Threat Personas

Output from the Threat Personas and Application Vulnerability Scoring Model session at #OSS2020

https://open-security-summit.org/

OPEN SECURITY SUMMIT

Threat Personas

Group	Persona name
Breakout Room 1	Vladimir Starsky: Hacker for Hire
Breakout Room 2	Leona Wolff: Cyber Criminal
Breakout Room 3	<Please complete for your group>
Breakout Room 4	APT Customer
Breakout Room 5	Dimitra: DevOps Engineer
Breakout Room 6	<Please complete for your group>
Breakout Room 7	<Please complete for your group>
Breakout Room 8	<Please complete for your group>
Breakout Room 9	<Please complete for your group>
Breakout Room 10	<Please complete for your group>

🤷‍♂️ WHAT AM I MEANT TO BE DOING?

You've been split into groups 🥳

Each *Breakout Room* has a template to populate from the list on the left 📝

1. Give your persona a name
(👈 and add it to the table)
2. Discuss and write their narrative
3. Add a photo

Try not to do the same as another group! ❌

EXAMPLE THREAT PERSONA

External Criminal

EXTERNAL, MALICIOUS

Misha Melnyk is a career criminal who believes himself out of the reach of the authorities although he is careful not to commit crimes in his home country. He has been an active criminal online for about 10 years. He regularly buys exploits on the dark market but is not himself a developer.

EXAMPLE!

GOALS

Personal Gain

OPPORTUNITY

Connected to the Internet

SKILLS

Power User

KNOWLEDGE

External to organisation

DETERRABILITY

Unconcerned criminal

BREAKOUT ROOM 1

Vladimir Starsky: Hacker for Hire

MALICIOUS, EXTERNAL

- Vladimir works in a hardware store. He is also a hacker for hire. Due to poor economical situation of his family he could never attend Computer Science University but is passionate about all things IT. He decided to take his economical situation in his ands and learn how to hack for various dubious characters.

- Financial Motivation
- He is from Oymyakon, Russia
- He works in a hardware store in Oymyakon
  - Financial gains, high mortgage and car payments
  - Angry and frustrated
  - His house, his luxurious car, his wife

GOALS

OPPORTUNITY

Connected to Internet

SKILLS

Developer

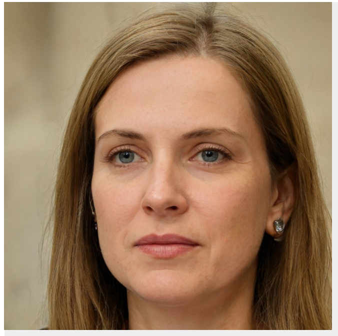
KNOWLEDGE

External to Organisation

DETERRABILITY

Careful Criminal

Leona Wolff: Cyber Criminal



Leona recently took over as head of the notorious Wolff crime family. She knows that shaking down local shop owners for protection money isn't the future: they need to diversify and digitise!

The Wolff's are motivated purely by financial gain and are very happy with their life of crime.

They are protected by 'legitimate' business interests, corrupt lawyers and - in cyberspace - being distant from their victims.

GOALS

Personal Gain

OPPORTUNITY

Connected to Internet

SKILLS

Power User

KNOWLEDGE

External to Organisation

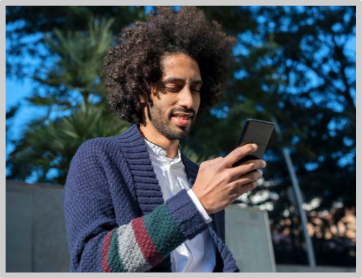
DETERRABILITY

Unconcerned Criminal

BREAKOUT ROOM 4

OPEN SECURITY SUMMIT

APT Customer



thispersondoesnotexist.com

- What is their story?

  The APT customer is a highly skilled individual (offensive security/computer security expert) who may sometimes violate laws or typical ethical standards, but does not have the malicious intent typical of a black hat hacker.

- Why are they a threat?

  He might compromise systems without permission and without scope limitation for the thrill of gaining privileged access into his target. He might not inform their victims that they have been compromised and his goal is to maintain his presence (persistence) into the company systems and networks while going completely unnoticed for the thrill of it. He might even apply security updates to ensure that he's the only attacker who has access to the systems.

  ○ What's their day-job?

  IT Security / Red Teamer

  ○ What motivates them?

  The Challenge: The higher the perceived security of the company is targeting, the more he is engaged.

  ○ Are they happy, angry, sad?

  Bored

  ○ What have they got to lose?

  Anonymity

GOALS

National Interests

OPPORTUNITY

Connected to Internet

SKILLS

Researcher

KNOWLEDGE

Customer

DETERRABILITY

Careful Criminal

OPEN SECURITY SUMMIT

Dimitra: DevOps Engineer

- Greek, DevOps Developer working in Mid-size company.
- Has access to various systems and ability to deploy to prod
- She’s frustrated with hermanager because he doesn’t understand her brilliance. Has got some contacts in the dark web and dabbled with the dark side as a teenager.
- Why are they a threat? -> Too much access and know-how of systems and environments

GOALS

Revenge

OPPORTUNITY

Access to System/Network

SKILLS

Developer

KNOWLEDGE

Employee

DETERRABILITY

Careful Criminal