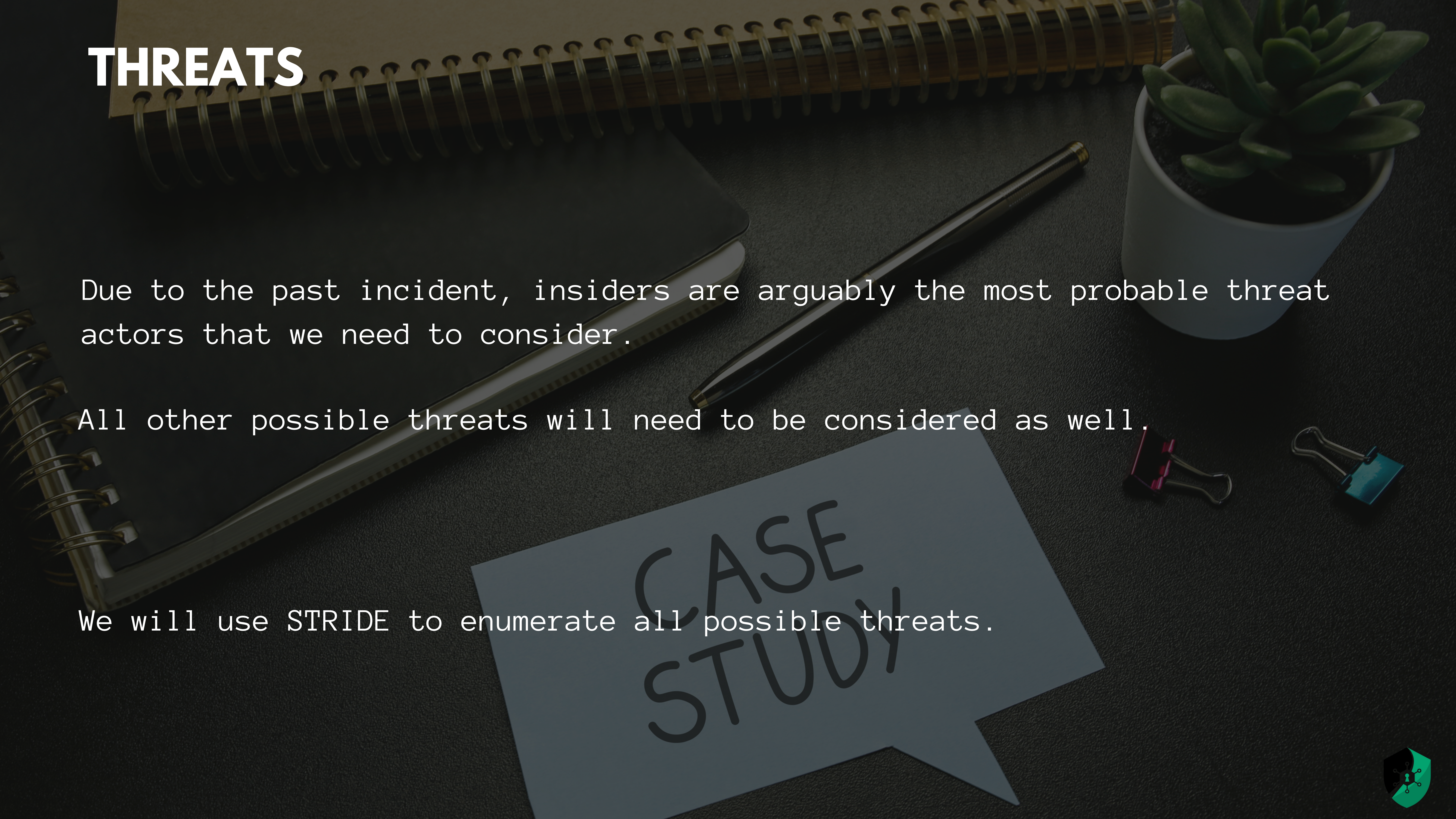
THREAT MODELLING

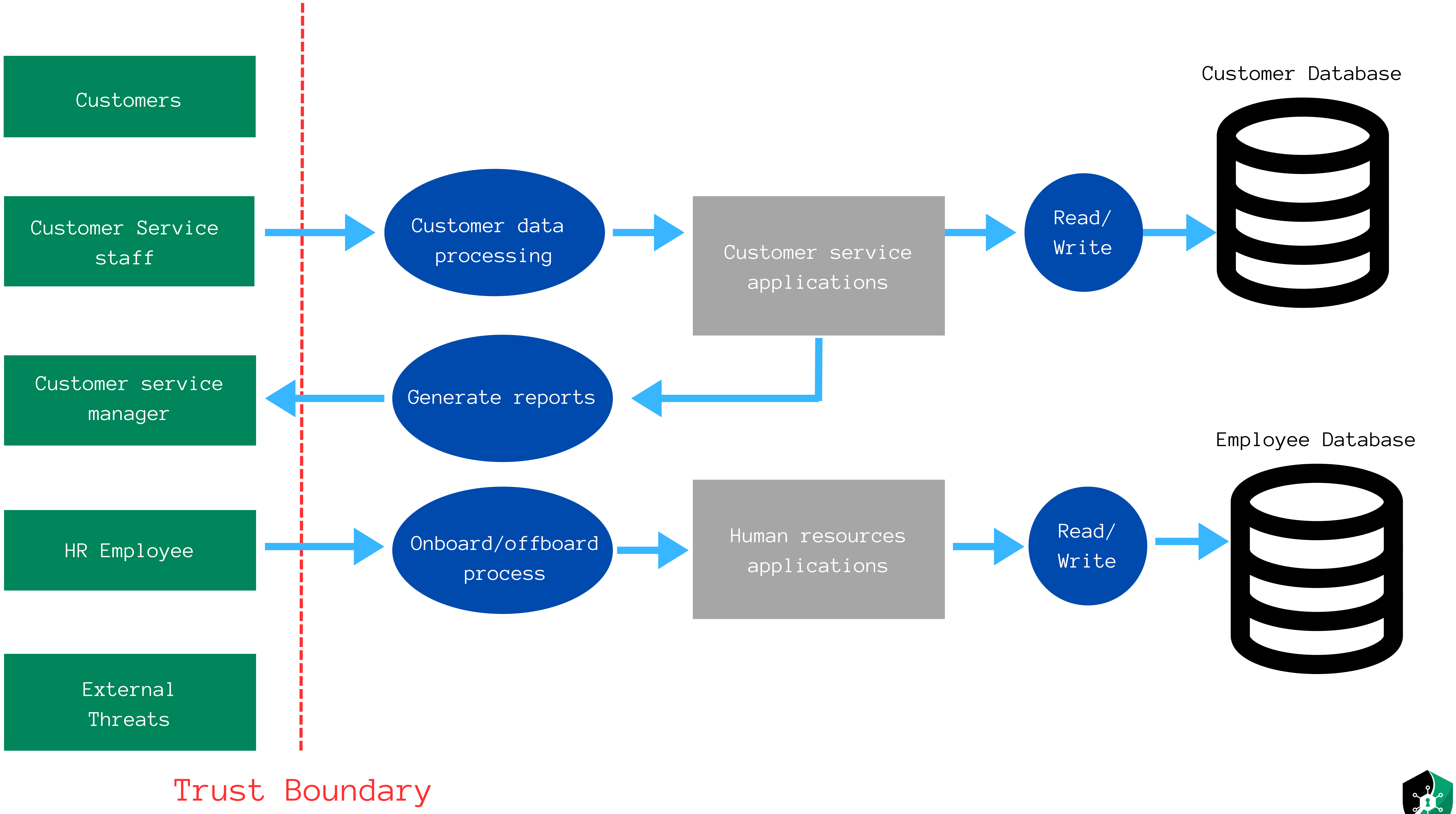
THREATS

Due to the past incident, insiders are arguably the most probable threat actors that we need to consider.

All other possible threats will need to be considered as well.

We will use STRIDE to enumerate all possible threats.





Customers

Customer Service staff

Customer service manager

HR Employee

External Threats

Customer data processing

Generate reports

Onboard/offboard process

Customer service applications

Human resources applications

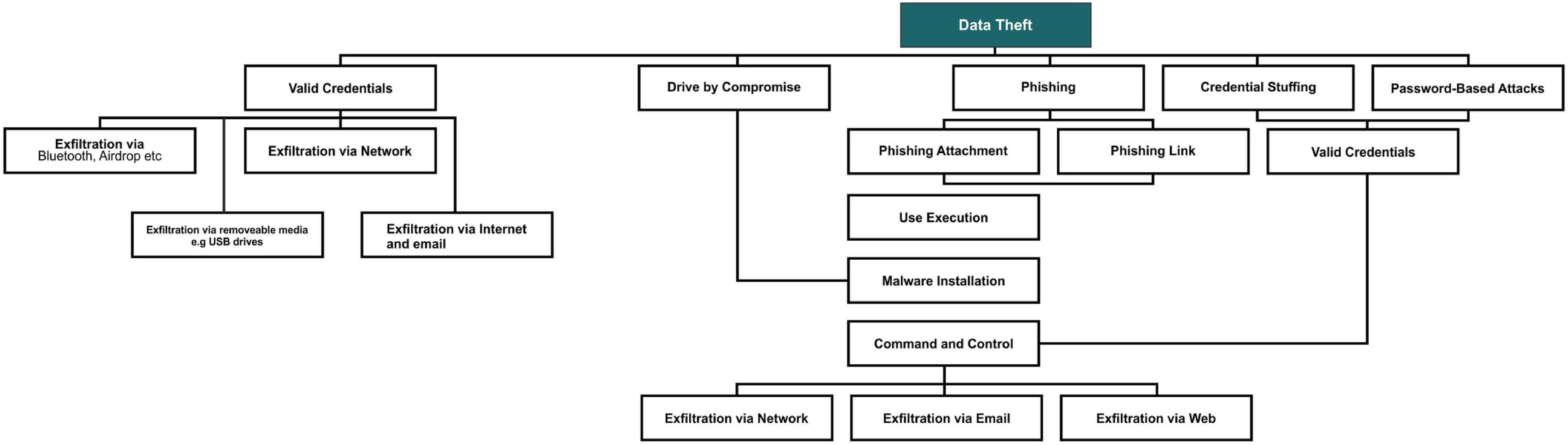
Read/ Write

Read/ Write

Customer Database

Employee Database

Trust Boundary


Data Theft
Valid Credentials
Drive by Compromise
Phishing
Credential Stuffing
Password-Based Attacks
Exfiltration via
Bluetooth, Airdrop etc
Exfiltration via Network
Phishing Attachment
Phishing Link
Valid Credentials
Exfiltration via removeable media
e.g USB drives
Exfiltration via Internet
and email
Use Execution
Malware Installation
Command and Control
Exfiltration via Network
Exfiltration via Email
Exfiltration via Web

THREAT ENUMERATION

Threat Actor	Threats	Likelihood	Impact
Internal	Use valid credentials to exfiltrate data via removable media	HIGH	HIGH
Internal	Use valid credentials to exfiltrate data via internet & email	HIGH	HIGH
Internal	Use valid credentials to exfiltrate data through network	LOW	HIGH
Internal	Use valid credentials to exfiltrate data via bluetooth etc	LOW	HIGH
External	Drive-by compromise leading to data exfiltration	MEDIUM	HIGH
External	Phishing attack leading to data exfiltration	LOW	HIGH
External	Credential stuffing attack leading to data exfiltration	LOW	HIGH
External	Password-based attack leading to data exfiltration	LOW	HIGH

THREAT ENUMERATION

Threats	Likelihood	Impact	Risk Score
Use valid credentials to exfiltrate data via removable media	HIGH	HIGH	**HIGH**
Use valid credentials to exfiltrate data via internet & email	HIGH	HIGH	**HIGH**
Use valid credentials to exfiltrate data through network	LOW	HIGH	MEDIUM
Use valid credentials to exfiltrate data via bluetooth etc	LOW	HIGH	MEDIUM
Drive-by compromise leading to data exfiltration	MEDIUM	HIGH	**HIGH**
Phishing attack leading to data exfiltration	LOW	HIGH	MEDIUM
Credential stuffing attack leading to data exfiltration	LOW	HIGH	MEDIUM
Password-based attack leading to data exfiltration	LOW	HIGH	MEDIUM

THREAT ENUMERATION

REFERENCE	Risks	Risk Score
P.RISK.1	Use valid credentials to exfiltrate data via removable media	HIGH
P.RISK.2	Use valid credentials to exfiltrate data via internet & email	HIGH
P.RISK 3	Drive-by compromise leading to data exfiltration	HIGH