WELCOME

Work

- 20+ years in the telecommunications industry – Military & Public Sector
- Technical Engineering background in telecoms infrastructure
- Continually Promote Secure by Design and Threat Modelling Methodologies

Home / Life

- Live in Eryri National Park
- Proud Military Veteran
- Average Ultra Runner
- Co-Host of the CAPB Podcast

WHO AM I?

AGENDA

- High-Level Overview of the What, Why How and Who of Threat Modelling?
- High – Level Walk-through Talk through of Edge to Core Approach and Methodology

AIM

- To understand the mechanisms of Threat Modelling in general
- To gain a basic level of understanding of the Edge to Core approach and methodology

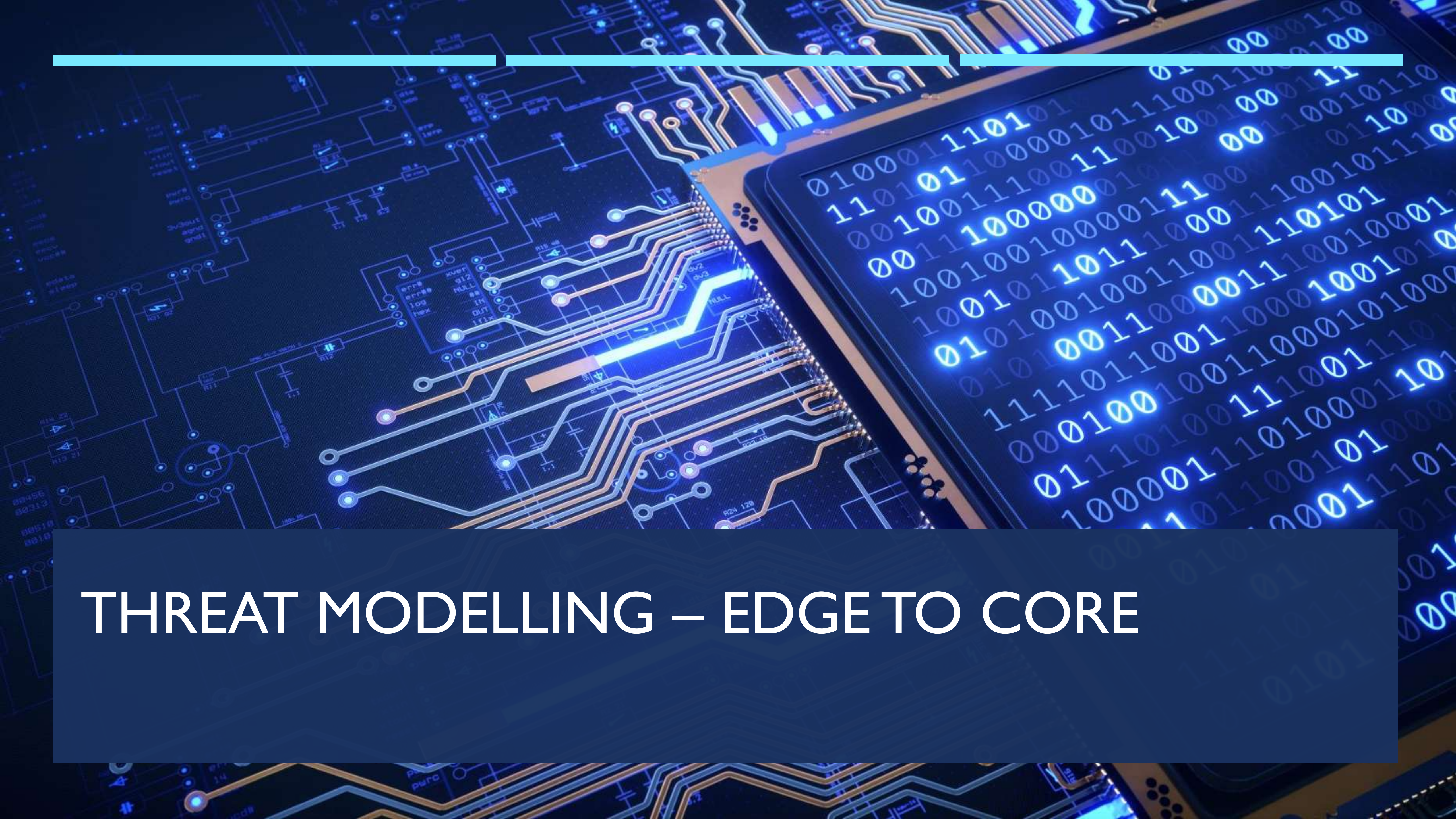
WE ALL THREAT MODEL…RIGHT?

WHAT IS A THREAT MODEL?

WHY DO WE NEED TO THREAT MODEL?

HOW DO YOU THREAT MODEL?

WHO DOES THE THREAT MODEL?



THREAT MODELLING – EDGE TO CORE

PREREQUISITE

- Have a good level understanding of the concepts of security and threats
- Understand what a ‘Control’ is and how it works
- Understand what the *MITRE ATT&CK framework is
- Understand what TTPs are and how they work.

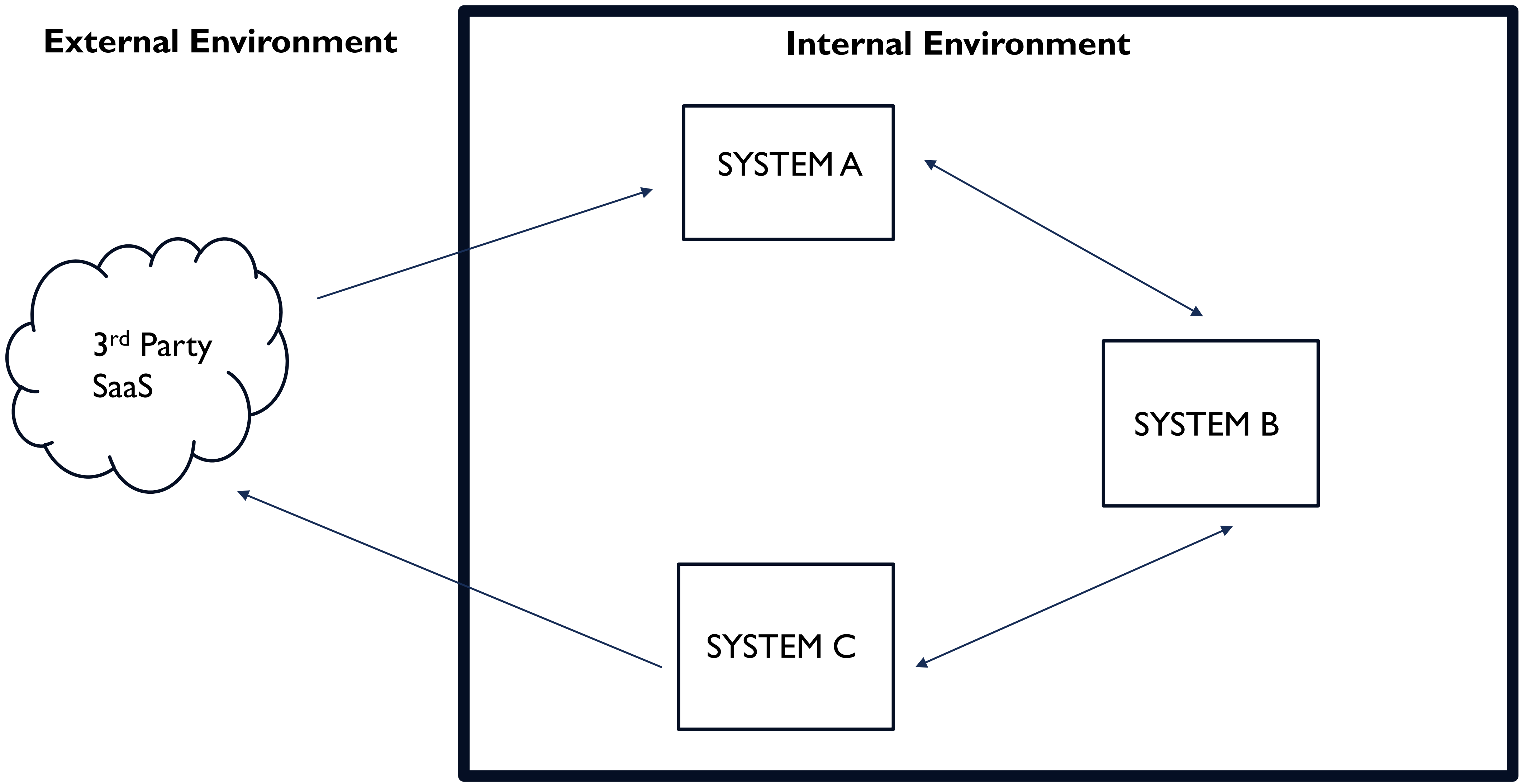
WHY EDGE TO CORE?

STAGES OF THE HOW

- Identify and Understand the Scope of the model
- Diagram and Map out the Attack Boundaries
- Identify and Analyse the Threats
- Review of Operational Data
- Mitigations & Next Actions

STAGE 1 – IDENTITY AND UNDERSTAND

STAGE 2 – DIAGRAM MODEL AND MAP OUT THE ATTACK BOUNDARIES



External Environment

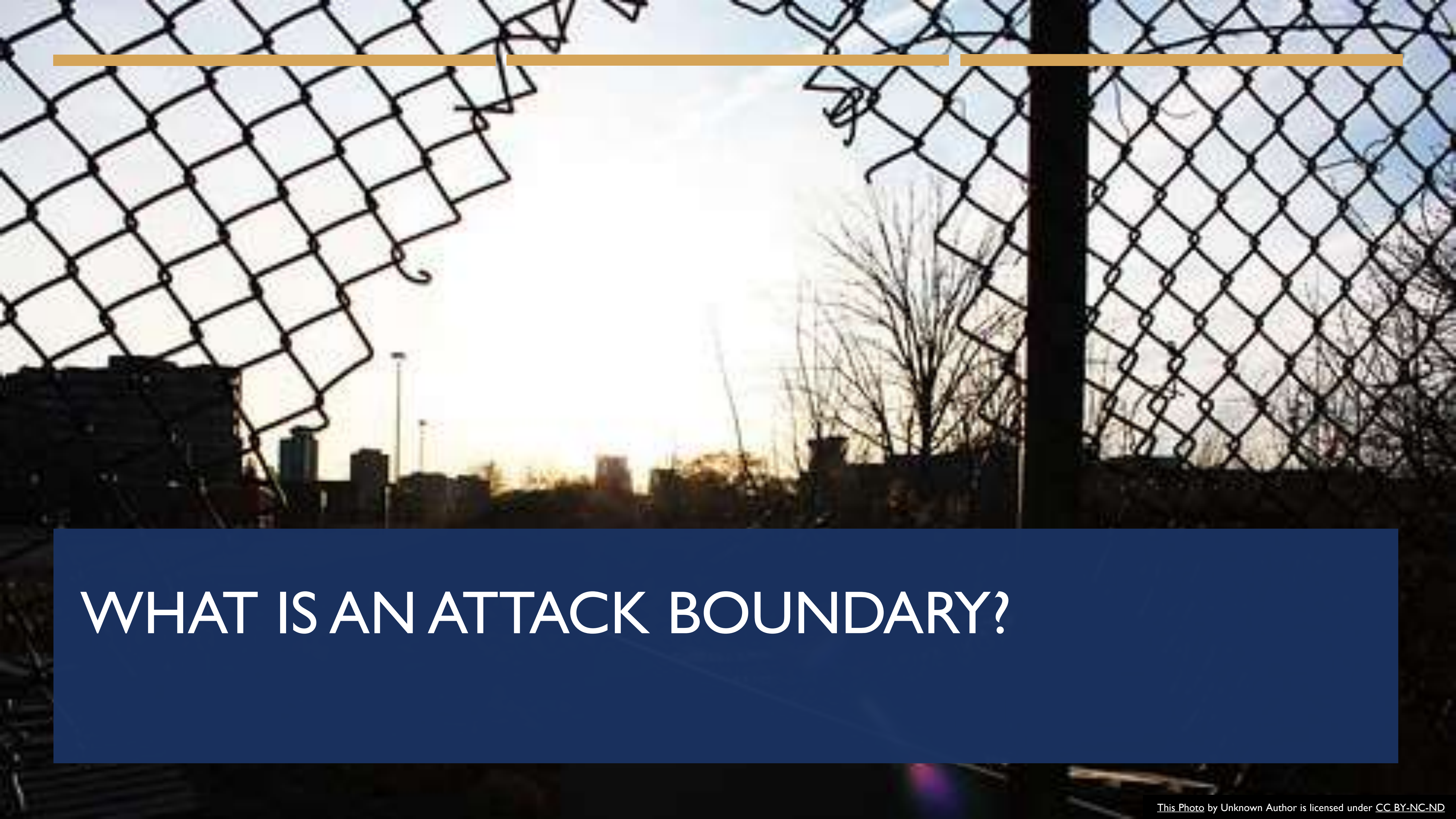
Internal Environment

SYSTEM A

SYSTEM B

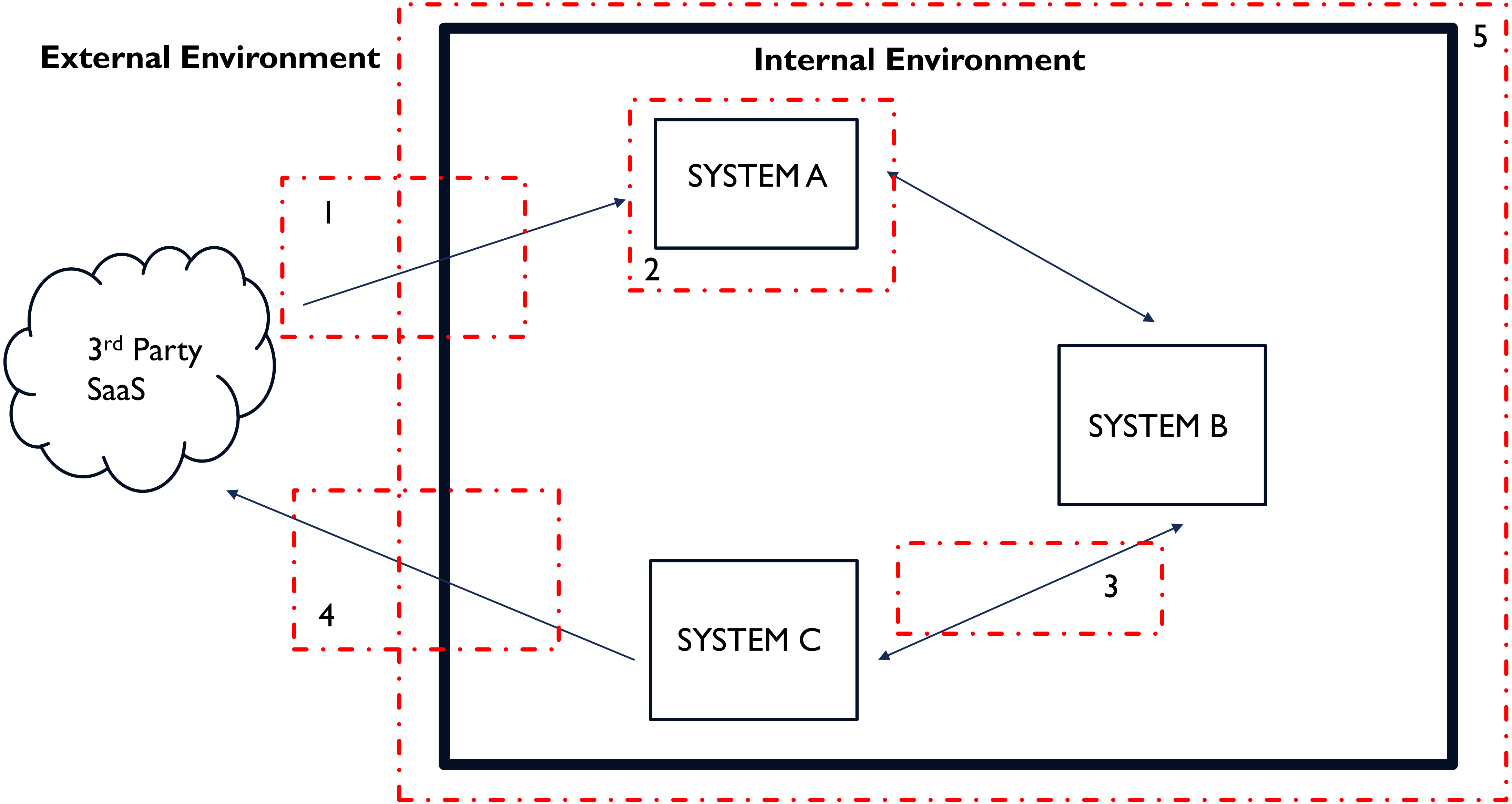
SYSTEM C

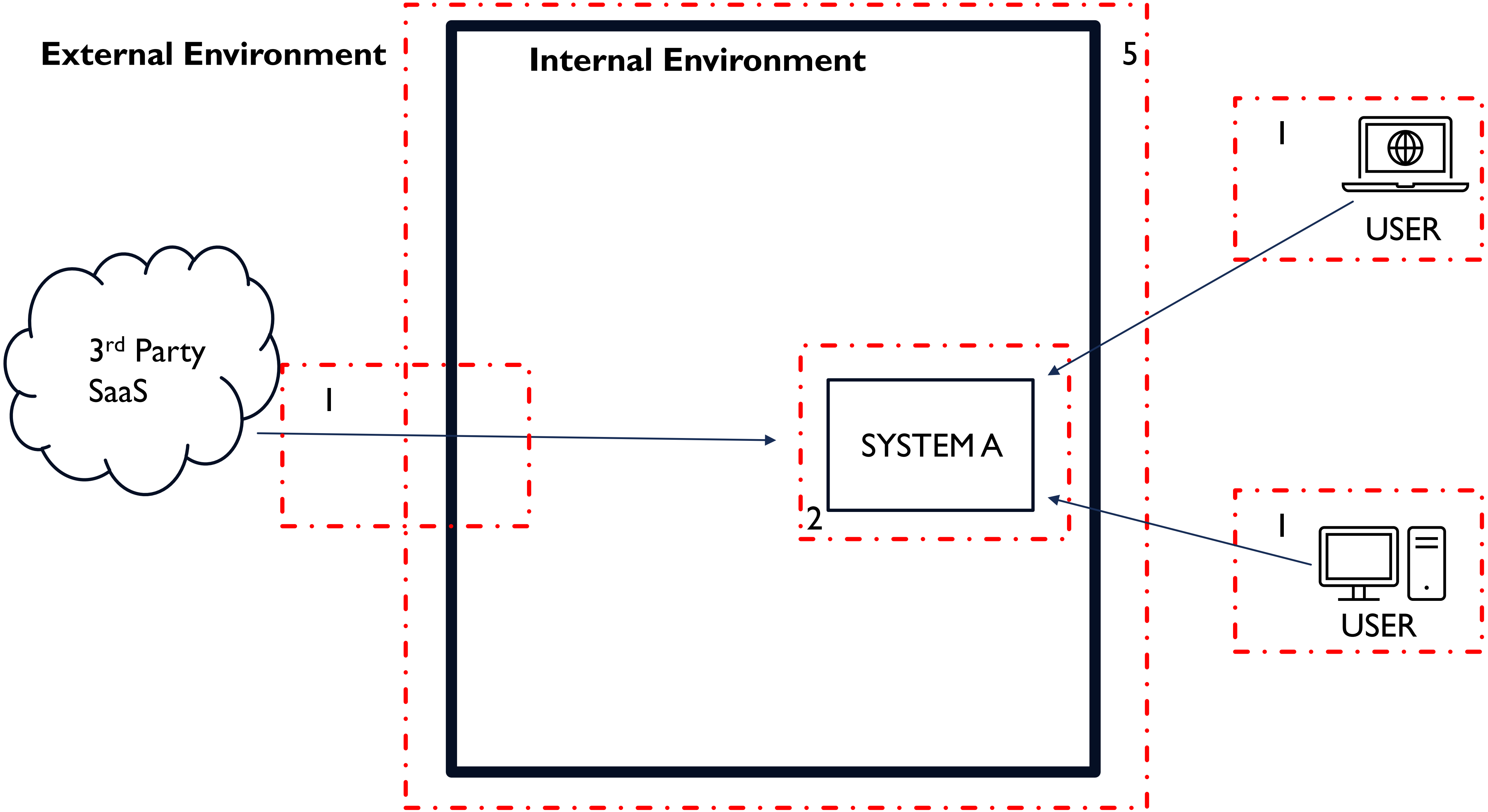
3rd Party SaaS



WHAT IS AN ATTACK BOUNDARY?

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


External Environment
Internal Environment
5
SYSTEM A
1
2
3rd Party
SaaS
SYSTEM B
3
4
SYSTEM C



External Environment

Internal Environment

5

I

USER

3rd Party
SaaS

I

SYSTEM A

2

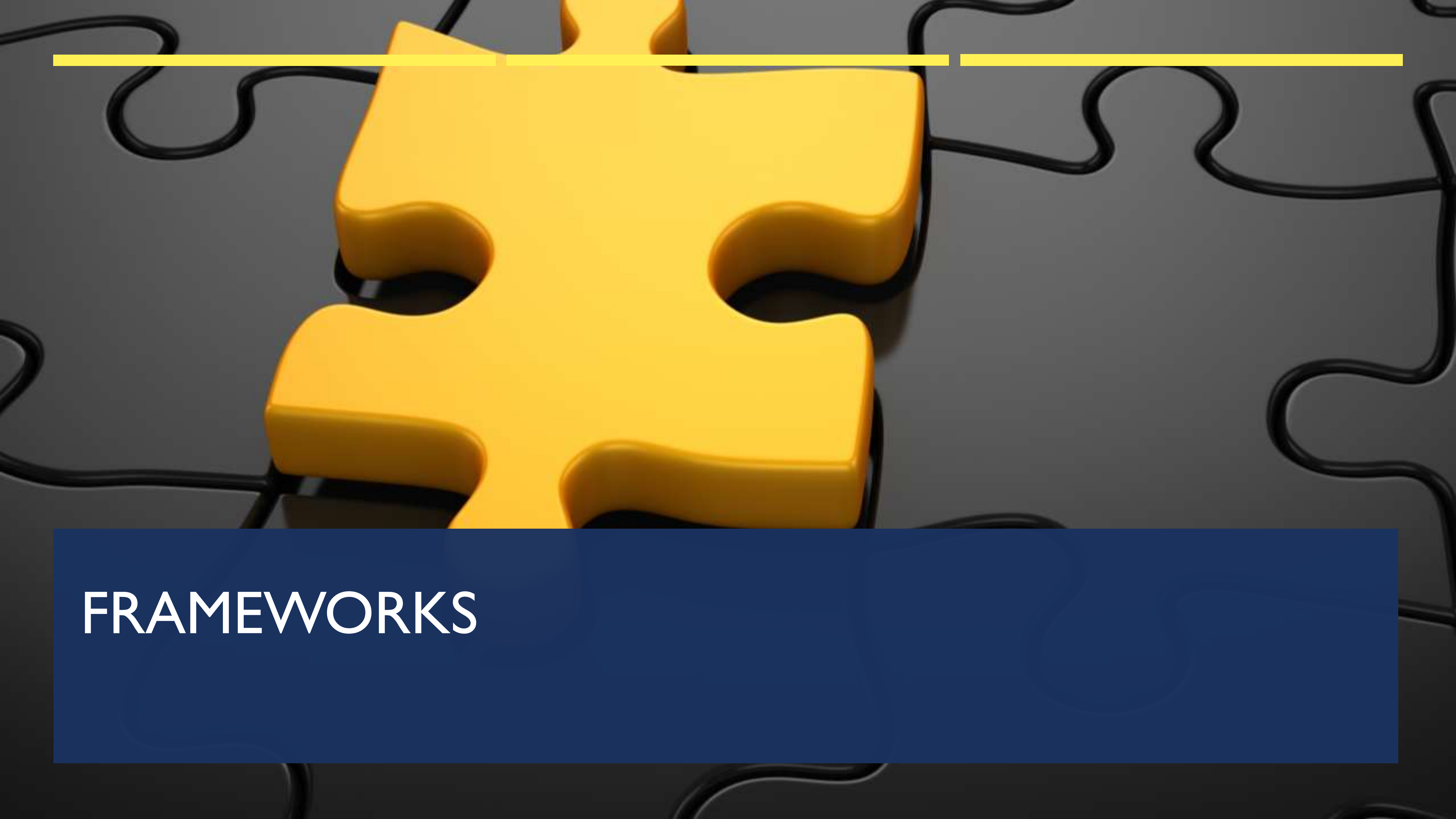
I

USER

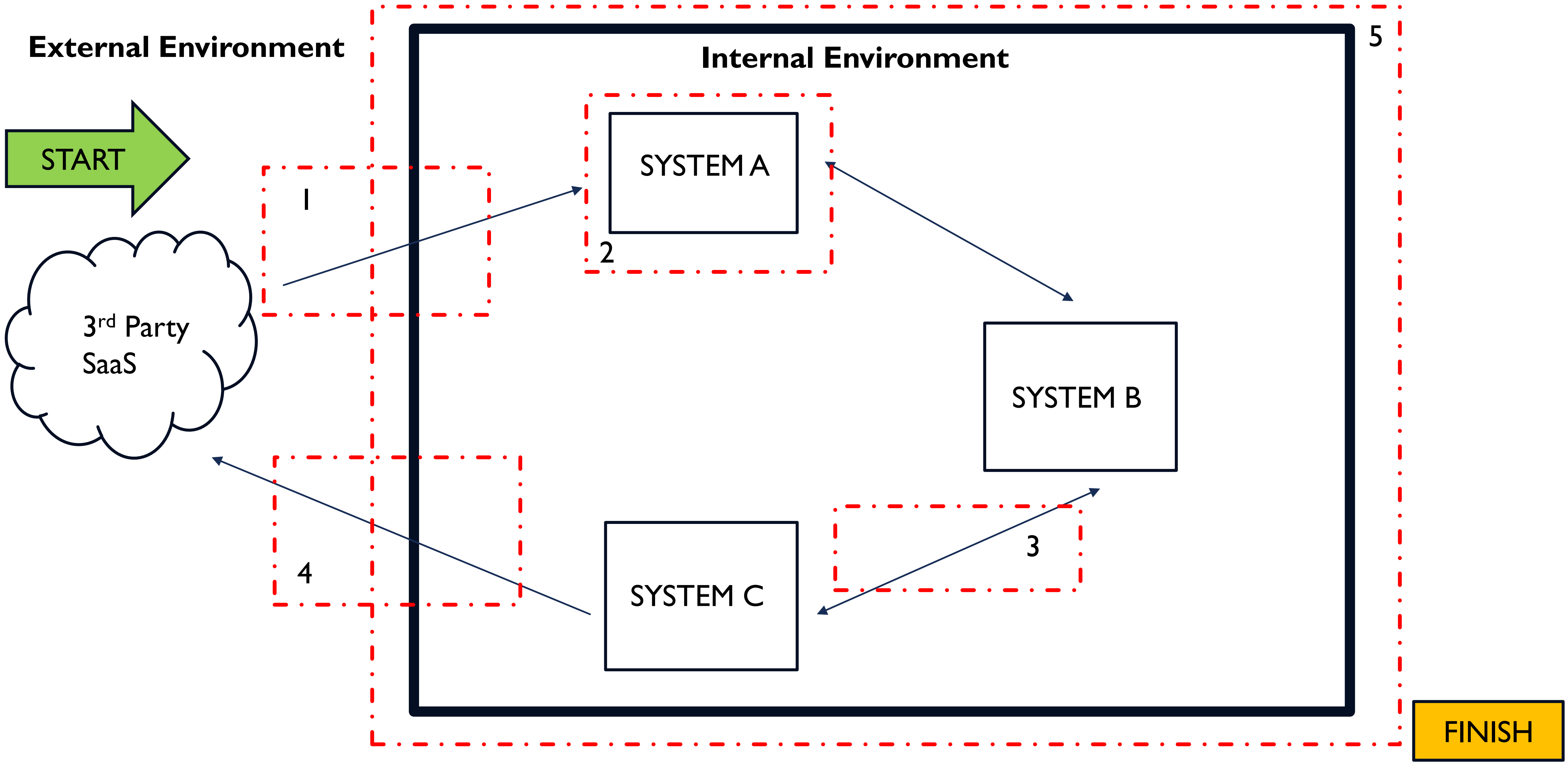
STAGE 3 – IDENTIFY AND ANALYSE THE THREATS

WHERE TO START?

START AT THE EDGE…..



FRAMEWORKS


External Environment
Internal Environment
START
3rd Party SaaS
SYSTEM A
SYSTEM B
SYSTEM C
1
2
3
4
5
FINISH

ASK THE QUESTION - DOES THE CONTROL…..

Prevent you gaining access?

Prevent you viewing information?

Prevent you moving around?

Prevent you from changing anything?

Prevent you from stopping it from working?

Prevent your actions to go unnoticed?

Prevent it to be accessed by a 3rd Party?

CONTROL VALIDITY

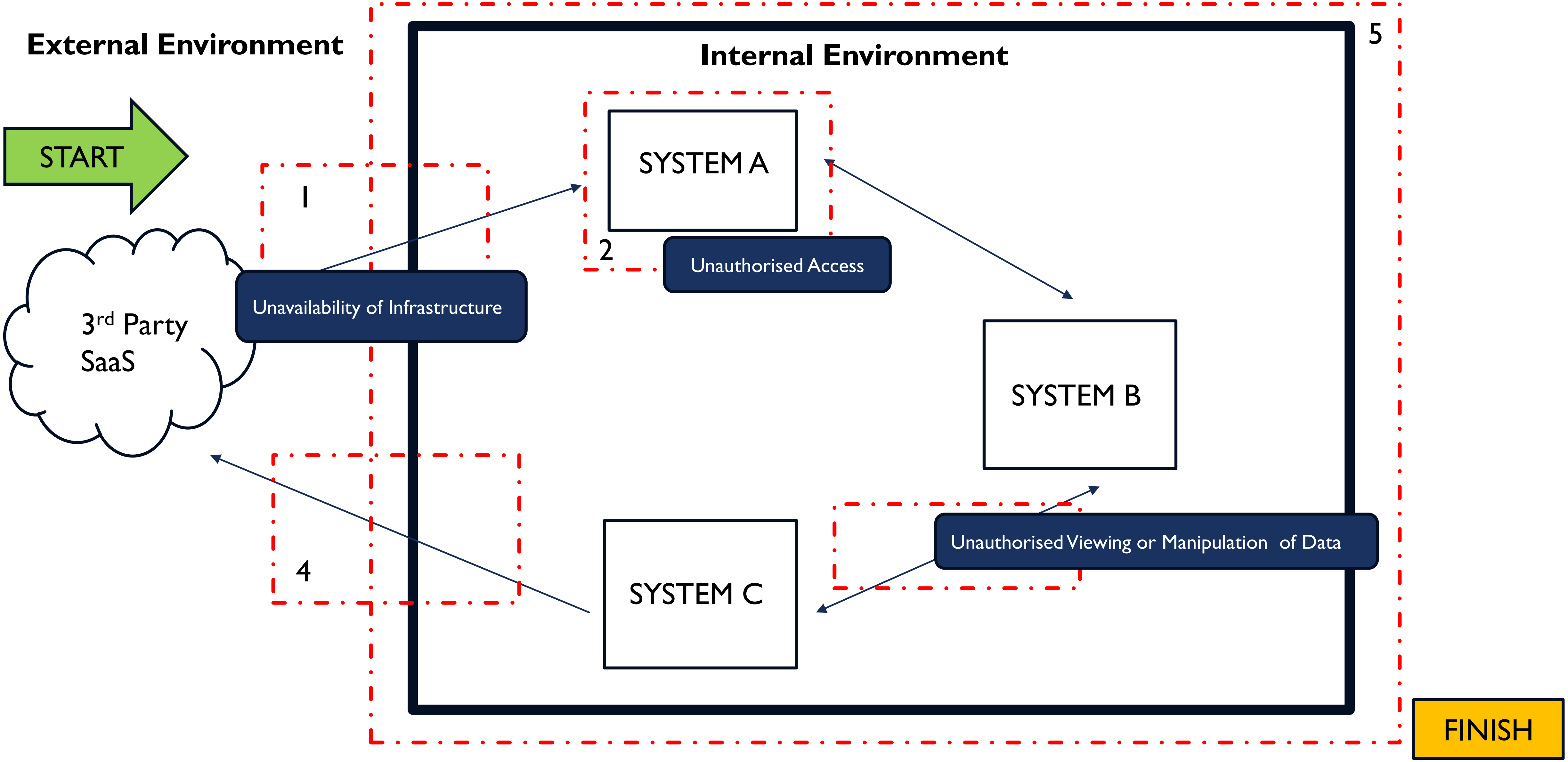
HIGH-LEVEL THREATS

LACK OF A HIGH-LEVEL CONTROL = A HIGH-LEVEL THREAT

Question	Lack of Control	High Level Threat	Threat Description
Prevent you gaining access?	Identity and Access Management (IDAM)	Unauthorised Access	This is when an individual who does not, and should not, have access to an environment, system or its data manages to gain access. Attackers will aim to gain access to and compromise the confidentiality, integrity or availability of ANY environments, systems or data
Prevent you viewing information?	Cryptographic	Unauthorised Viewing or Manipulation of Data	This is when an individual who does not, and should not, have access to an environment, system or its data manages to view or manipulate data whilst at rest or in transit.
Prevent you moving around?	Segregation	Lateral Movement	When a user can move between environments or systems without being detected. Attackers will leverage incorrect or incomplete movement / access rules relating to environments, systems, applications or services to do this.

Questions	Lack of Control	High Level Threat	Threat Description
Prevent you from changing anything?	Application	Poor Implementation or Mis-configuration	Attackers will leverage weaknesses that has been unknowingly introduced into, an environment, a tool, a piece of software, a system or a device, which then can be exploited.
Prevent you from stopping it from working?	Availability	Unavailability of a Service, Infrastructure or Data	When an entity is unable to function due to it being either unreachable or unusable. Attackers will target environments, systems or data in order to compromise their availability, these may come in the form of a Denial of Service (DOS) or Ransomware attacks
Prevent your actions to go unnoticed?	Vulnerability Management	Exploitation	The environment, systems, asset or persons can be manipulated or modified unknowingly or without detection. Attackers will leverage a weakness or flaw in an environment, system, process, tooling or people that could allow a malicious task to be carried out.

Questions	Lack of Control	High Level Threat	Threat Description
Prevent it to be accessed by a 3rd Party?	Supplier	Supply Chain	When a vulnerability can be introduced into or exploited from a 3rd Parties infrastructure. Attackers will aim to compromise a supplier's environment (including ingress and egress connectivity), their software or hardware, at any stage of the supply chain journey, in order to gain access into the primary environment.



External Environment

START

3rd Party SaaS

1

Unavailability of Infrastructure

Internal Environment

5

SYSTEM A

2

Unauthorised Access

SYSTEM B

Unauthorised Viewing or Manipulation of Data

SYSTEM C

4

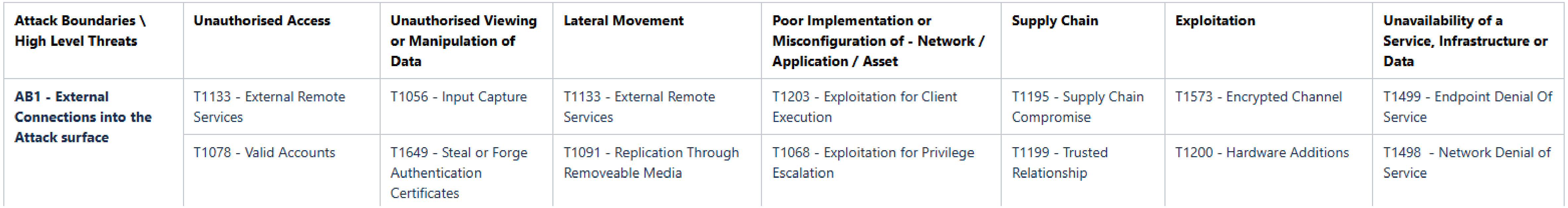
FINISH

High-Level Threats	Mitigation
Unauthorised Access	Implement a complex access control policy on System A
Unavailability of Infrastructure	Implement resiliency controls like load balancers or firewalls at the edge of environment
Unauthorised Viewing or Manipulation of Data	Use encryption or secure methods of data transfer – TLS or SFTP

DIG A LITTLE DEEPER…..

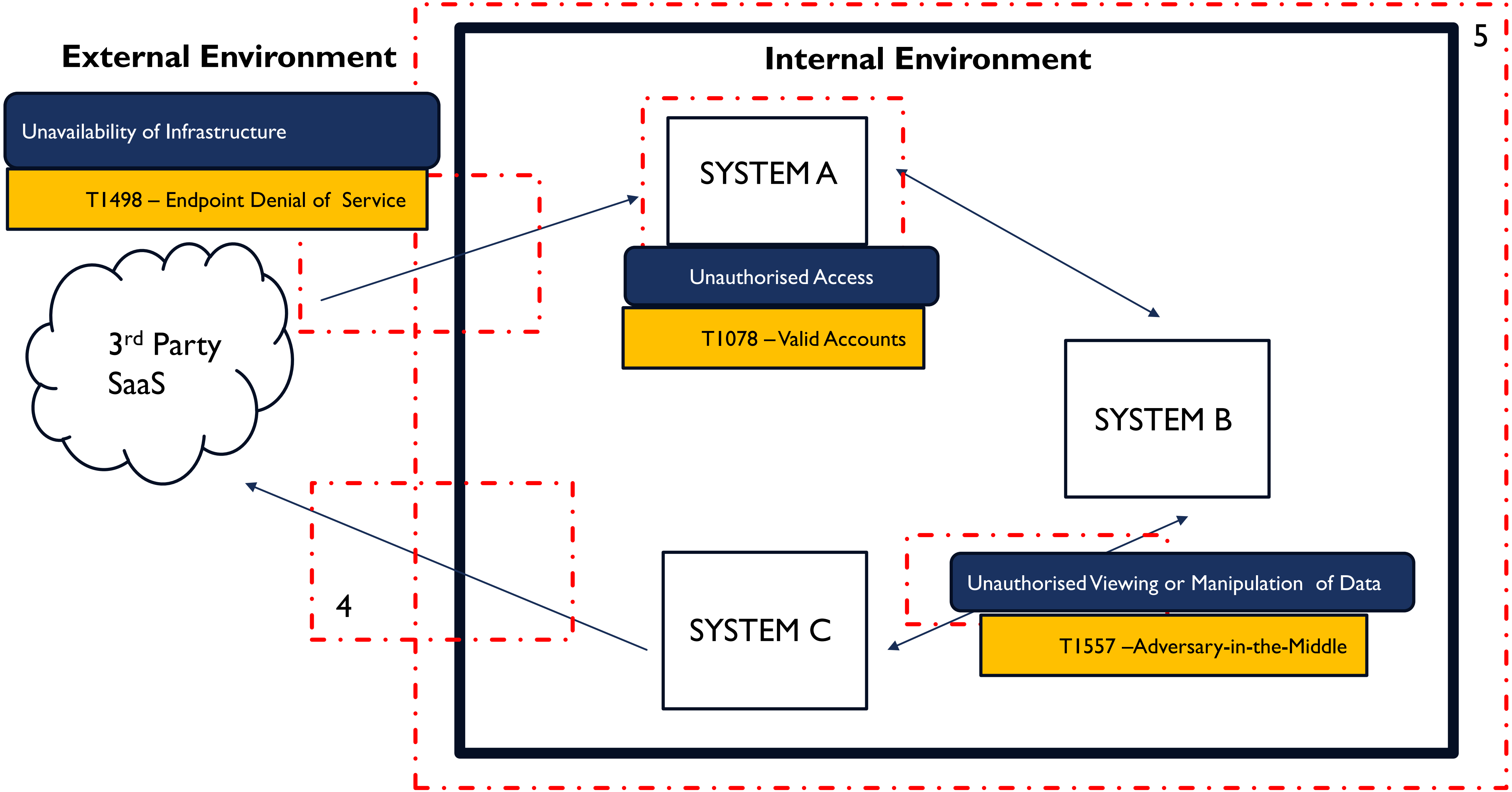
THREATS TO TTP’S (TOOLS , TECHNIQUES AND PROCEDURE)

THREAT – BOUNDARY – TTP



Attack Boundaries \ High Level Threats	Unauthorised Access	Unauthorised Viewing or Manipulation of Data	Lateral Movement	Poor Implementation or Misconfiguration of - Network / Application / Asset	Supply Chain	Exploitation	Unavailability of a Service, Infrastructure or Data
AB1 - External Connections into the Attack surface	T1133 - External Remote Services	T1056 - Input Capture	T1133 - External Remote Services	T1203 - Exploitation for Client Execution	T1195 - Supply Chain Compromise	T1573 - Encrypted Channel	T1499 - Endpoint Denial Of Service
	T1078 - Valid Accounts	T1649 - Steal or Forge Authentication Certificates	T1091 - Replication Through Removeable Media	T1068 - Exploitation for Privilege Escalation	T1199 - Trusted Relationship	T1200 - Hardware Additions	T1498 - Network Denial of Service

DISCOUNTING TTP'S



External Environment
Internal Environment
5
Unavailability of Infrastructure
T1498 – Endpoint Denial of Service
3rd Party SaaS
SYSTEM A
Unauthorised Access
T1078 – Valid Accounts
SYSTEM B
SYSTEM C
4
Unauthorised Viewing or Manipulation of Data
T1557 –Adversary-in-the-Middle

High-Level Threats	MITRE ATT&CK TTP
Unauthorised Access	T1078 – Valid Accounts
Unavailability of Infrastructure	T1498 – Endpoint Denial of Service
Unauthorised Viewing or Manipulation of Data	T1557 – Adversary-in-the-Middle

OPERATIONS AND DESIGN COLLABORATION

STAGE 4 – REVIEW OF OPERATIONAL DATA

WHAT DATA

- Threat Intelligence
- Incident Data
- Threat Actors of Interest

THREAT INTELLIGENCE

INCIDENT DATA

THREAT ACTORS OF INTEREST

HOW DOES IT HELP?

REAL – TIME DYNAMIC UPDATES

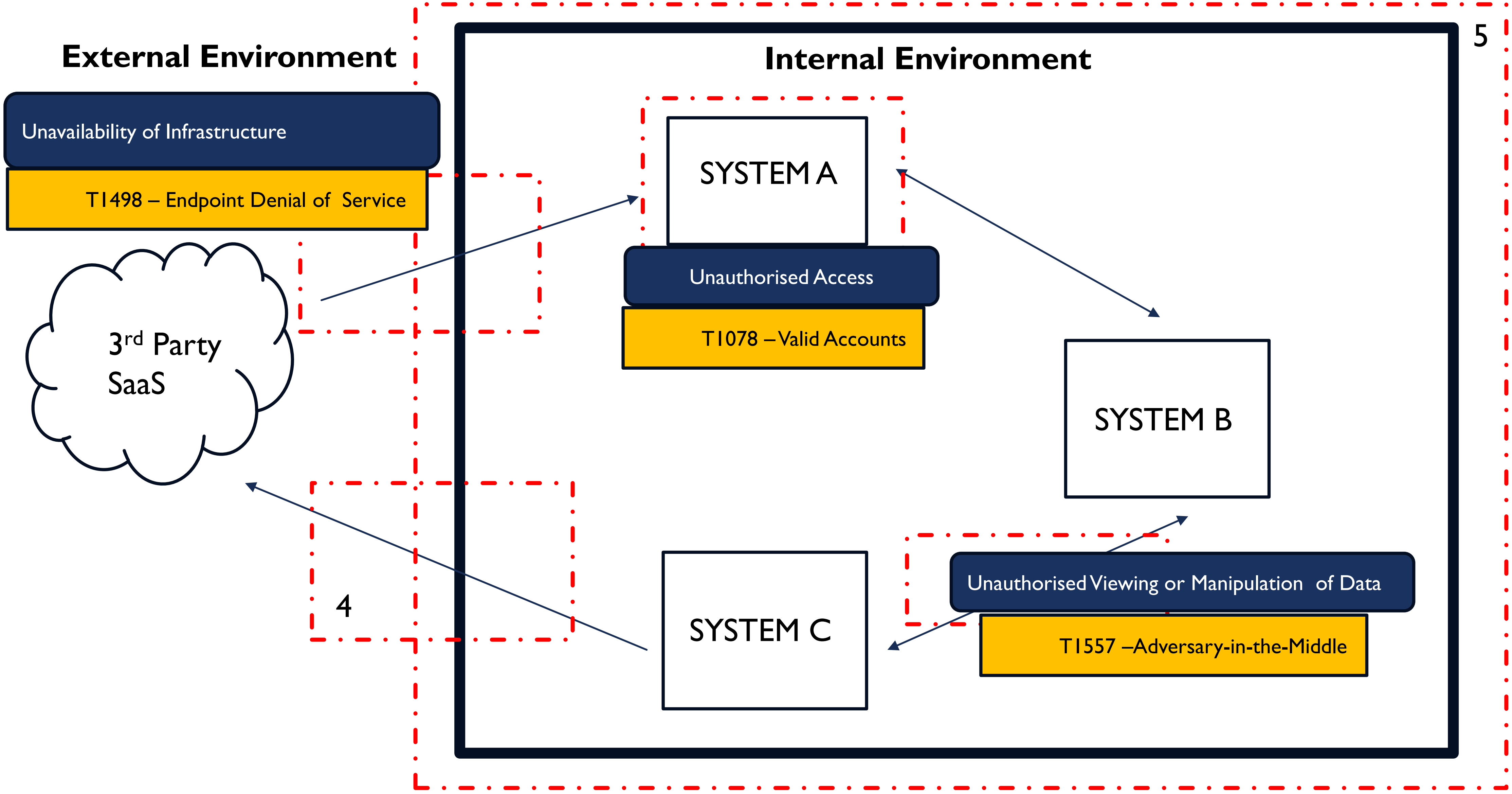
ENHANCED THREAT PRIORITISATION

UNDERSTANDING OF MOTIVATIONS AND TACTICS

DATA DRIVEN INSIGHTS

CREATES A CONTINUOUS FEEDBACK MECHANISM

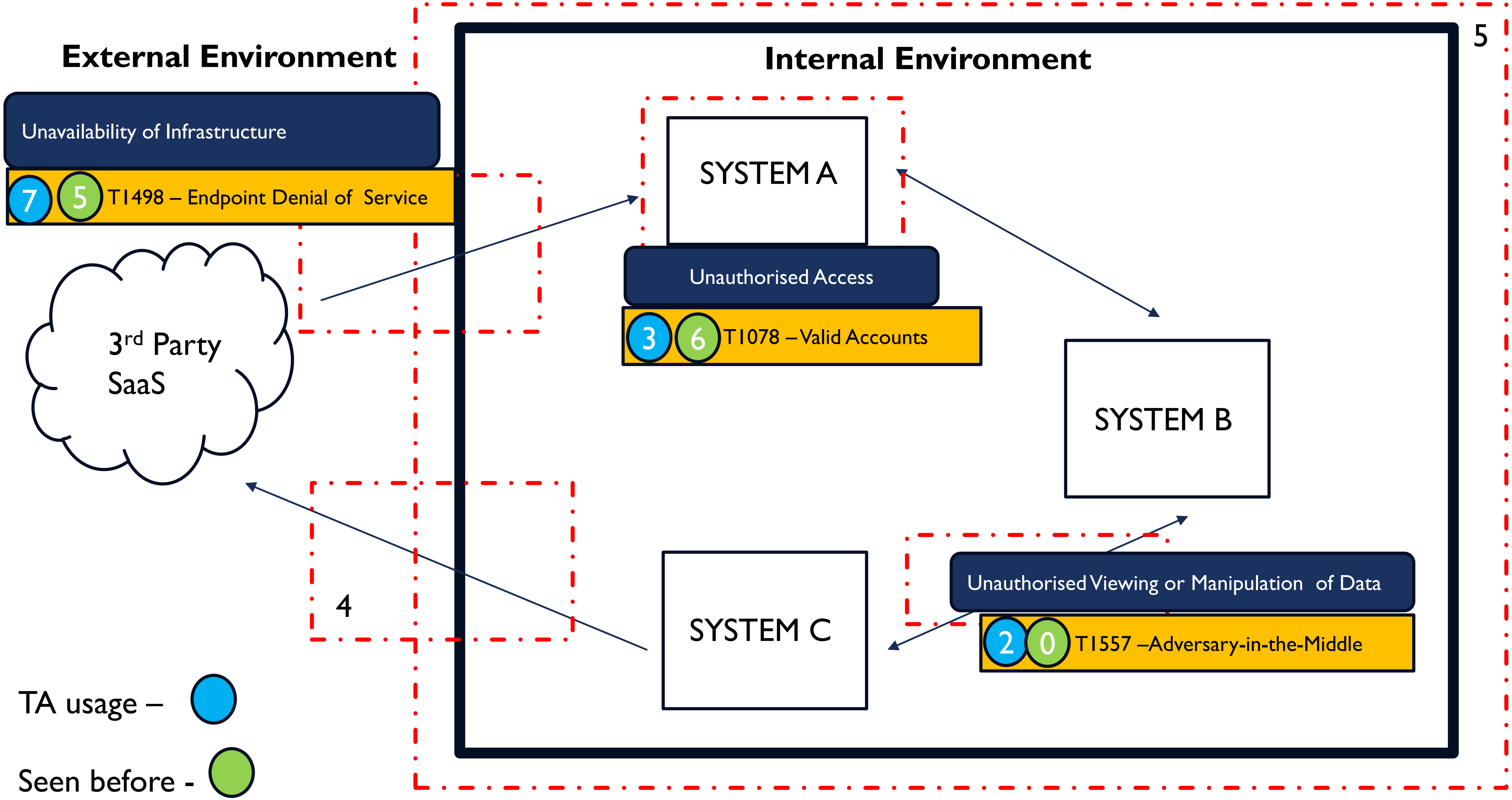
STAGE 5 - MITIGATIONS & NEXT ACTIONS


External Environment
Internal Environment
5
Unavailability of Infrastructure
T1498 – Endpoint Denial of Service
SYSTEM A
Unauthorised Access
T1078 – Valid Accounts
3rd Party SaaS
SYSTEM B
4
SYSTEM C
Unauthorised Viewing or Manipulation of Data
T1557 –Adversary-in-the-Middle

High-Level Threats	MITRE ATT&CK TTP	Mitigation
Unauthorised Access	T1078 – Valid Accounts	Implement a complex access control policy on System A Implement MFA on system A
Unavailability of Infrastructure	T1498 – Endpoint Denial of Service	Implement resiliency controls like load balancers or firewalls at the edge of environment Filter Network Traffic Implement DDOS or EDR tooling
Unauthorised Viewing or Manipulation of Data	T1557 –Adversary-in-the-Middle	Use encryption or secure methods of data transfer – TLS or SFTP Encrypt sensitive data at source Use MTLS

THREAT PRIORITISATION WITH OPERATIONAL DATA

How many of the Threat Actors on the list use TTP?	Previous occurrences of the TTP being realised against the business?	Priority Score
0-3	0-3	LOW
4-6	4-7	MEDIUM
7-10	8 Upwards	URGENT



External Environment

Unavailability of Infrastructure

7 5 T1498 – Endpoint Denial of Service

3rd Party SaaS

Internal Environment

SYSTEM A

Unauthorised Access

3 6 T1078 –Valid Accounts

SYSTEM B

SYSTEM C

Unauthorised Viewing or Manipulation of Data

2 0 T1557 –Adversary-in-the-Middle

4

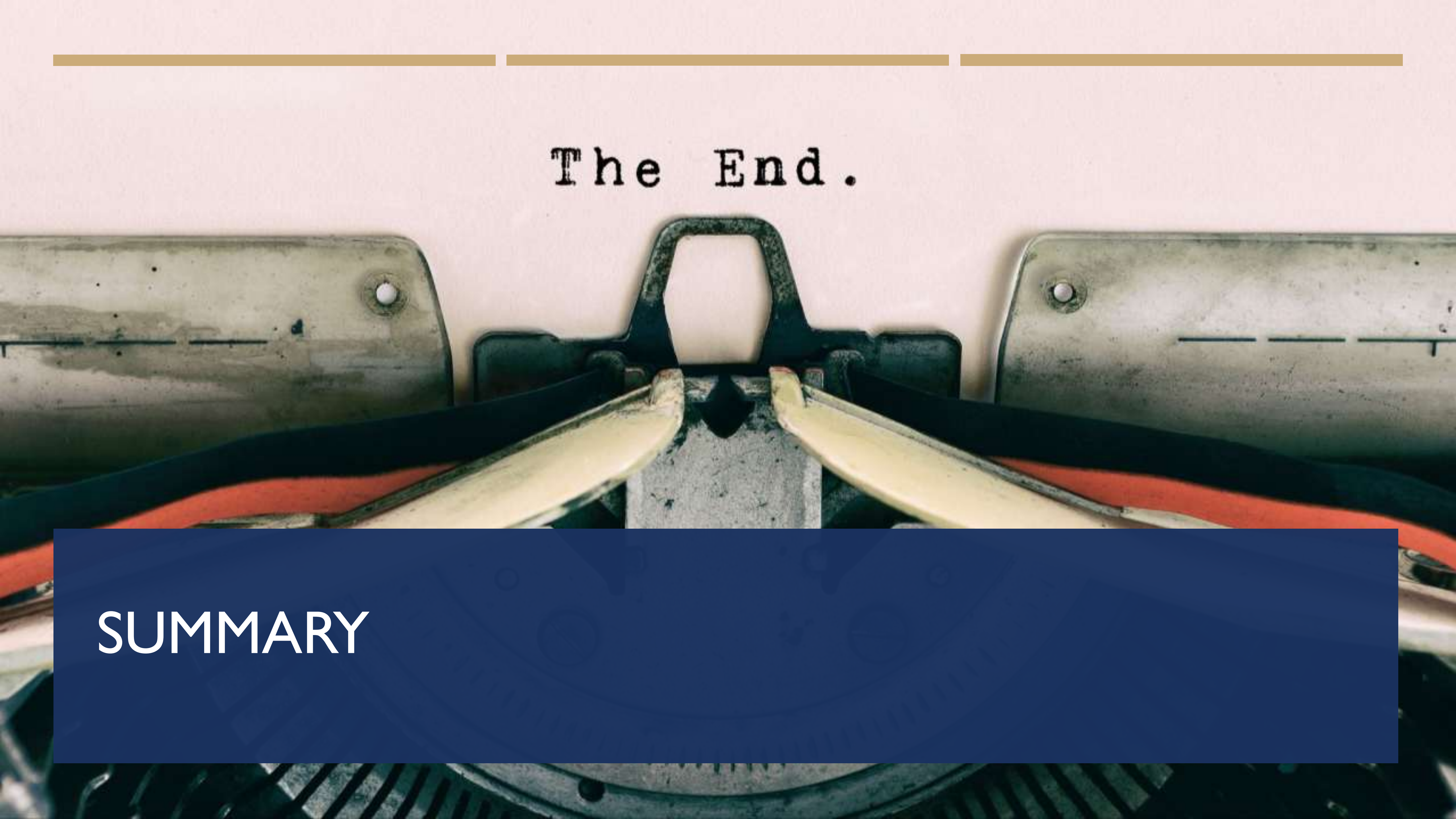
5

TA usage – ●

Seen before - ●

High-Level Threats	MITRE ATT&CK TTP	Mitigation	Priority Score
Unauthorised Access	T1078 – Valid Accounts	Implement a complex access control policy on System A Implement MFA on system A	MEDIUM
Unavailability of Infrastructure	T1498 – Endpoint Denial of Service	Implement resiliency controls like load balancers or firewalls at the edge of environment Filter Network Traffic Implement DDOS or EDR tooling	URGENT
Unauthorised Viewing or Manipulation of Data	T1557 –Adversary-in-the-Middle	Use encryption or secure methods of data transfer – TLS or SFTP Encrypt sensitive data at source Use MTLS	LOW

THREAT LIBRARY



SUMMARY

THANK YOU