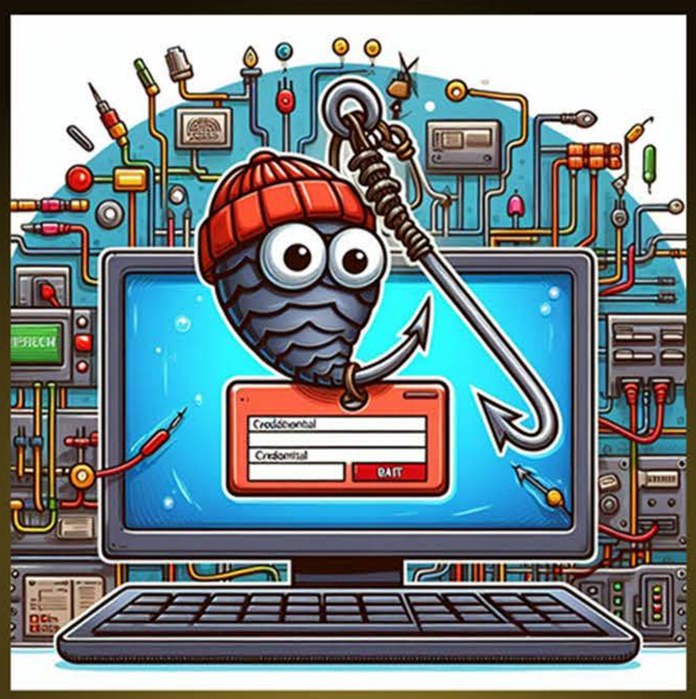
Back Door Attack Card

Requirement:
Hacker Laptop, Penetration Specialist,
Port Scanner, Malware Developer Kit.
A Back Door is when hackers install a secret way to access your stsyems at will without you finding out.
Impact:
There's only one way to mitigate a back door, repatch your systems. It costs 75,000. and you lose 3 reputation.
A Back Door is a persistant threat. If it is not mitigated you suffer Data Exfiltration, Credential Harvest at the end of your next turn.

Credential Harvesting Attack Card



Requirement:
Hacker Laptop, OSINT Officer or Penetration Specialist

Credential Harvesting can take many forms from hackers stealing passwords, Phishing Campaigns, to hackers buying lists of credentials from the dark web.
Impact:
If Credential Harvesting is successful lose 15,000 in costs and lose 1 reputation.
Return Credential Harvesting to the Attack Pile at the end of the turn.

Data Exfiltration Attack Card

Requirement:
Hacker Laptop, C2 Server, Malware

Data exfiltration is when someone secretly steals important information from a computer or website without permission.

Impact:
If Data exfiltration is successful the the Blue Team must pay 30,000 in costs and lose 2 reputation.

Distributed Denial of Service (DDOS) Attack Card

Requirement:
Hacker Laptop, Command and Control Server (C2), Botnet.
DDOS Attacks take place when an adversary floods your systems with large amounts of traffic from multple sources hoping to overwhelm the system.
Impact:
If DDOS Attack is successful the the Blue Team must pay 30,000 in costs and lose 2 reputation.
A DDOS Attack is persistant and remains in play until mitigated.

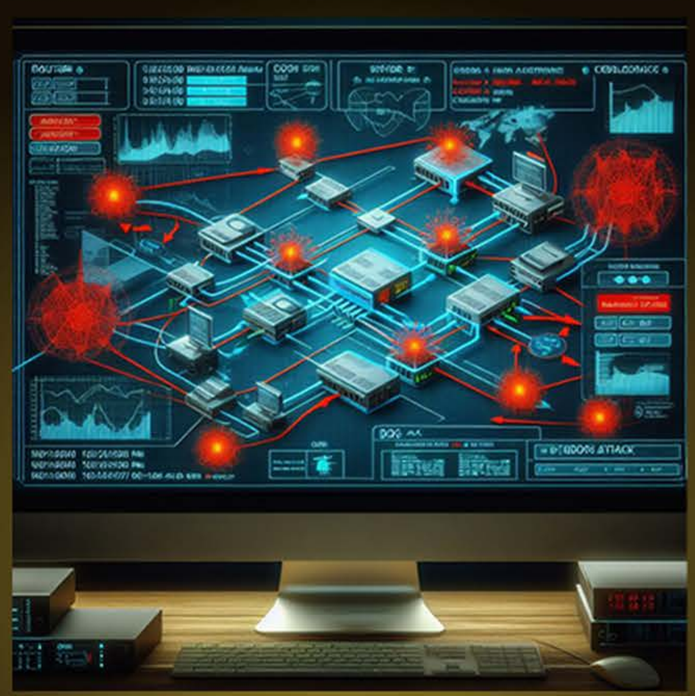
UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Denial of Service (DOS) Attack Card



Requirement:
Hacker Laptop, Command and Control Server (C2)

DOS Attacks take place when an adversary floods your systems with large amounts of traffic hoping to crash the system.

Impact:
If DOS Attack is successful the the Blue Team must pay 20,000 in costs and lose 1 reputation.
A DOS Attack is persistant and remains in play until mitigated.

Insider Threat Attack Card

Requirement:
Social Engineering Expert, OSINT Officer, Rubber Ducky

Exploit or manipulate an insider within the Blue Team to gain unauthorised access.

Impact:
If Insider Threat is successful then the Blue Team must pay 40,000 in legal costs and lose 2 reputation

Once Insider Threat has been played remove it from the game.

Malware Attack Card

Requirement:
Hacker Laptop, Malware Developer Kit,
Network Intrusion or Phishing email.

Malware is malicious code that enables hackers to do a number of things from spy on your network, exfiltrate data or deliver ransomware.

Impact:
If Malware is successful lose 20,000 in clean up costs and lose 1 reputation.

Network Intrusion Attack Card

Requirement:
Hacker Laptop, Penetration Specialist,
Port Scanner.

Network inrusion is what we all think of when someobe say 'You've been hacked', Unaathourised access to your computers..

Impact:
If network instrusion is not mitigated
It costs 20,000 and you lose 1 reputation.
A Network Intrusion is a persistant threat. If it is not mitiigated by the end of your turn you suffer
Data Exfil. at the start of your next turn.

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Phishing Campaign Attack Card

Requirement:
Phishing Emails, Social Engineering Expert, OSINT Officer

Uses tailored phishing emails to deceive Blue Team members into compromising security, a fundamental cyber tactic.

Impact:
If Phishing Campiagn is successful then the Blue Team must pay 25,000 in staff awarenesss training and lose 1 reputation

Randsomware Attack Card

Requirement:
Hacker Laptop, Malware Developer Kit,
Phishing Emails.
Ransomware encypts and locks all your data so cyber criminals can extort a ransom to unlock it.
Impact:
If Ransomware is not mitigated
It costs 50,000 and you lose 3 reputation.
Ransomware is a persistant threat. You suffer the impact at the end of each turn until it is mitigated.

SQL Injection Attack Card

Requirement:
Hacker Laptop

SQL Injection tricks a website into spilling secrets by sneaking in commands where it shouldn't.

Impact:
If SQL Injection Attack is successful the Blue Team suffers 10,000 in damages, and lose 1 reputation.

Supply Chain Hack Attack Card

Requirement:
Hacker Laptop, Malware Developer Kit,
Phishing Emails or Rubber Ducky
A supply chain hack occurs when someone targets one of your the suppliers that are critical to the operation of your business.
Impact:
If Supply Chain Hack is successful, you lose one of your Business Contracts. The Red Team can choose their target. in singple player the Blue Team can choose.
Loose Capital and Reputation equal to the contracts benefits.

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Data Backups
Blue Team Asset

Cost: 10,000
Requirements: SOC Analyst, Cloud Services.

Cloud services provide storage, computing power, and applications over the internet, offering flexibility, scalability, and efficiency for users and businesses.
Mitigates:
Ransomware Attack.

Cloud Services
Blue Team Asset

Cost: 20,000
Requirements: DMZ, Web Server, SOC Analyst

Cloud services provide storage, computing power, and applications over the internet, offering flexibility, scalability, and efficiency for users and businesses.
Mitigates:
Denial of Service (DOS),
Distributed Denial of Service (DDOS).

Demilitarised Zone (DMZ)
Blue Team Asset

Cost: 15,000
Requirements: SOC Analyst, Firewall

A DMZ is a safe area between your network and the internet, where you can place public services without risking internal security.

Mitigates:
Network Intrusion,
Denial of Service Attack (DOS).

Firewall
Blue Team Asset

Cost: 10,000
Requirements: Start Up

A firewall acts like a security guard for your computer network,
deciding who gets in or out to keep it safe.
Mitigates:
Network Scans, Network Intrusion

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Honey Pot
Blue Team Asset

Cost: 15,000
Requirement: SOC Analyst, DMZ.
A Honey Pot is a fake network environment designed to trick hackers.
Mitigates:
Network Intrusion,Data Exfiltration, Randsomware Attack, Malware Attack.
Once a Honey Pot is deployed to mitigate an attack return it to your Asset pile.

Intrusion Detection System (IDS)
Blue Team Asset

Cost: 15,000
Requirements: Start Up

An IDS monitors network activity like a spy, watching for unusual behaviour or attacks, and alerts when something's amiss.
Mitigates:
Malware Attack, Network Intrusion

Incident Response Manager
Blue Team Asset

Cost: 50,000
Requirement: N/A
Incident Responders specialise in neutralising successful cyber attacks. Getting your business up and running as quickly as possible.
Mitigates:
Reduces the financial damage of a successful attack by 50%. Reduces Reputation damage by 1.

Intrusion Prevention System (IPS)
Blue Team Asset

Cost: 15,000
Requirement: Start Up

An Intrusion Prevention System (IPS) blocks hackers and viruses instantly, acting like an automatic gatekeeper for your network's safety.
Mitigates:
Network Intrusion, Network Scan

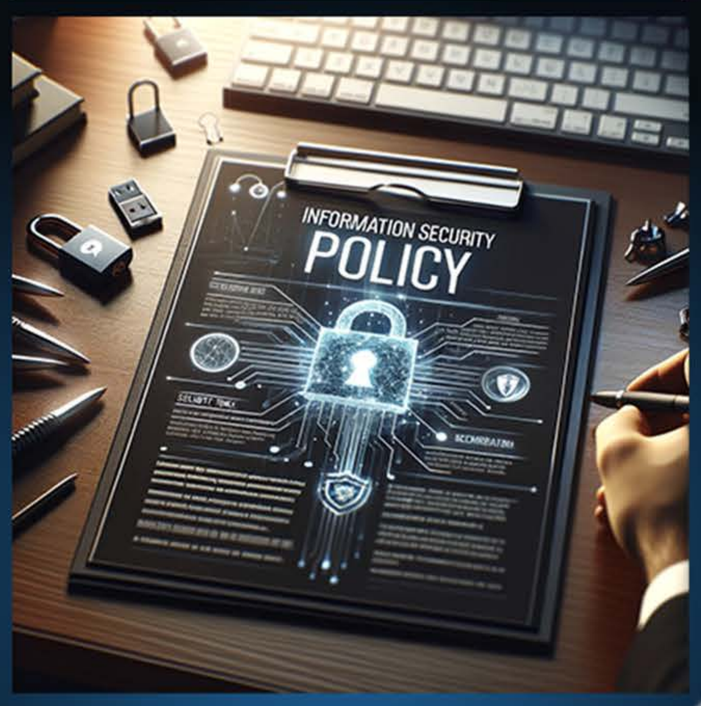
UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Regulation and Legal Compliance
Blue Team Asset



Cost: 40,000
Security Manager is turned face down for 1 round
Requirements:
Security Manager
Cybersecurity regulations ensure companies protect data
and networks, complying with laws
to avoid breaches, fines, and maintain customer trust.
Mitigates:
Insider Threat.

Security Operations Center Manager
Blue Team Asset

Cost: 60,000
Requirement: SOC Analyst

A Security Operations Center Manager is responsible
for assessing threats and managing responses.
Mitigates:
A SOC Manager canbe turned in a SOC,
and mitigate any attack.
If you do this then turn this card face down
and it is inactive for 1 turn.

Security Information and Event Management (SIEM)
Blue Team Asset

Cost: 40,000
Requirements: Security Manager

SIEM combines security info and event logs,
analysing them to identify threats,
ensuring quick response to protect your network's security.
Mitigates:
Supply Chain Attack, Insider Threat,
Data Exfiltration.

Security Operations Centre (SOC)
Blue Team Asset

Cost: 150,000
Requirements: Security Manager, DMZ, Firewall, IDS or IPS
SOC Analyst

A SOC is a team using advanced tools to monitor, detect,
and respond to cybersecurity threats in real-time.

Mitigates:
All known attacks.

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Security Operations Centre (SOC) Analyst. Blue Team Asset.

Cost: 40,000
Requirements: Start Up

A SOC Analyst is a your first line of defence. Tasked with monitoring network activity for abnormal or malicious activity

Mitigates:
Once per game your SOC analyst can be used to mitigate any attack.

Third Party Support Contract Blue Team Asset

Cost: 30,000
Requirements: Incident Response Manager

Sometimes no matter what you do it isn't enough. Third Party Support helps you when you need it the most

Mitigates:
Denial of Service (DOS), Distributed Denial of Service (DDOS), Ransomeware.

Web Server Blue Team Asset

Cost: 10,000
Requirements: Firewall, IPS or IDS

A web server hosts web services, serving pages to visitors over the internet upon their request.

Mitigates:
SQL Injection

Financial/Banking Security Contract Blue Team Contract

Requirement:
Security Manager. SIEM, Regulation and Legal Compliance.

Bonus: You gain 4 reputation and 100,000 for securing this contract.

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Corporate Services Contract
Blue Team Contract

Requirement:
SOC Analyst, SIEM, Security Manager or Incident Response Manager

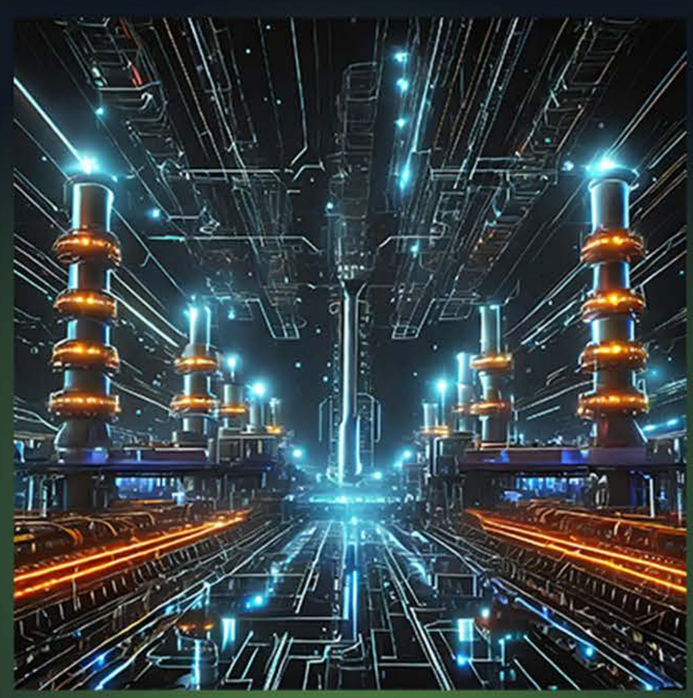
Bonus: You gain 4 reputation and 75,000 for securing this contract.

Education Contract
Blue Team Contract

Requirement:
SOC Analyst, Firewall

Bonus: You gain 1 reputation and 35,000 for securing this contract.

Energy Contract
Blue Team Contract



Requirement:
Regulation and Legal Compliance, SIEM, Security Manager.

Bonus: You gain 2 reputation and 50,000 for securing this contract.

FinTech Contract
Blue Team Contract

Requirement:
Regulation and Legal Compliance, Incident Response Manager, Data Backups.

Bonus: You gain 3 reputation and 60,000 for securing this contract.

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Food Security Contract
Blue Team Contract

Requirement:
SOC Analyst, DMZ, Web Server

Bonus: You gain 1 reputation and 40,000 for securing this contract.

Government Contract
Blue Team Contract

Requirement:
Regulation and Legal Compliance, Incident Response Manager, SIEM.

Bonus: You gain 3 reputation and 80,000 for securing this contract.

Healthcare Contract
Blue Team Contract

Requirement:
SOC Analyst, SIEM, Third Party Support Contract

Bonus: You gain 1 reputation and 15,000 for securing this contract.

Multimedia Contract
Blue Team Contract

Requirement:
Firewall, IDS or IPS

Bonus: You gain 1 reputation and 30,000 for securing this contract.

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Pharmacuetical Contract
Blue Team Contract

Requirement:
SOC Analyst, IDS, Firewall

Bonus: You gain 1 reputation and 35,000 for securing this contract.

Telecommunications Contract
Blue Team Contract

Requirement:
Firewall, IPS and Back Ups

Bonus: You gain 2 reputation and 50,000 for securing this contract.

Transport Contract
Blue Team Contract

Requirement:
SOC Analyst, Web Server,
Back Ups

Bonus: You gain 2 reputation and 40,000 for securing this contract.

Faiza Ahmed
CISO Card

Chief Information Security Officer:
Faiza Ahmed

Background:
Faiza is an expert coder, and comes from with a wealth of knowledge in Malware design and mitigation. She offers expert skills in protecting your team from malware based threats.

Benefit:
Faiza's reputation gains you 1 extra reputation at the start of the game. You automatically mitigate the Malware Attack Card.

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

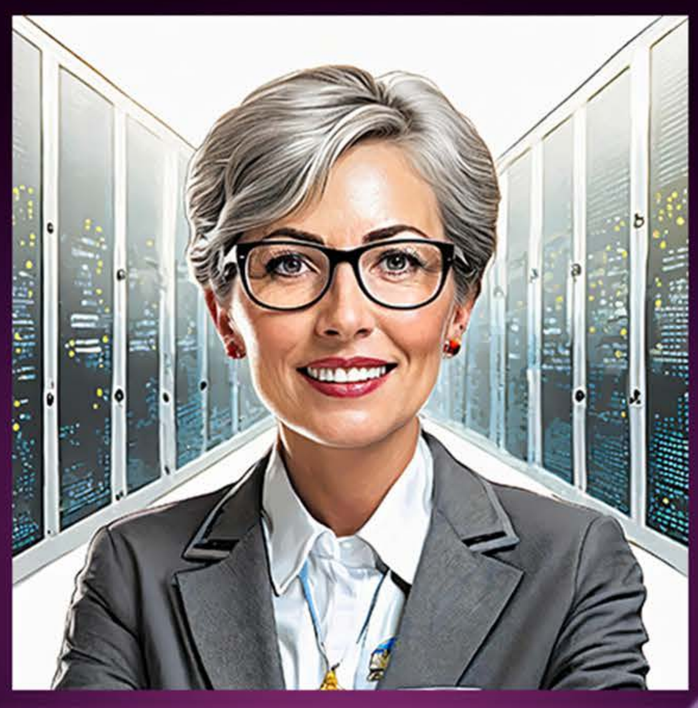
UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Gemma Yang
CISO Card

Chief Information Security Officer:
Gemma Yang
Background:
Gemma began her career as a SOC Analyst and has worked her way up through the ranks of Security Engineer and Security Manager. With a wealth of technical and industrial experience she is expertly placed to support your team.
Benefit:
Gemma's experience gains you 1 extra reputation at the start of the game. Like the Security Manager she can be used to mitigate an attack.

Helena Cartwright
CISO Card



Chief Information Security Officer:
Helena Cartwright
Background:
Helena comes from the financial sector and specialises in cyber fraud, and financial risk management. Her reputation is one of a skilled negotiator.
Benefit:
Helena's reputation gains you 1 reputation at the start of the game. Should you be declared bankrupt Helena will negotiate 20,000 in investment once per game.

Ioshi Yakimata
CISO Card

Chief Information Security Officer:
Ioshi Yakimata

Background:
Ioshi is a rising star of the industry, one of the youngest CISO's around, he has a glow reputation for security governance and administration.
Benefit:
Ioshi's reputation gains you 2 extra reputation at the start of the game. Start the game with Regulation and Legal Compliance Contract.

Namdi Ubaka
CISO Card

Chief Information Security Officer:
Namdi Ubaka
Background:
Namdi began his career in business administration and project management. Moving to cyber security later in his career. He's an excellent co-ordinator and well respected across many business sectors.
Benefit:
Namdi's reputation gains you 1 reputation at the start of the game, additionally you gain an additional 5000 for each contract you gain.

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Rajiv Sharma
CISO Card

Chief Information Security Officer:
Rajiv Sharma

Background:
Rajiv is a tech entrepeneur, with a proven track record of successful start ups and has a genuine drive and passion to help your team..
Benefit:
Rajiv's reputation gains you 2 extra reputation at the start of the game. Additionally, you may choose one tech start up asset for free at the start of the game.

Botnet
Red Team Asset

Cost: 20,000
Requirements:
Hacker Laptop, Command and Control (C2) Server

A botnet is a network of hacked/infected computers and devices that hackers use to launch large scale attacks.

Launches: Distributed Denial of Service (DDOS) Attack

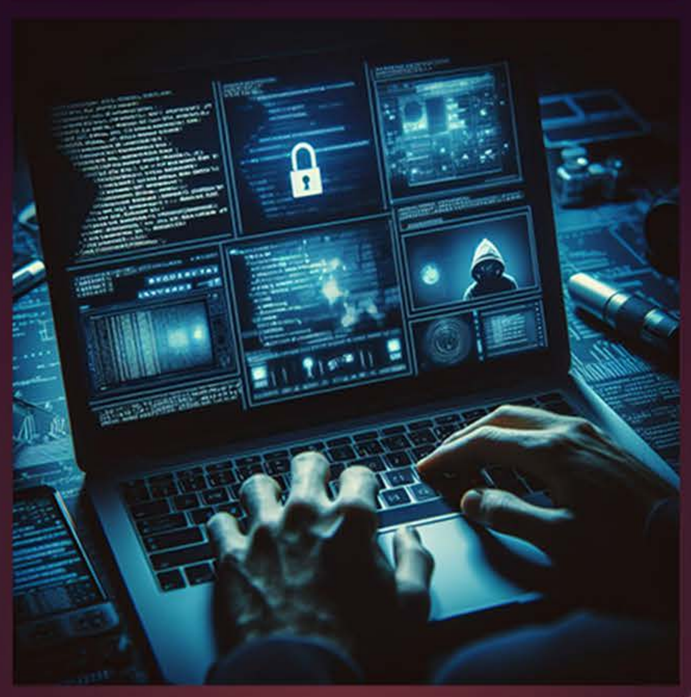
Command and Control (C2) Server
Red Team Asset

Cost: 15,000
Requirements: Startup Asset

A C2 Server is used by hackers to maintain persistance over networks they compromise. Allowing to regain access and deliver malicious payloads.

Launches:
DDOS Attack, DOS Attack, Ransomware, Data Exfiltration.

Hacker Laptop
Red Team Asset



Cost: 15,000
Requirements:
Startup Asset

A hackers laptop is the weapon from which they cause all their chaos. It's often covered in stickers!.

Launches:
SQL Injection, Malware, Phishing Email Campaigh
Network Intrusion.

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Malware Developer Kit
Red Team Asset

Cost: 20,000
Requirements:
Hacker Laptop, Penetration Specialist
A Malware Developer Kit helps hackers write all that malicious code that infects the internet.

Launches:
Malware, Ransomware

Open Source Intelligence Officer (OSINT)
Red Team Asset

Cost: 40,000
Requirements:
Startup Asset
An OSINT Officer speciallises in browsing the internet gathering intelligence on their targets from websites, forums, and even the dark web.

Launches:
Credential Harvesting, Insider Threat, Phishing Campaign.

Penetration Specialist
Red Team Asset

Cost: 55,000
Requirements:
Hacker Laptop, Cammand & Control (C2) Server

A Penetration Specialist is your typical hacker, someone the specialised in hacking into computers.

Launches:
Credential Harvest, Network Intrusion, Back Door

Phishing Email
Red Team Asset

Cost: 15,000
Requirements:
Hacker Laptop, Social Engineer

Social Engineers use Phishing Emails that are disguised to look like genuine emails, to trick people to clicking on links and downloading malware without them knowing.
Launches:
Phishing Email Campiagn, Credential Harvesting.

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Port Scanner
Red Team Asset

Cost: 10,000
Requirements: Startup Asset

Port Scanners are software applications that scan computers, networks and the internet looking for open ports. Ports are like doors that grant access to a computer.

Remote Access Tool
Red Team Asset

Cost: 10,000
Requirements:
Hacker Laptop

A remote access tool is a piece of software that allows hackers to connect to other peoples computers.

Launches:
Network Intrusion, Back Door

Rubber Ducky/
Bad USB
Red Team Asset

Cost: 5,000
Requirements: N/A

A Rubber Ducky or Bad USB is a USB drive loaded with Malware or Trojan's that hackers leave lying around for people to unwittingly plug in and infect their systems.

Launches:
Insider Threat, Malware Attack

Socieal Engineer
Red Team Asset

Cost: 60,000
Requirements:
OSINT Officer
Social Engineers specialise in performing developing target profiles, and figuring out how to mamipulate people into doing things they want.

Launches:
Phishing Email Campiagn, Credential Harvesting
Insider Threat.

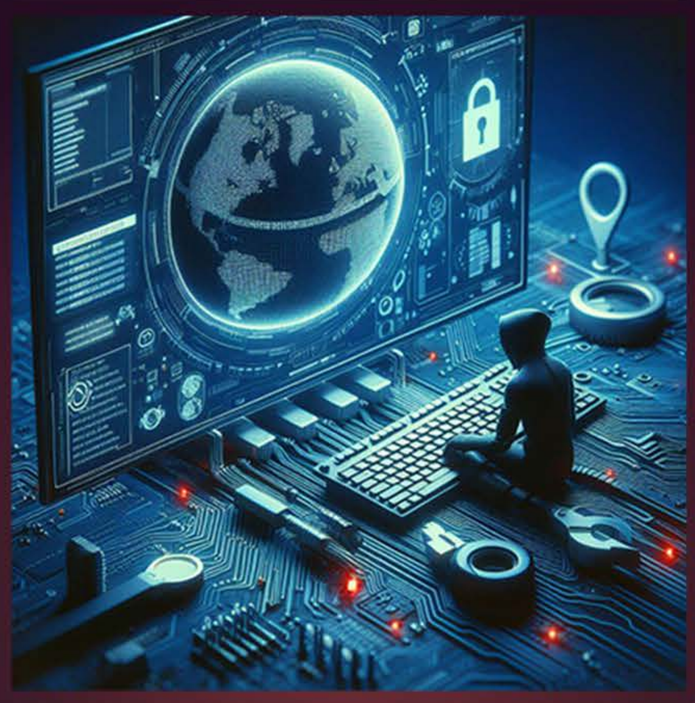
UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

UWE Bristol
UWEcyber

Vulnerability Scanner
Red Team Asset



Cost: 20,000
Requirements:
N/A
A vulnerability scanner allows a hacker to assess potential weaknesses in your system configuration.

Launches:
Tap your Vulnerability Scanner horizontal to activate whilst running it negates Firewalls, unless The Blue Team have RLC.

UWE
Bristol
UWEcyber