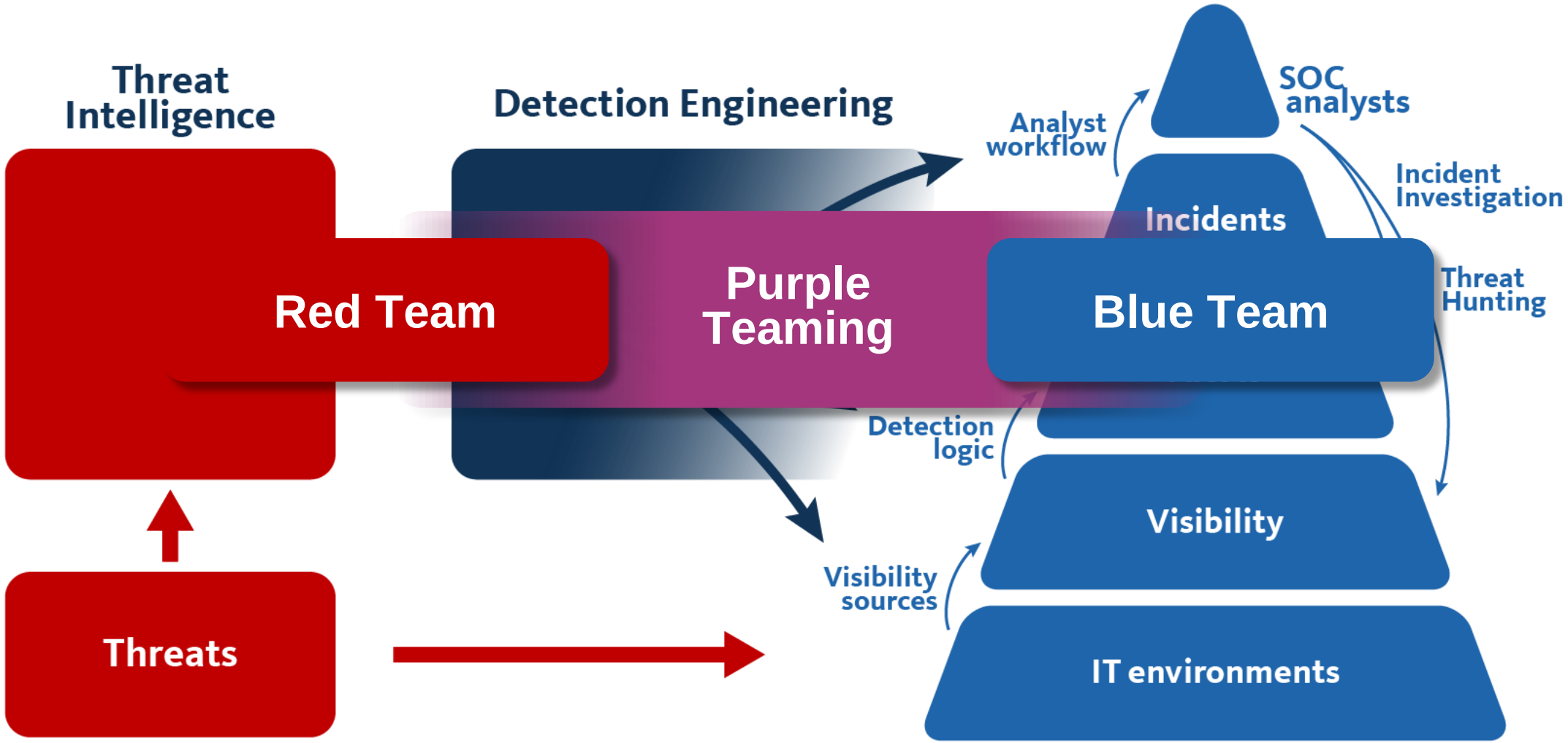
https://www.cobaltstrike.com/

› Determine what your current security setup blocks / detects

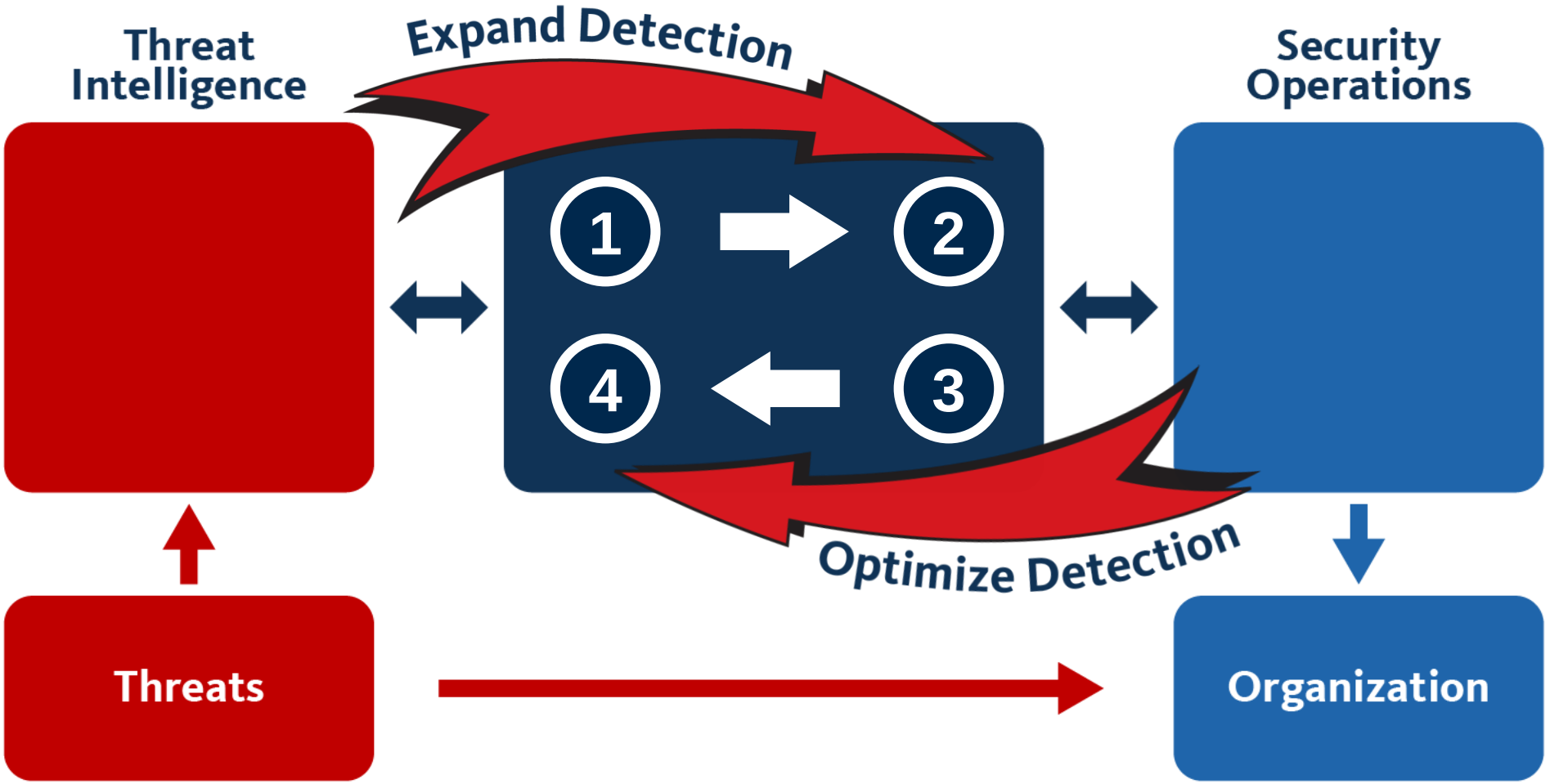
› Identify detection gaps

› Prioritize detection development
- Better tools
- Better detection logic

https://www.cobaltstrike.com/



FOX IT part of nccgroup


Threat Intelligence
Expand Detection
Security Operations
1
2
3
4
Optimize Detection
Threats
Organization

- Measure the real performance of your detection
- How your Blue Team time is spent
  - False positive rates
  - Contextless alerts
  - Investigation efficiency
- Missed detections

› Optimize your detection pipeline

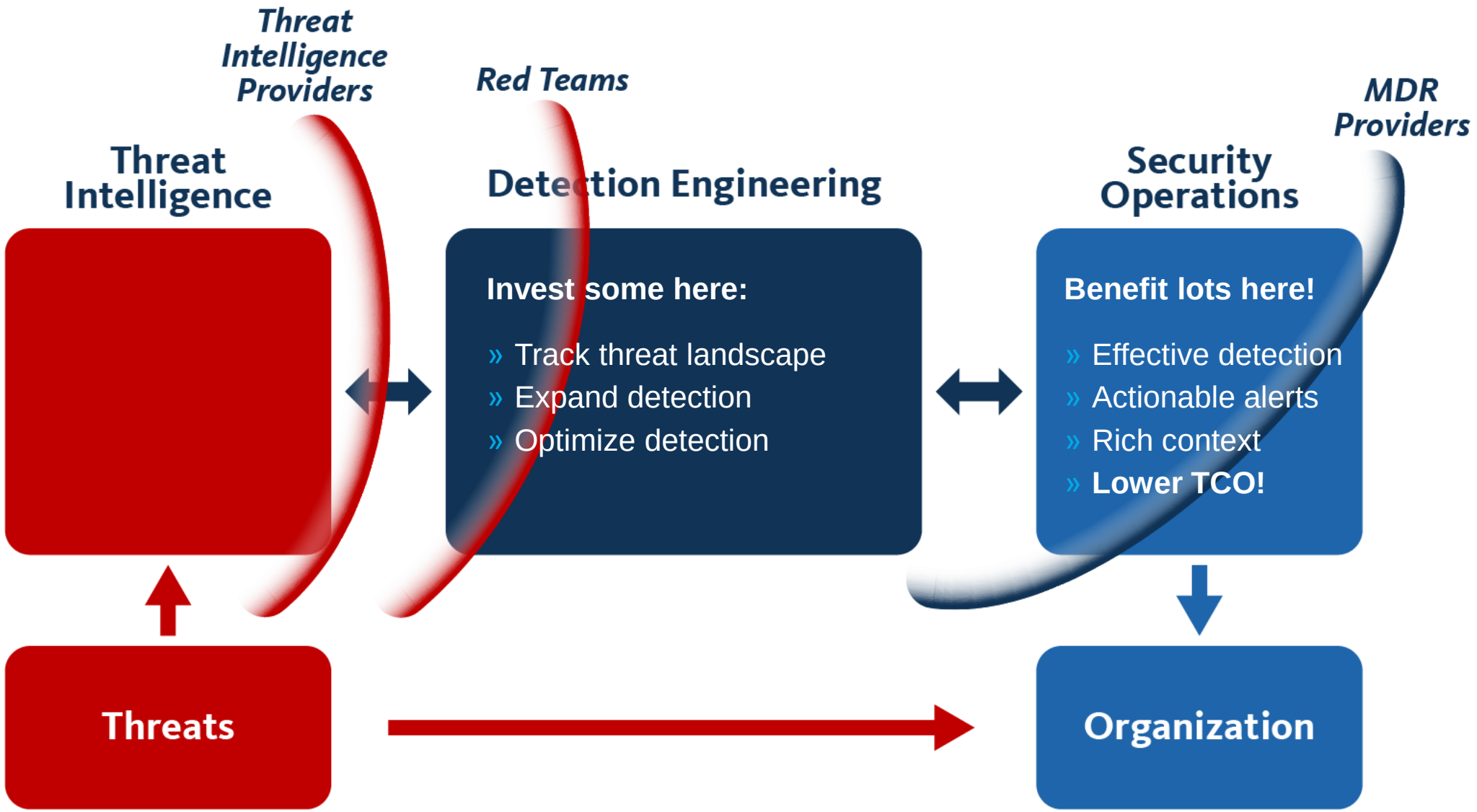
› Tune detection tools & rules

- Minimize false positive rate
- Verify detection remains effective

› Improve escalation and investigation

- Automated enrichment
- Data preparation, dashboards, etc.

- Ensure your detection covers current and relevant threats
- Retire out-of-date detection
- Continue threat intelligence-driven detection engineering iterations



FOX IT part of nccgroup

Conclusion

Three properties of successful security operations

- Active not passive
- Proactive and reactive
- Red and blue

Active not passive

Photo by Logan Weaver on Unsplash

Proactive and reactive

Photo by Alessandro Erbetta on Unsplash

Red and blue

Photo by Mayur Badhe on Unsplash

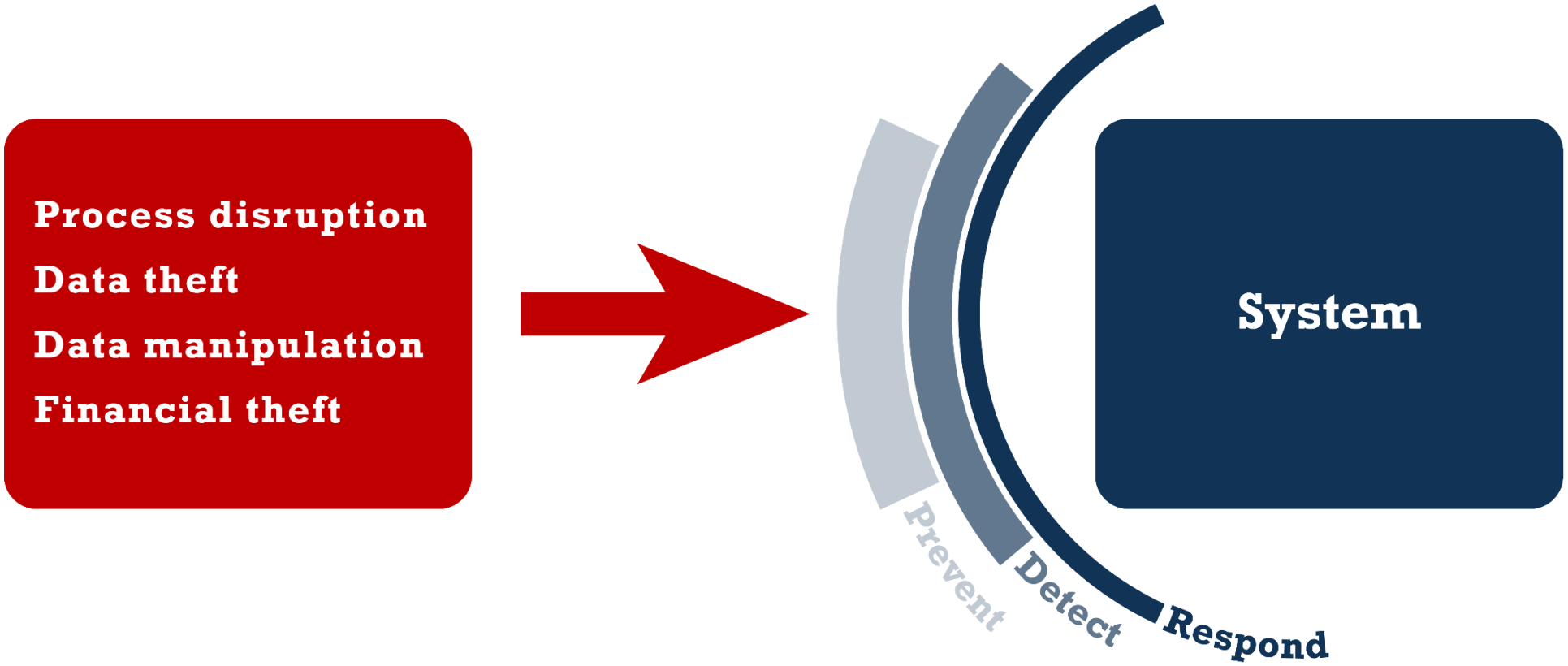
Three properties of successful security operations

- Active not passive
- Proactive and reactive
- Red and blue

Three strategic properties of successful security operations

- Resilience of business processes
- Scope of security
- Threats countered by security

Resilience of business processes



Scope of security

Photo by Geio Tischler on Unsplash

Threats countered by security

Conclusion

Operations

- Active not passive
- Proactive and reactive
- Red and blue

Strategy

- Resilience of business processes
- Scope of security
- Threats countered by security


FOX IT
part of nccgroup
Call us before you need us...