



ven•r

Philip Törner

Om Philip

- Penetrationstestare
- Security Operation Center
- Ansvarig för säkerheten hemsida för Retailföretag.
- Säkerhetsgranskning
- Utbildar styrelsemedlemmar i IT-säkerhet

Om Venor

- 10 personer 7 konsulter
- Fokuserar på defensiv teknisk säkerhet.
- Spännande kunder trots sin storlek
- Kunniga medarbetare
- Försöker bygga något långsiktigt

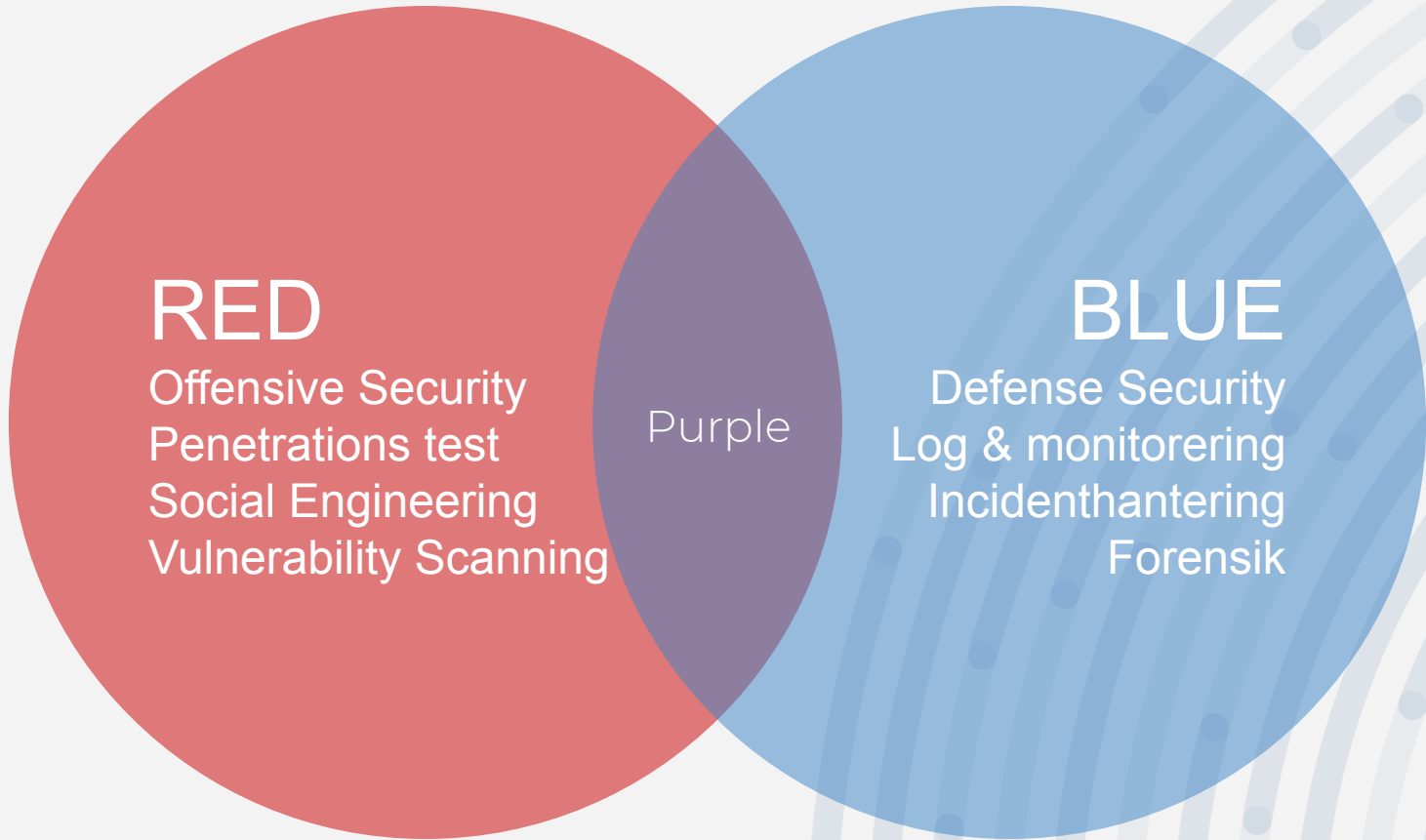
Agenda

- Vad finns det för områden inom IT-säk
- Rött och Blått
- Hackade databaser
- Attacker mot hemsidor
- Vad man som privatperson göra?

IT-säkerhet

Stort område

- Informationssäkerhet
- Säker utveckling / kod
- Penetrationstest
- Sårbarhetskanning
- Övervakning / Larm (SOC)
- Incidenthantering
- ...



RED

Offensive Security
Penetrations test
Social Engineering
Vulnerability Scanning

Purple

BLUE

Defense Security
Log & monitoring
Incidenthantering
Forensik

Attacker

Om man ställer en server på internet hur lång tid tar det innan första anslutningen kommer?

Mindre än 1 min

Hur tar sig en angripare in?

- Email / sätter sig i receptionen
- Klient dator (fotfäste)
- Samlar information
- Attackerar fler i närheten
- Hoppas in på andra servrar
- Exfiltrerar data

Attacker mot hemsidor

- Login (Credential dumping)
- Gift Card
- Checkout

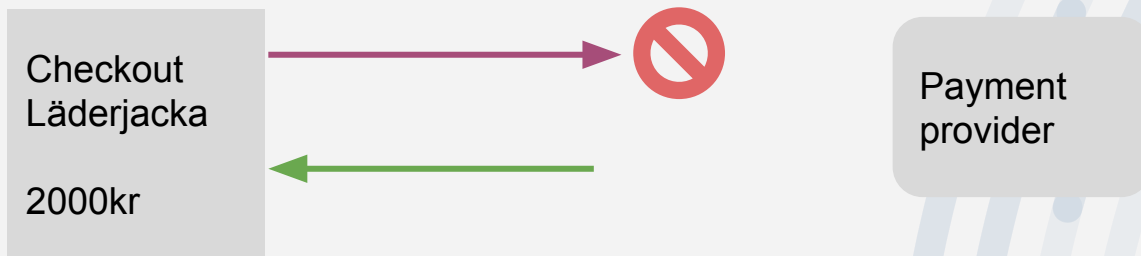
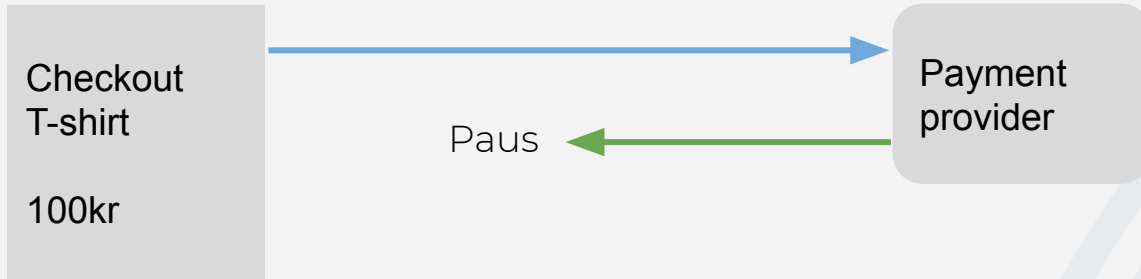
Där det finns pengar att tjäna!



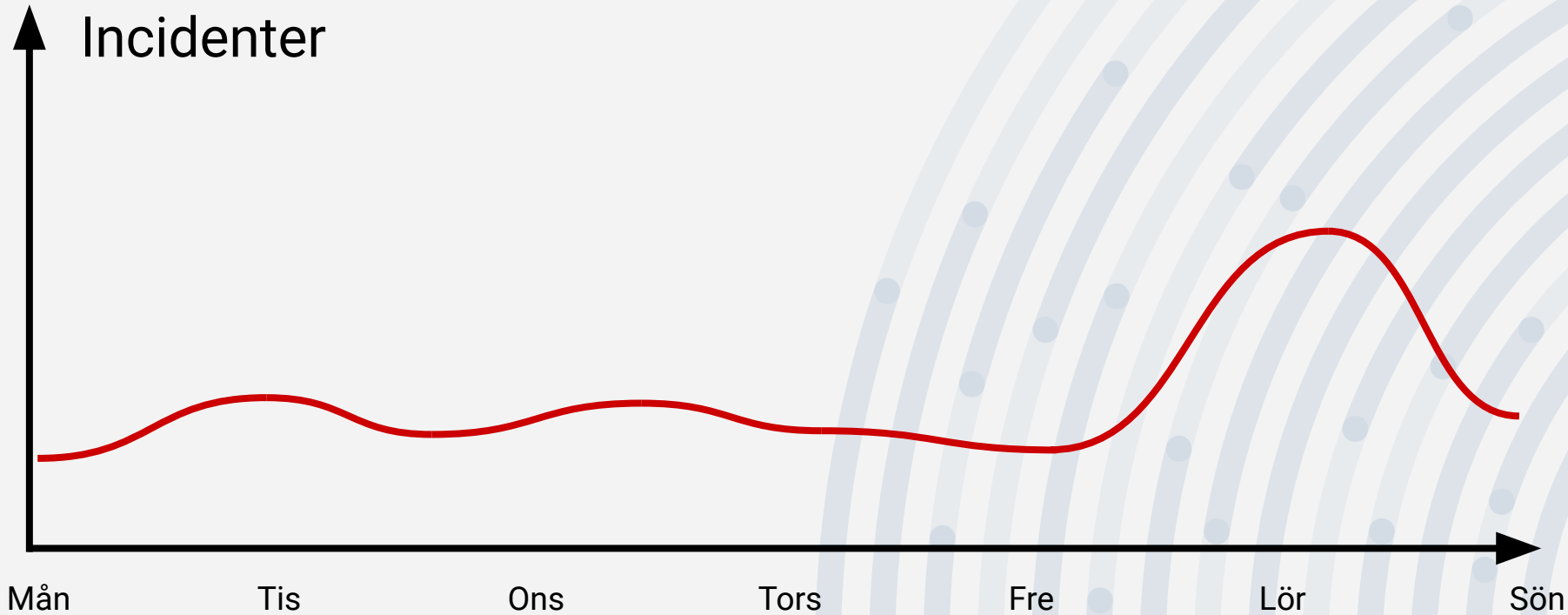
100 kr



2000 kr



Incident Friday!



Stulna databaser

1. Hackerar sig in på en hemsida med dålig säkerhet
2. Själ databasen med användarnamn och lösenord
3. Credential dump mot andra sidor
4. Med lite tur finns sparade kreditkort

Sker oftare än ni tror

Password manager

- Unika lösenord för varje hemsida
- Du behöver bara komma ihåg ett!
- Fyller i automatiskt

1Password, Lastpass, Dashlane,...

Dashlane familjekonto 5 pers 50kr/mån



Thank You