
CyberSecure

CYBERSECURE HALMSTAD

CYBER WAKE-UP CALL

Var med och skapa ett CyberSäkert Halmstad.

Talare - Frukostseminarie 30 Maj 2024

Sanne Femling

IT Security Manager

Resursbank

Caroline Lendowski

Business Continuity
and Risk Consultant

Benify

Edward Wasilchin

Sr. Advisor -
Cybersecurity

Observata

CyberSecure

CyberSecure Halmstad - Mission och Vision

Mission -

Skapa ett CyberSäkert Halmstad för tryggt företagande.

Vi strävar efter att göra Halmstad till en CyberSäker bastion, där företag är cybermedvetna, förberedda och har cybersäkerhet som en självklar del av sin vardagliga verksamhet.

CyberSecure Halmstad - Uppgift och roll

Utbilda

Vi stärker företag med kunskap, medvetenhet och metodik gällande cybersäkerhet.

Samverka

Vi bygger en kollektiv säkerhetskultur genom aktiva samarbeten.

Rådgöra

Vi erbjuder expertstöd, kompetens och råd i cybersäkerhetsfrågor och regelverk.

Motverka

Vi arbetar proaktivt för att förhindra och bekämpa cyberhot.

Omvärldsanalys och sårbarheter

Hot och risker idag och varför bry sig.

Sanne Femling

CyberSecure

Sanne Femling

IT security officer @ Resurs

33 years old, Halmstad

IT forensics and information security

Six years in cyber security

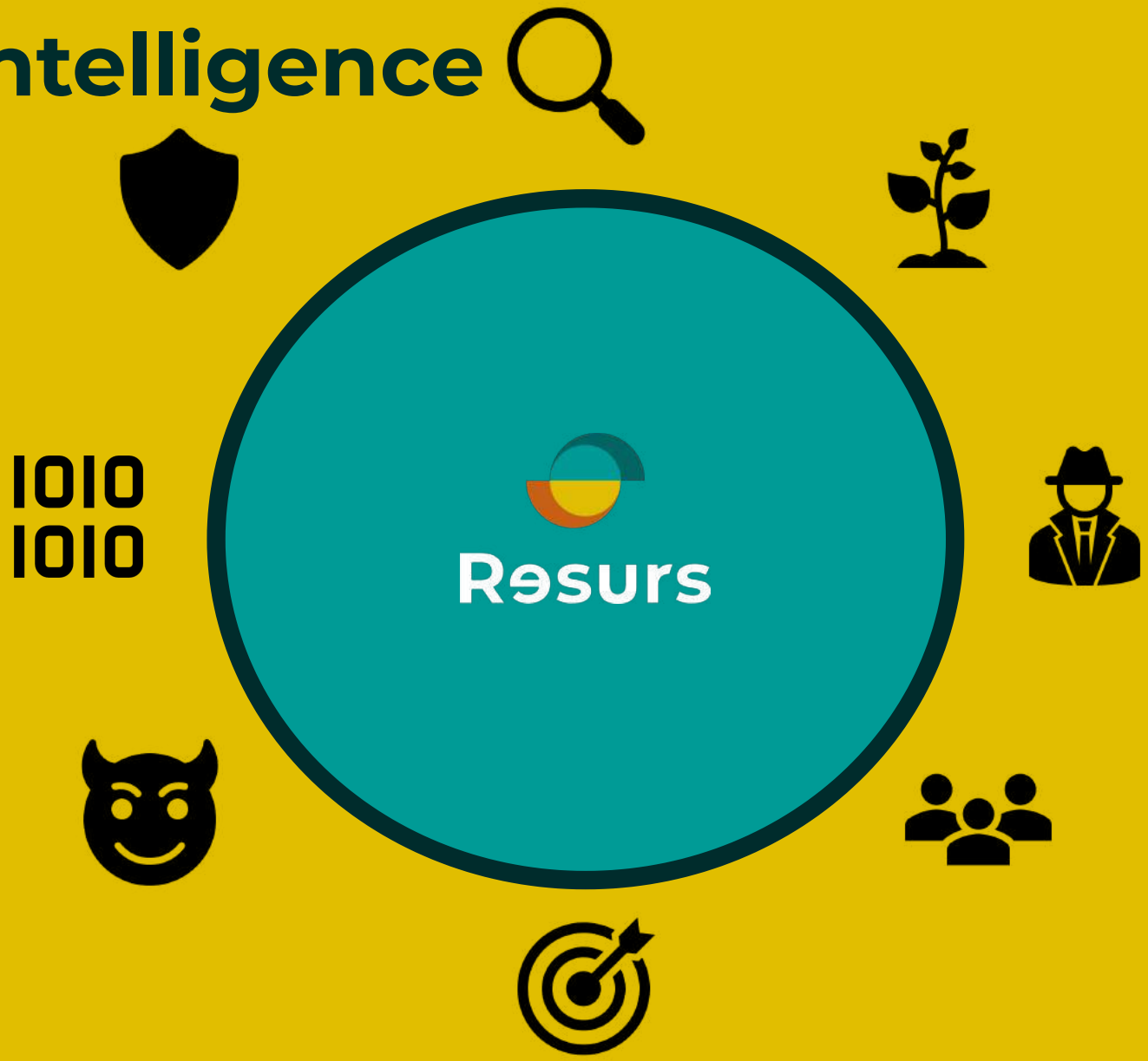
Automotive and finance industries

Sanne Femling

IT security officer @ Resurs

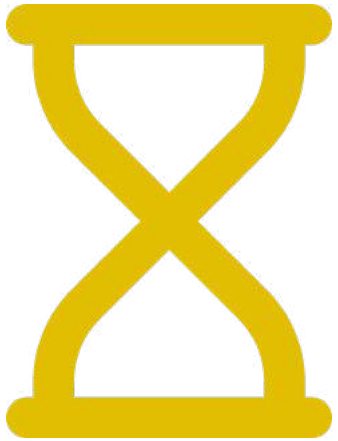
- **Penetration test management**
- **Vulnerability management**
- **Threat intelligence**
- **Awareness and education**

Threat intelligence



- Akira
- Pro Russia
- Created 2022
- Cisco VPN client
- Active in the Nordic countries

5 days



2 days

Threat Actors

- Hacktivists
- Cyber criminals
- APT/State sponsored hacker groups

”Advanced persistent threat (APT) are groups that often work in a very sophisticated and use advanced attack methods. Often sponsored by a state and work with espionage”

“Cybercriminals are groups with varying motivations, for example financial gain, and employ tactics such as hacking, identity theft, and other types of cyber crime to achieve their goals.“

“Hacktivism is the act of hacking, or breaking into a computer system, for politically or socially motivated purposes.”

Cyber attacks

- Vulnerabilities
- Access harvesting
- Ransomware attacks
- Business email compromise

“Business email compromise (BEC). Which is a cyber attack that relies on trying to get access to the companies' mailboxes to steal money.”

“Ransomware attacks consist mainly of attacks that is based on some kind of extortion. The most common one is when criminals encrypts the companies' environments which makes it impossible for the company to work and function. “

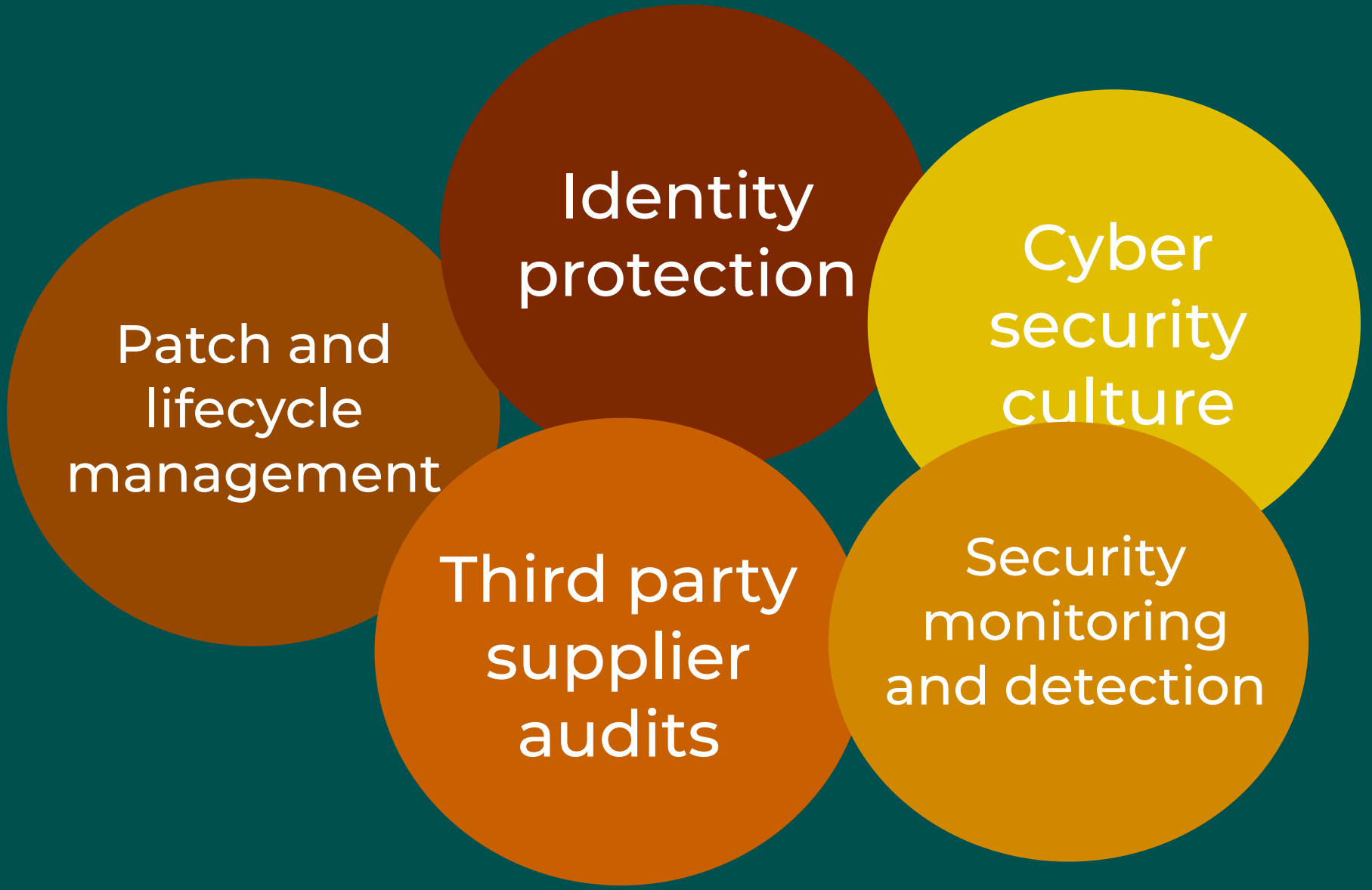
“Access harvesting occurs when a threat actor obtains access to a network intending to sell access to other cybercriminals for profit.”

“Organizations with good patch management will be targeted to a lesser extent than others because cybercriminals often gain foothold through exploiting vulnerabilities, and vulnerable systems can be found in online databases making the targeting fast and simple.“

Truesec, 2024

“Patch management is the process of applying updates to software, drivers, code, firmware etc..”

- intel


Identity protection
Cyber security culture
Patch and lifecycle management
Third party supplier audits
Security monitoring and detection

Work proactively, Not reactively

Beredskap och kontinuitet

Hur skapas en beredskapsplan för en krissituation idag.

Caroline Lendowski

CyberSecure

Kontinuitets-hantering

Behöver det vara så krångligt?

benify

Vem är jag & varför står jag här?

Caroline Lendowski,
Business Continuity & Risk Manager, Benify

Connecta gärna

benify

Benify

Engagera dina medarbetare med Benifys marknadsledande plattform för förmåner, ersättning och kommunikation

benify


Behöver kontinuitetshantering vara så krångligt?
benify


För det som är kritiskt,
identifiera risker för avbrott,
minska risken att det sker,
ha en plan B och öva!
benify

Lärdomar och utmaningar från implementering & certifiering av ISO22301

benify

TACK!

Caroline Lendowski

benify

Gallup, September 2022

Tips och verktyg

De vanligaste hoten och konkreta skyddsåtgärder.

Edward Wasilchin

CyberSecure

There are only **two types** of companies in the world: Those who have been breached and **know it** and those who have been breached and don´t know it.

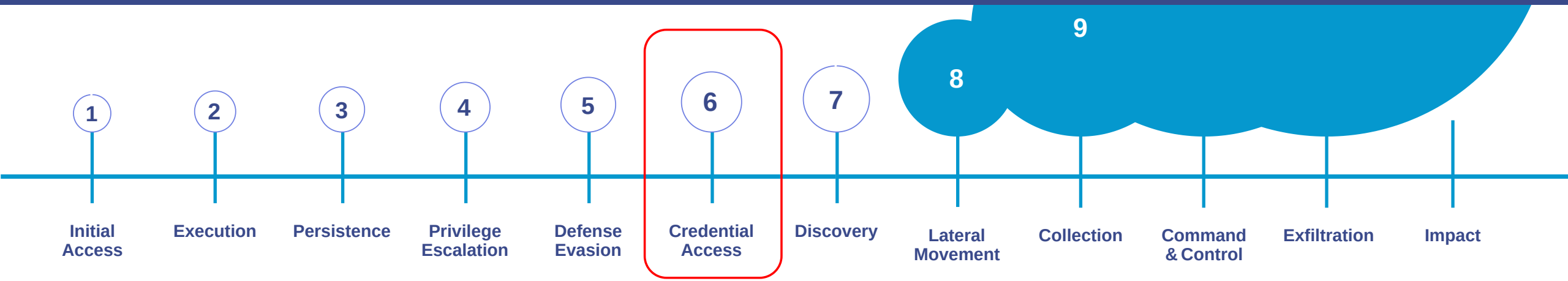
> Ted Schlein,
> *Investor*

OBSERVATA

Hur går en attack till?

För att avvärja en attack måste du kunna…

Upptäcka inom	Utreda inom	Åtgärda inom
1 min	10 min	60 min



MITRE ATT&CK FRAMEWORK
https://attack.mitre.org/#

OBSERVATA

De vanligaste attack vektorerna och hur man skyddar sig.

Supply Chain

Attack genom att utnyttja relationer till tredje part.

68%

Credentials

Stöld och utnyttjande av behörigheter för intrång.

83%

Ransomware

Användande av skadlig kod för att ta data som gisslan.

82%

75%

Phishing

Användande av mail eller meddelande för distribution av skadlig kod eller beteende.

80%

Vulnerability Exploits

Exploatering av sårbarheter för att implementera skadlig kod.

31%

Social Engineering

Manipulering av social media för att tillskanska sig information

OBSERVATA

Vanligaste hoten och skyddsåtgärder - Supply chain

Supply Chain

Teknik

Mjukvaru infiltrering
Bedrägligt beteende
Förfalskade komponenter
Felaktiga uppdateringar
Behörigheter

Motivation

Data stöld
Industriell spionage
Finansiellt motiverat
Skapa oreda och avbrott.
Skada förtroende

Skyddsåtgärd

Övervakning med åtgärd
Tredje parts reglering
Hantering av behörigheter
Kodhantering

OBSERVATA

Vanligaste hoten och skyddsåtgärder - Credentials

OBSERVATA

Vanligaste hoten och skyddsåtgärder - Ransomware

Ransomware

Teknik

Phishing
Exploits
Credentials
Social Engineering
Supply chain
Brute force

Motivation

Data stöld
Finansiellt motiverat
Skapa oreda och avbrott.
Skada förtroende

Skyddsåtgärd

Övervakning med åtgärd
Utbildning
Lösenordspolicy
Frekventa backuper
Incident hantering/försäkring
Sårbarhetshantering
Nätverkssegmentering

OBSERVATA

Vanligaste hoten och skyddsåtgärder - Phishing

OBSERVATA

Vanligaste hoten och skyddsåtgärder - Vulernability Exploits

Vulnerability Exploits

Teknik

Exploit Kits (AI, Automation)
Zero-Day Exploits
Vulerability Scanning
Port Scanning

Motivation

Data stöld
Industriell spionage
Finansiellt motiverat
Skapa oreda och avbrott.
Skada förtroende

Skyddsåtgärd

Övervakning med åtgärd
Sårbarhetshantering (Patch)
Nät segmentering
Multifaktor autentisering
Stark lösenordspolicy
Hantering av admin behörigheter

OBSERVATA

Vanligaste hoten och skyddsåtgärder - Social Engineering

OBSERVATA

Thinking of cybersecurity solely as an IT issue is like believing that a company's entire workforce, from the CEO down, is just one big HR issue.

Steven Chabinsky,
Global Chair of Data, Privacy & Cybersecurity at White & Case LLP

OBSERVATA

Vad kan jag göra när jag kommer hem?

Lösenordspolicy

47%

Byt ofta och till starka lösenord.

Backuper

31%

Backa flera gånger per dag.
Öva på att återställa.

Utbildning

27%

Utbilda personalen. Security awreness training.

EndPoint skydd

68%

Bevaka beteenden - De flesta intrång sker utan användandet av skadlig kod.

Behörigheter

83%

Framgångsrika attacker görs genom behörigheter.

Patch Management

27%

Patcha - Minska attack ytan genom att ständigt se till att minimera dina sårbarheter.

OBSERVATA

När du behöver hjälp?

www.cybersecure.nu

CyberSecure Halmstad

host@cybersecure.nu