Insiders

Adversarial Behaviours

Insiders

Adversarial Behaviours

- Enterprises and other organisation are usually good at securing their organisation against **external threats**.
- Enterprises and other organisations **often neglect** the internal threat of employees performing non-malicious and malicious actions.

What is an insider?

What is an insider?

Insiders

- Trusted individuals that exploits or intend to exploit access and/or knowledge of enterprise or organisation assets for unauthorised purposes.

Typical insider actions

Typical malicious insider actions

European Union Agency for Cyber security

- Privilege abuse.
- Mishandling of data.
- Use of non-approved hardware.
- Privilege possession.

Typical non-malicious insider actions

European Union Agency for Cyber security

- Phishing.
- Poor passwords.
- Devices not properly secured, i.e. no control lock.
- Sharing passwords.
- Networks not properly secured.

Types of insiders

Types of insiders

Saxena et al.

Malicious insider

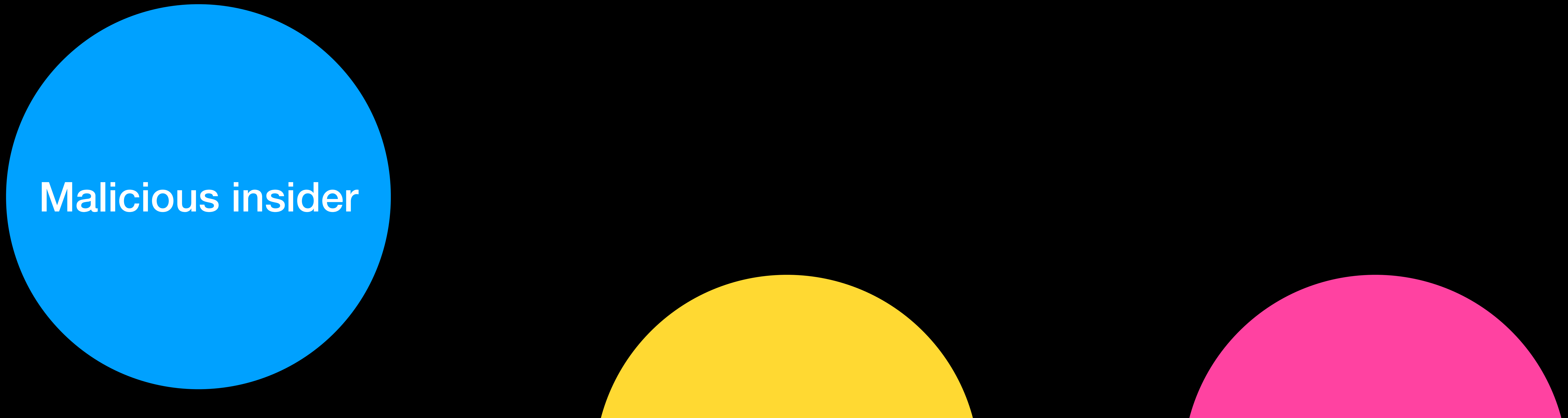
Compromised insider

Carless insider

Malicious insider

Types of insiders

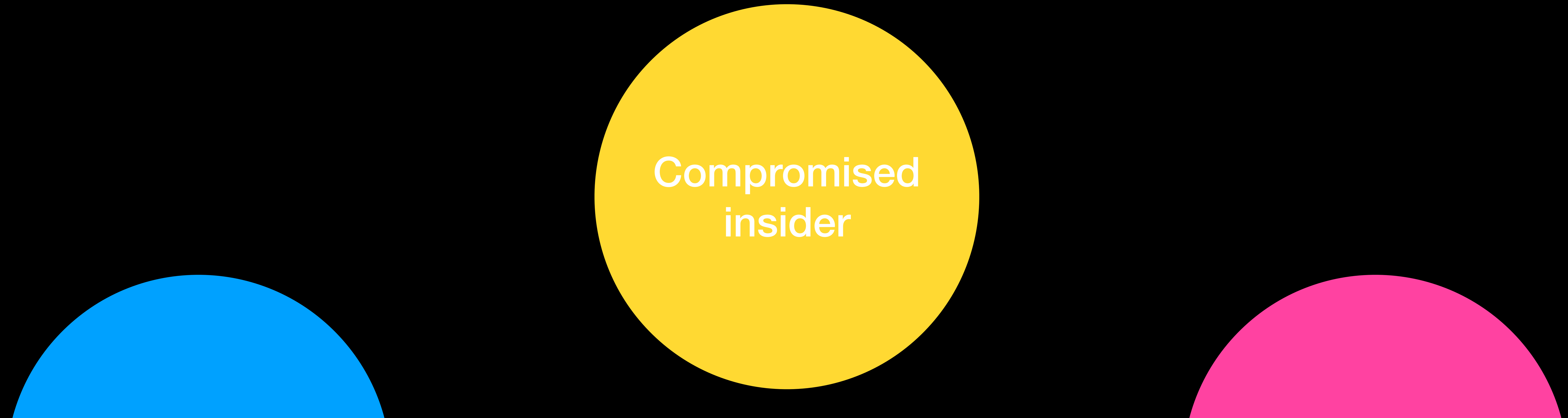
- An insider that abuses legitimate access to assets and credentials to acquire assets for gain.



Compromised insider

Types of insiders

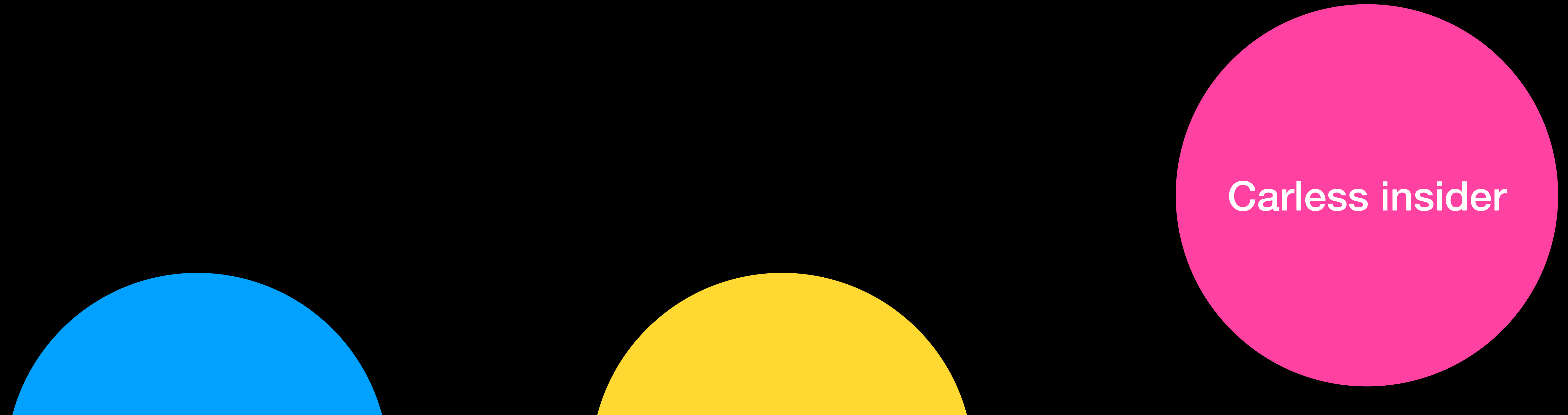
- Credentials and access to assets that have been harvested and afford attackers to again access to resources.



Carless insider

Types of insiders

- Trusted individuals that make mistakes and are not aware of security practices.



Carless insider

Types of insiders

Saxena et al.

Malicious insider

Compromised insider

Carless insider

Inception of insiders

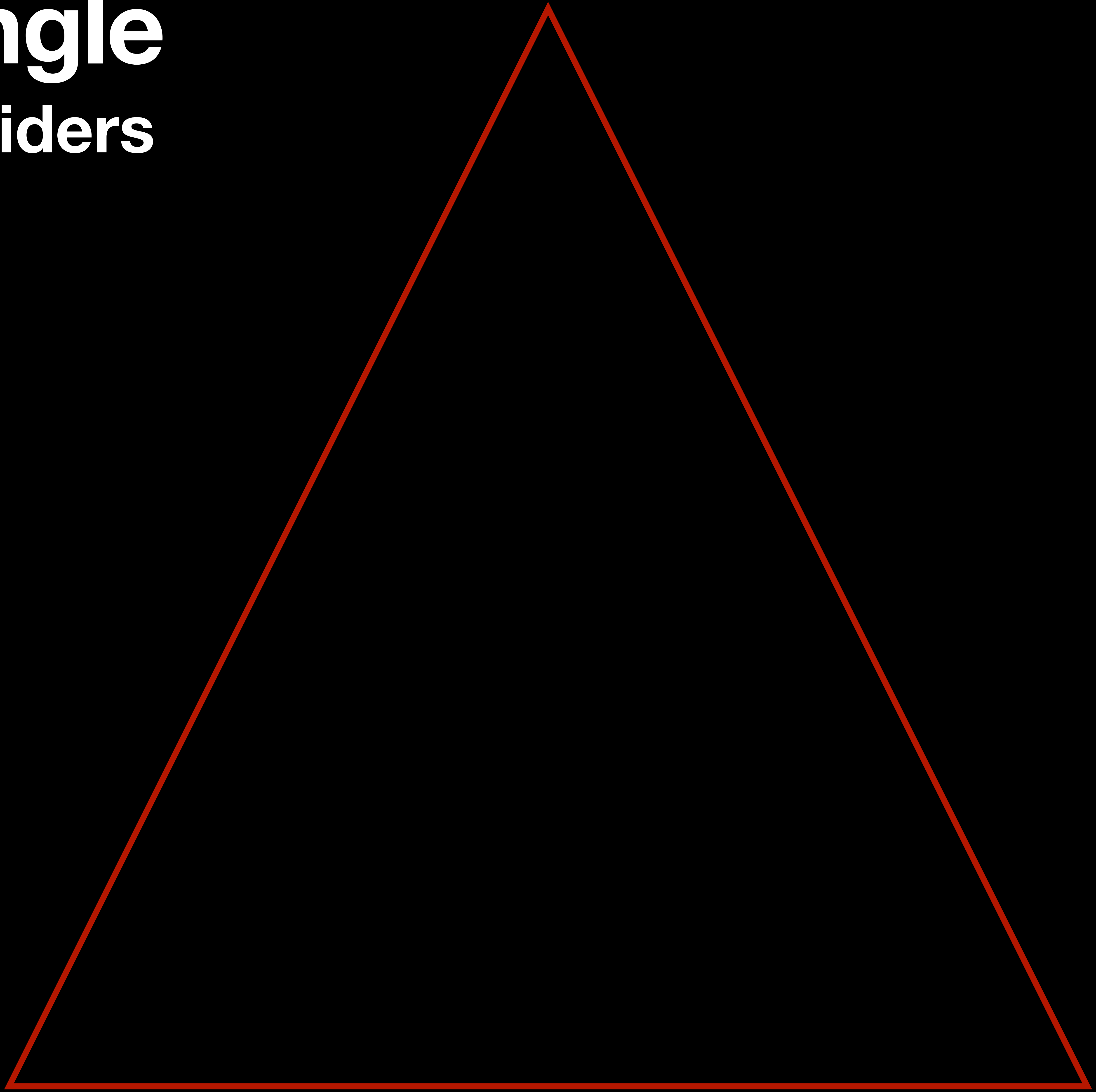
Inception of insiders

Insiders

- Insiders are often disgruntled and unhappy with the organisation.
    - Unfriendly atmosphere, poor office environment, lack of progression.
- Insiders often act, but not always, after a negative event.
    - Loss autonomy, poor relationships within organisation or general unhappiness.
- Unusual behaviour is often indicative of the inception of insider attack.
    - Possible to identify insider threats through behaviour monitoring.

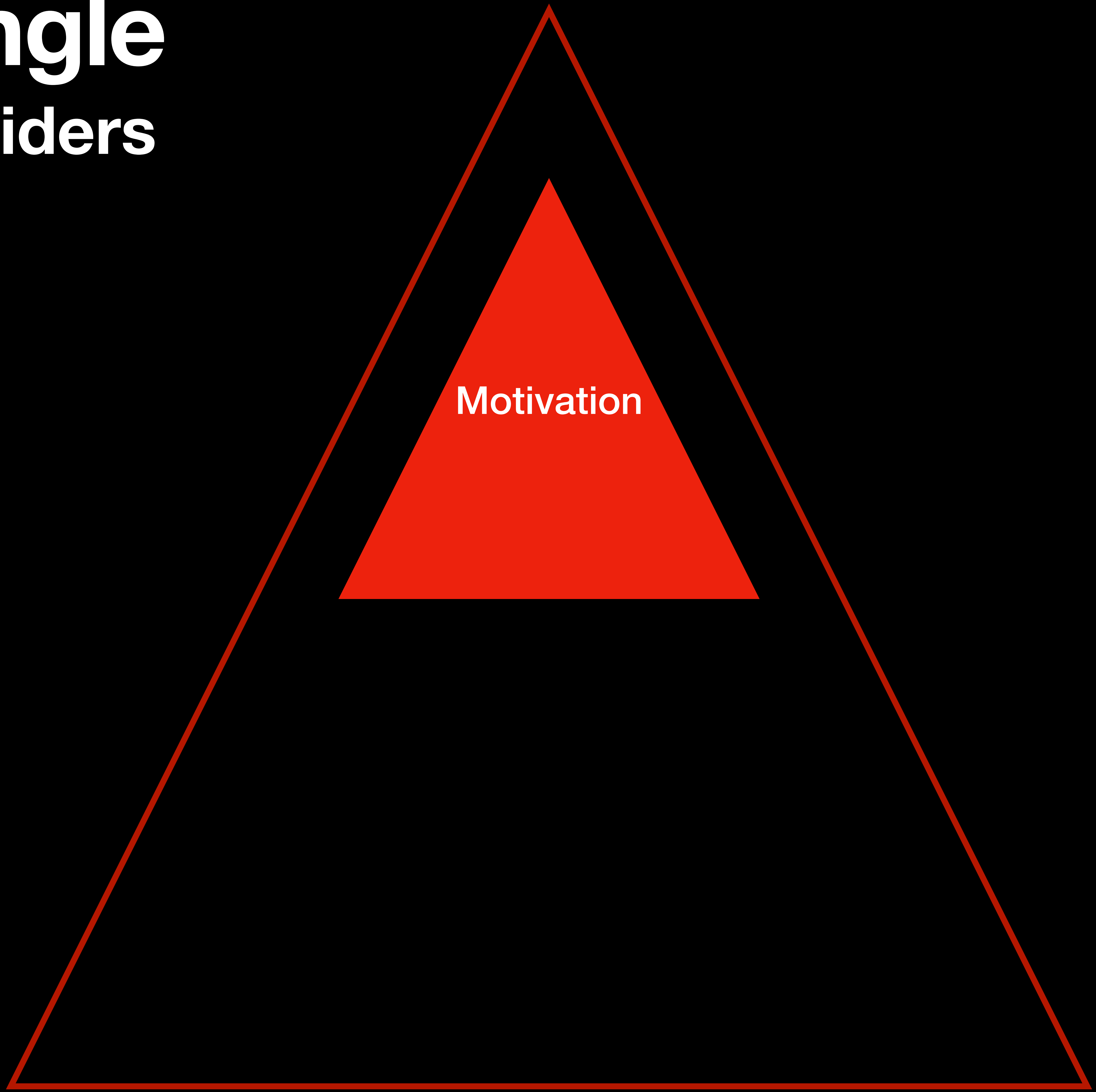
Fraud triangle

Inception of insiders



Fraud triangle

Inception of insiders



Motivation

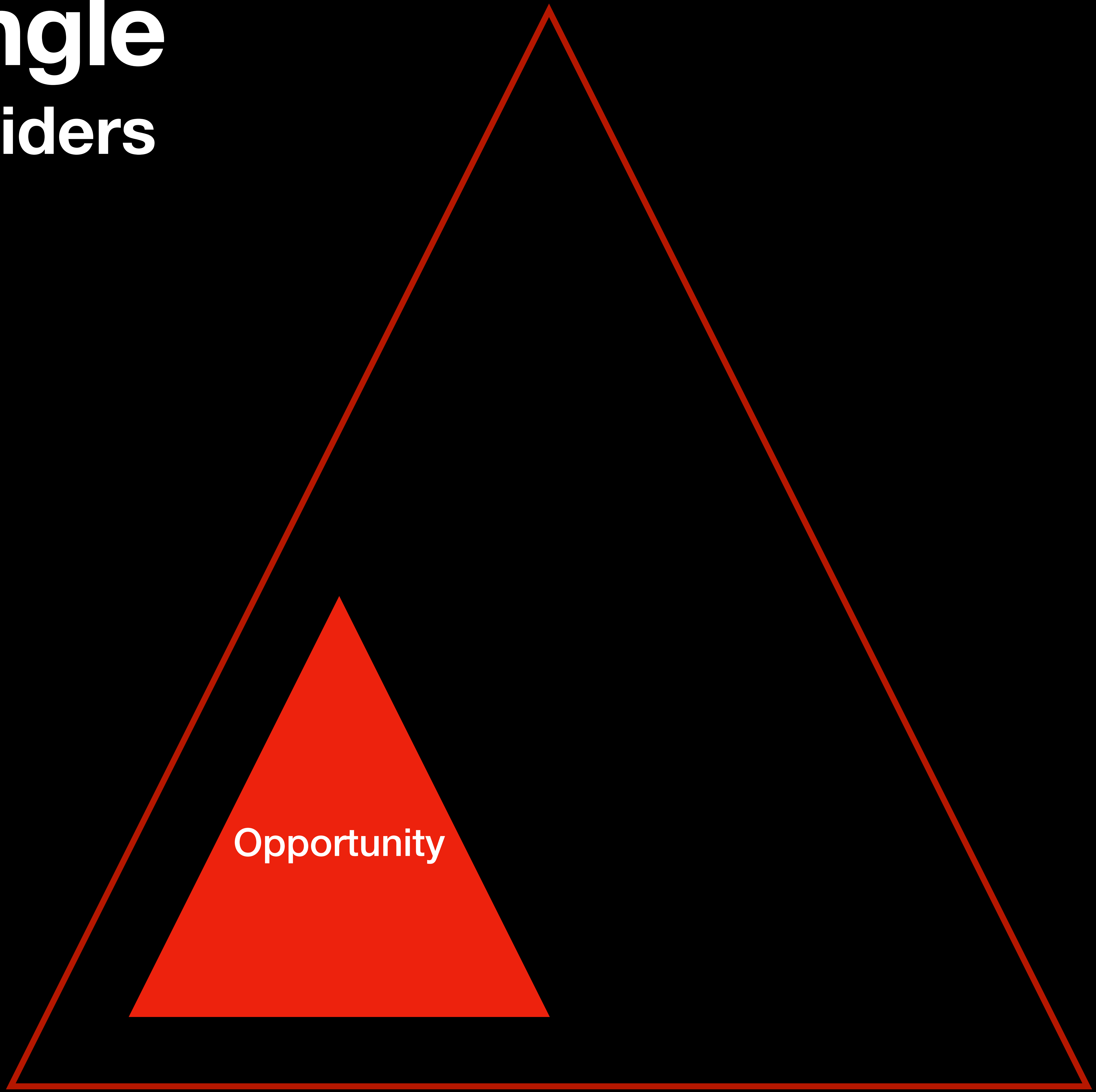
Motivation

Fraud triangle

- Pressure/non-Shareable financial problems
  - Unable to meet obligations
  - Personal failure
  - Business reversals
  - Physical isolation
  - Status gaining
  - Employer-employee relations
- Mostly status seeking or status maintaining

Fraud triangle

Inception of insiders



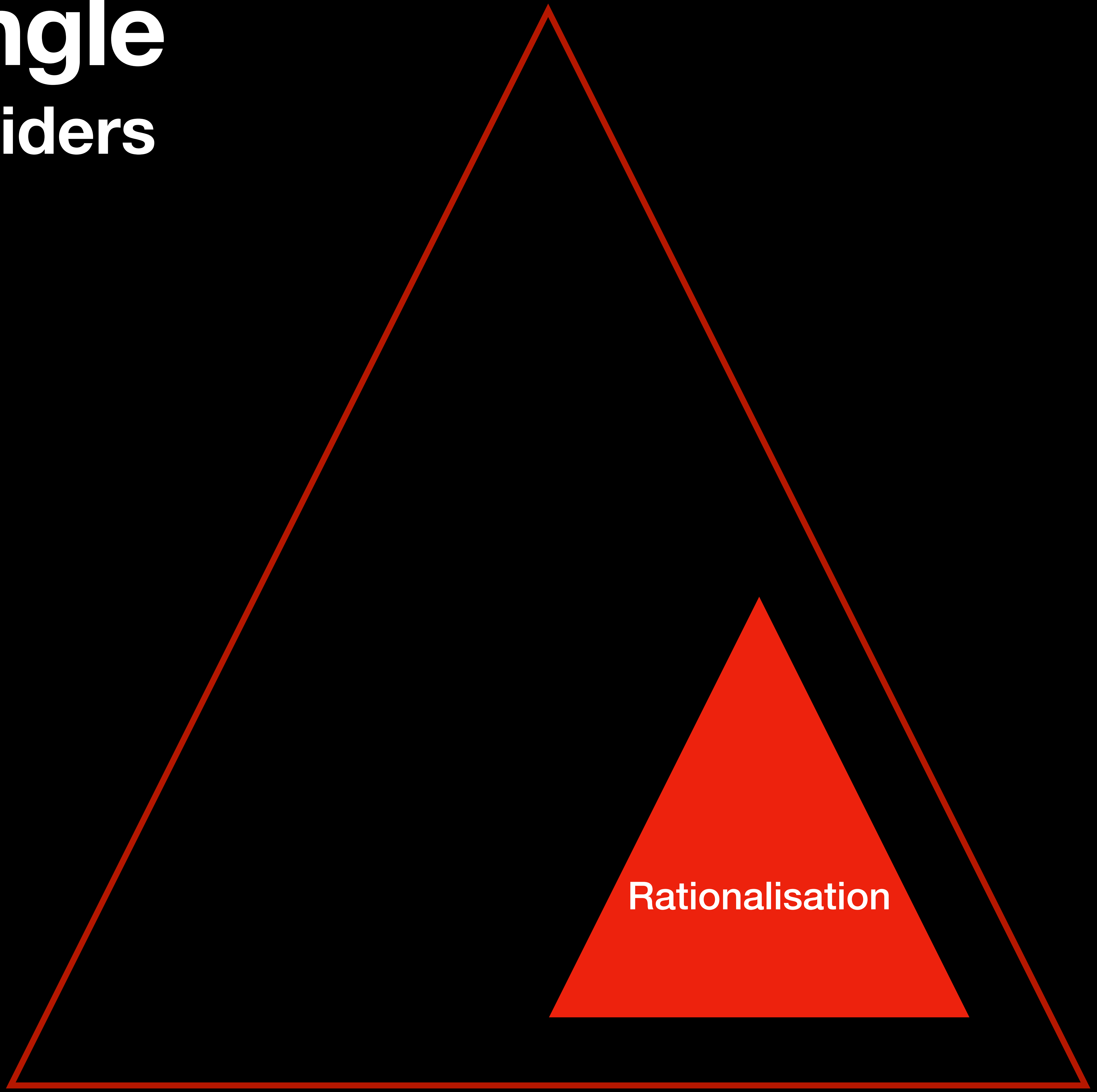
Opportunity

Fraud triangle

- Technical Skills
- Position of trust
- Hearing about other violations
- Getting access to someone else’s password
- Poor Management Practices

Fraud triangle

Inception of insiders



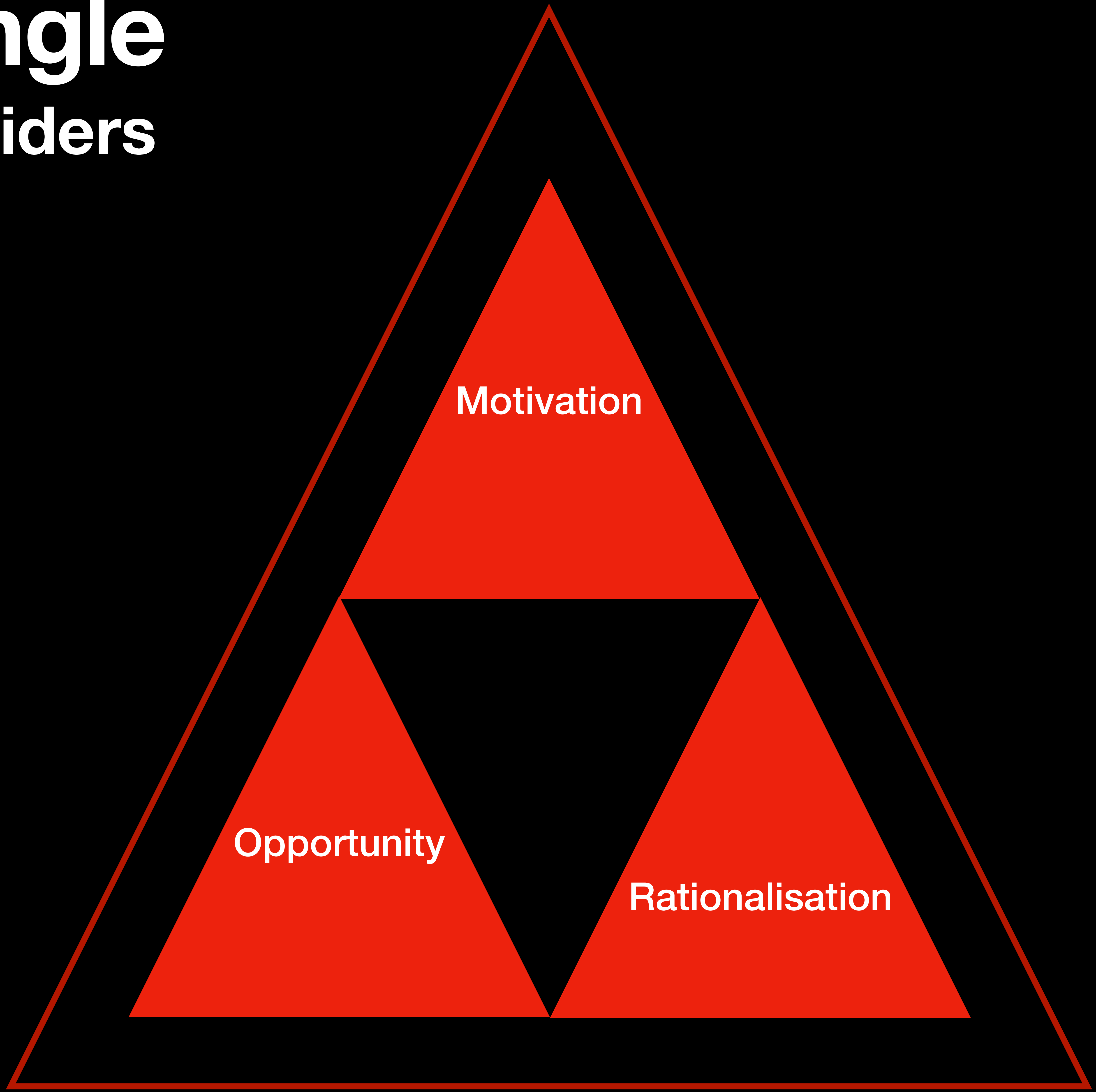
Rationalisation

Fraud triangle

- Insiders view themselves as
    - Non criminal
    - Justified
    - Part of general irresponsibility in the organisation

Fraud triangle

Inception of insiders



Goals

Goals of insiders

Insiders

Fraud

Sabotage

Theft

Mistakes

Fraud

Goals of insiders

- Fraud is a common insider goal with the general aim of fraud for financial gain.

Fraud

Sabotage

Goals of insiders

- Sabotage is a common insider goal among those individuals with technical skills, knowledge and the position to exert change.
- Common attacks could involve privilege escalation techniques, installation of tools and/or malware.

Theft

Goals of insiders

- Theft of assets, for many organisations and enterprises this could be customer data.
- It could also include source code and intellectual property, ultimately insiders could use authorised access to steal assets belonging to organisations.

Mistakes

Goals of insiders

- **Trusted individuals** that have **authorised access** to systems, services and assets that cause **harm to those assets**, but **without malicious intent.**

Mistakes

Goals of insiders

Insiders

Fraud

Sabotage

Theft

Mistakes

Common insider attacks

Common insider attacks

Insiders

Privilege Escalation

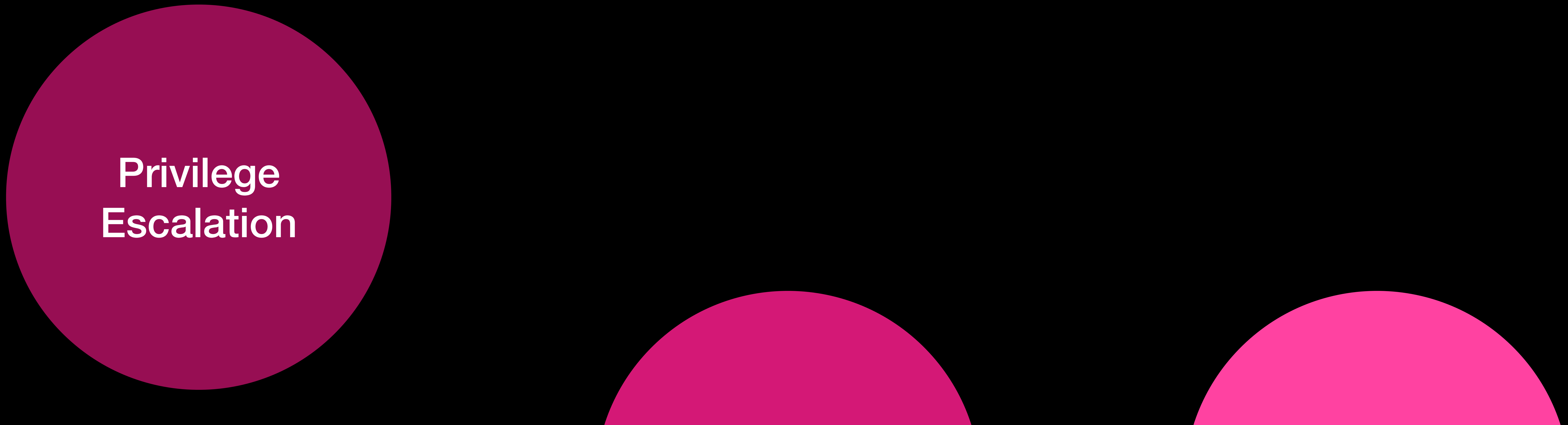
Exfiltration Attacks

Phishing

Privilege Escalation

Common insider attacks

- Compromise and misuse of authorised access, either through horizontal privilege escalation or vertical privilege escalation.



Privilege Escalation

Exfiltration Attacks

Common insider attacks

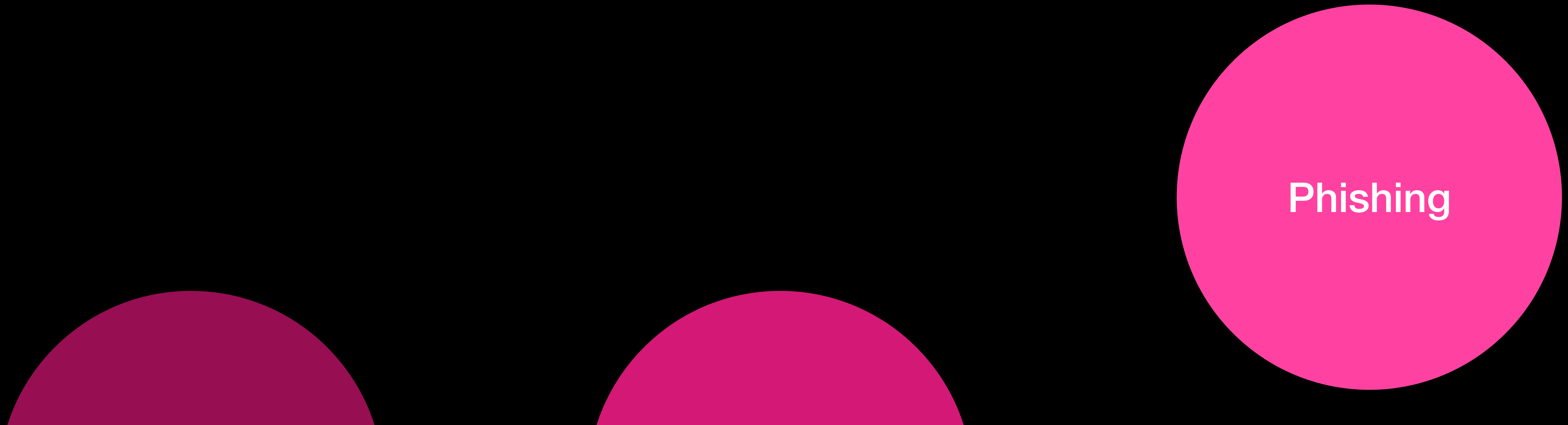
- Transfer of assets outside the perimeter of the organisation as to profit or gain from those assets.

Exfiltration Attacks

Phishing

Common insider attacks

- Utilise false communications within an organisation to expand control to other systems or launch attacks.



Phishing

Common insider attacks

Insiders

Privilege Escalation

Exfiltration Attacks

Phishing

Insiders

Adversarial Behaviours

- Enterprises and other organisation are usually good at securing their organisation against **external threats**.
- Enterprises and other organisations **often neglect** the internal threat of employees performing non-malicious and malicious actions.

Insiders

Adversarial Behaviours