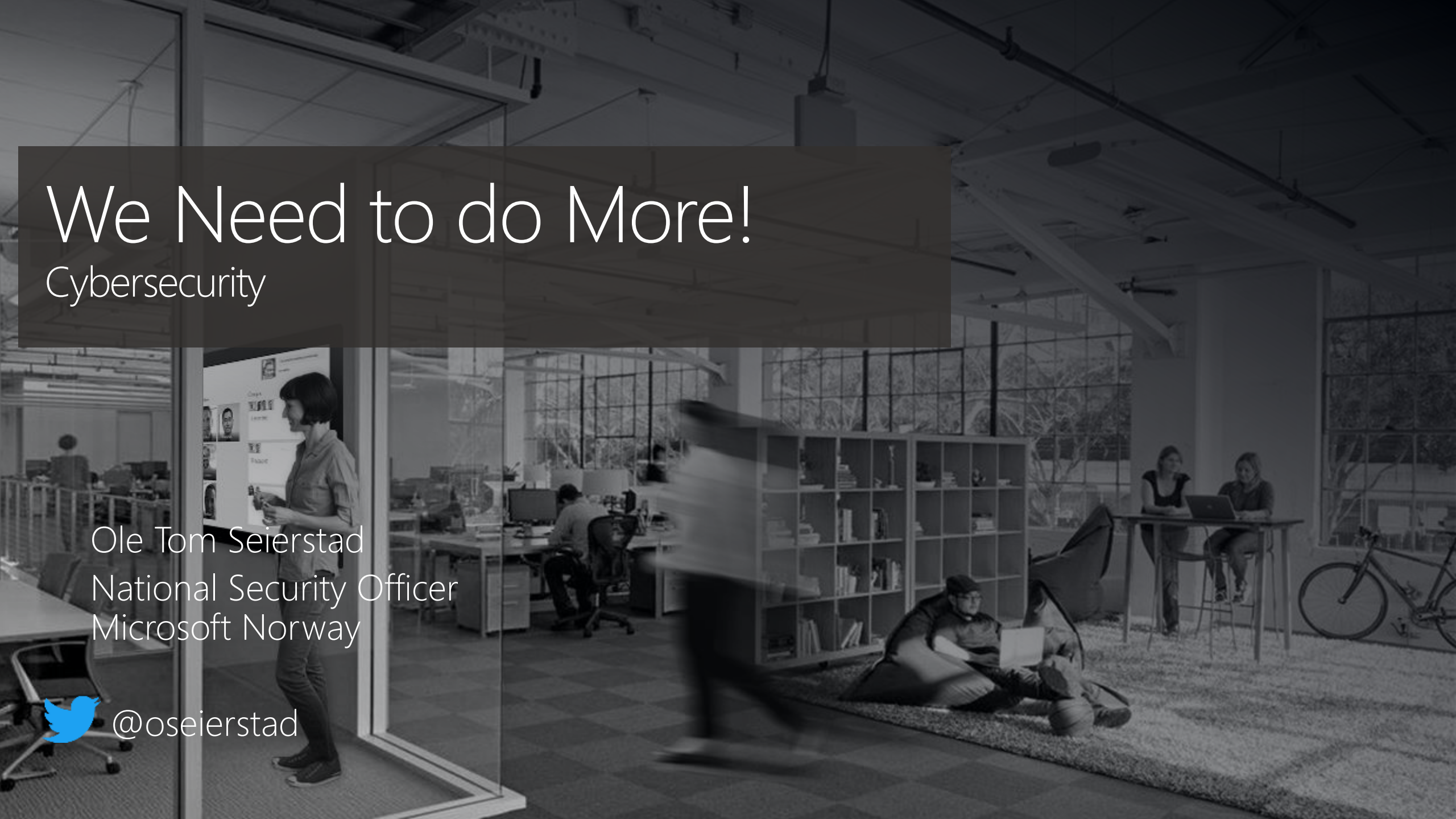


We Need to do More!

Cybersecurity

Ole Tom Seierstad
National Security Officer
Microsoft Norway

@oseierstad

CYBERSECURITY TODAY impacts us all

$4million

Average cost of a data breach in 2017

$8trillion

Estimated cost of cybercrime to world economy by 2022

6billion+

Records stolen by hackers in 2017

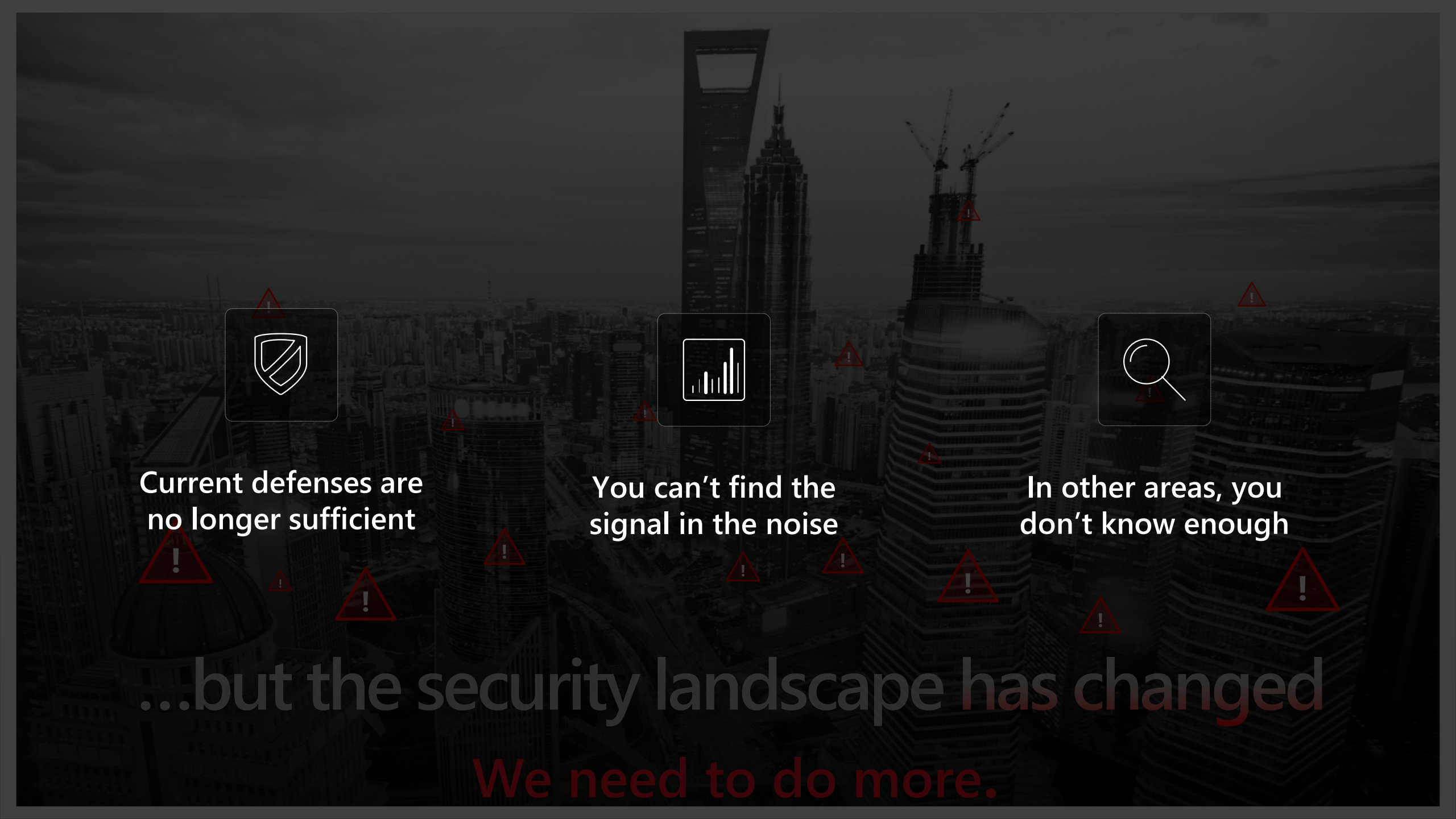
1million+

New malware variants created each day

>99days

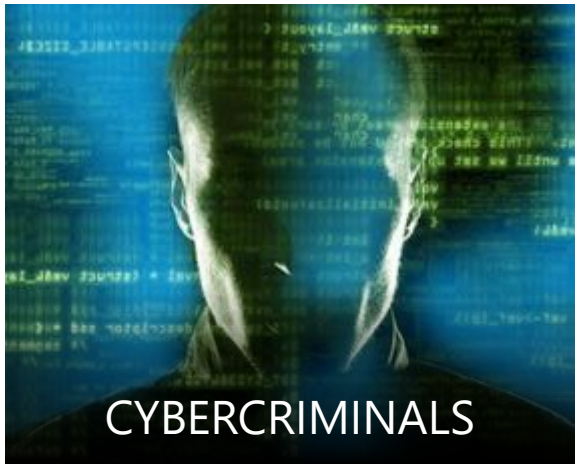
Median # of days between infiltration and detection


You have many of the best security solutions…


Current defenses are no longer sufficient
You can't find the signal in the noise
In other areas, you don't know enough
...but the security landscape has changed
We need to do more.

Today's top THREAT ACTORS pose unique challenges

An effective strategy must respond to a broad range of continually evolving attack types



FINANCIAL

Persistent presence
Professional execution
Ransomware

ESPIONAGE

Near-unlimited resources
Sophistication
Legal autonomy

POLITICAL

Shape/influence opinions
Undermine trust

OPPORTUNISTIC

Access to IT environment
Trusted to access sensitive info

Attack Vectors

SOCIAL ENGINEERING

PHISHING

IDENTITY SPOOFING

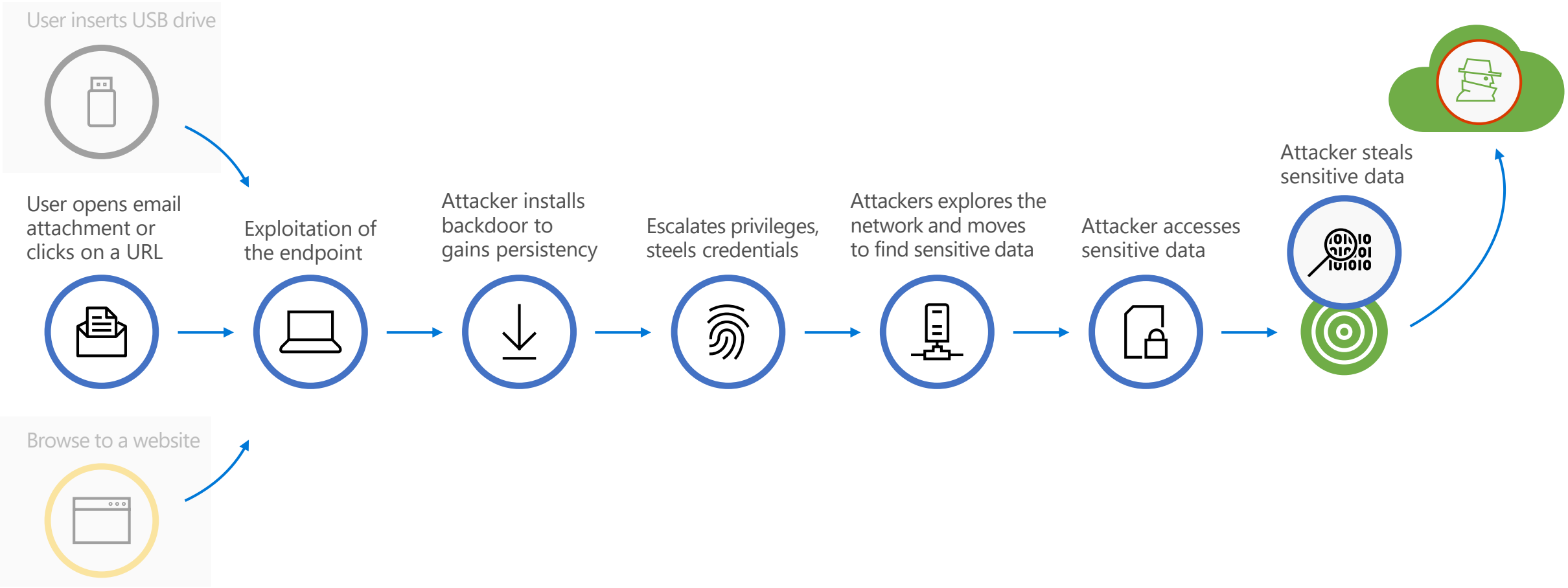
MALWARE

SUPPLY CHAIN INSERTION

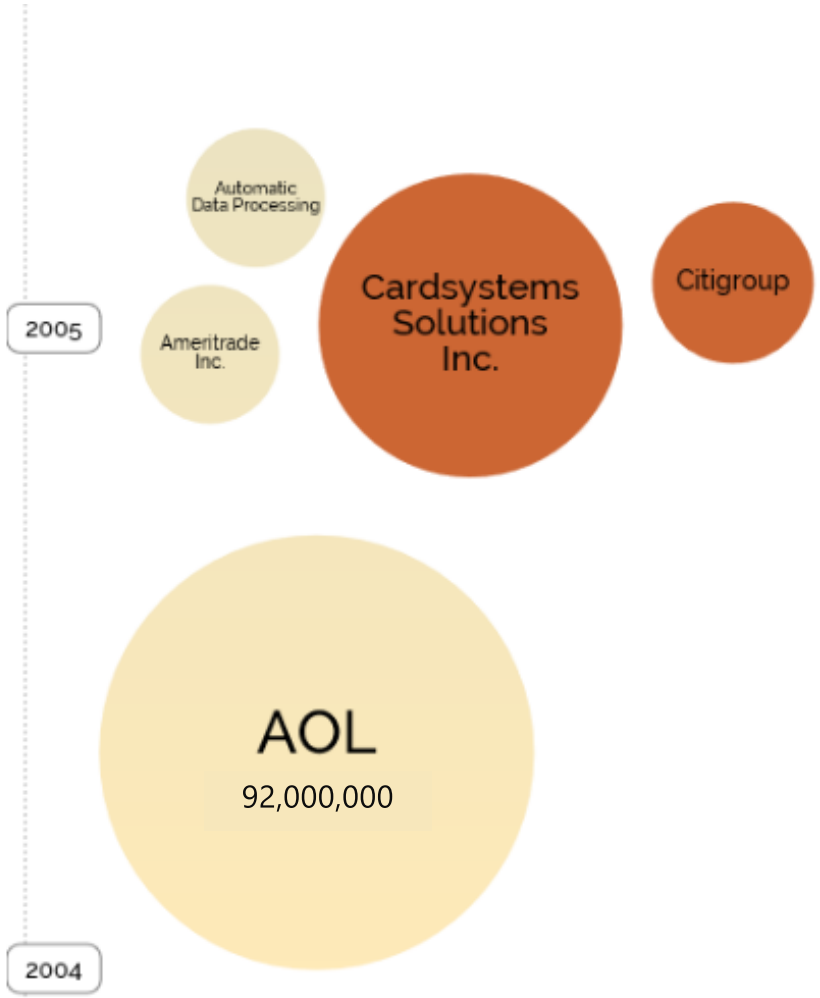
MAN-IN-THE-MIDDLE

DENIAL OF SERVICE

Various stages of **an attack**



BRIEF HISTORY OF BREACHES

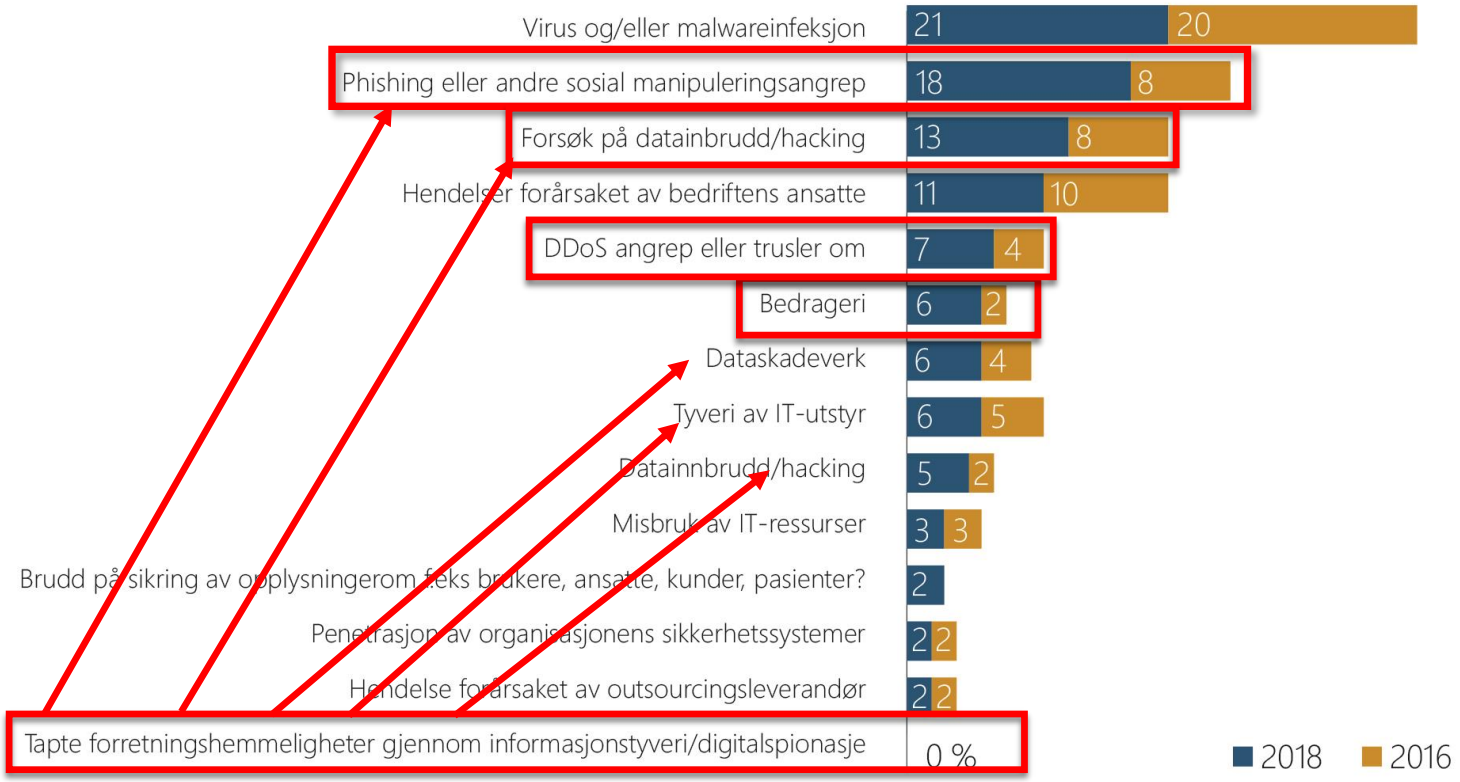


Næringslivets sikkerhetsråd

Mørketallsundersøkelsen 2018

Hendelser

Spørsmål: Jeg vil nå lese opp noen mulige informasjonssikkerhetshendelser og ber deg svare ja eller nei på om virksomheten har vært utsatt for disse i kalenderåret 2017? (n=1500)

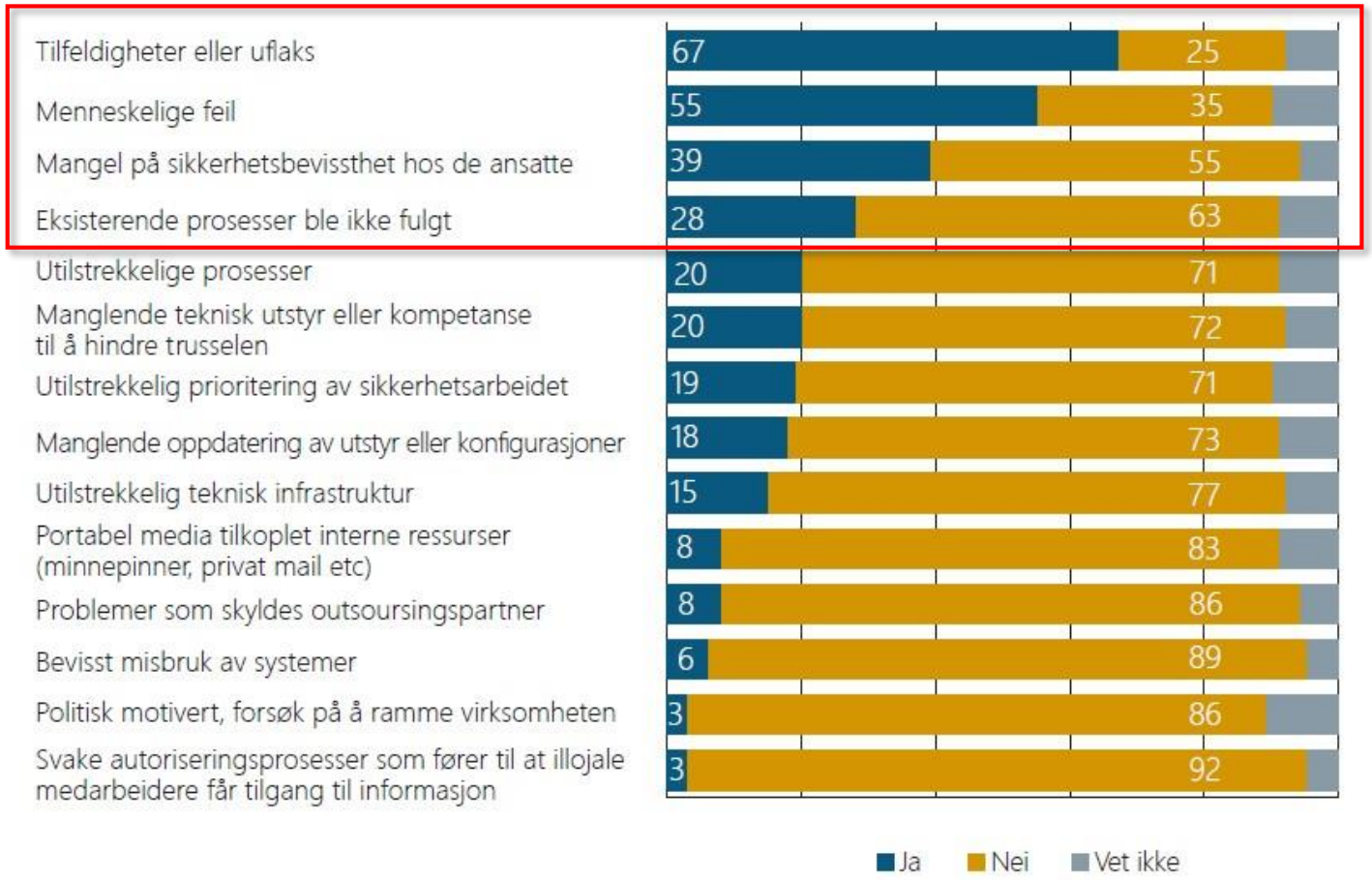


Sammenlignet med 2016 er det spesielt phishing, datainnbrudd/hacking, DDoS-angrep eller trussel om dette, samt bedrageri som har økt.

Ingen oppgir at de har tapt forretningshemmeligheter på grunn av digital spionasje.

Årsaker

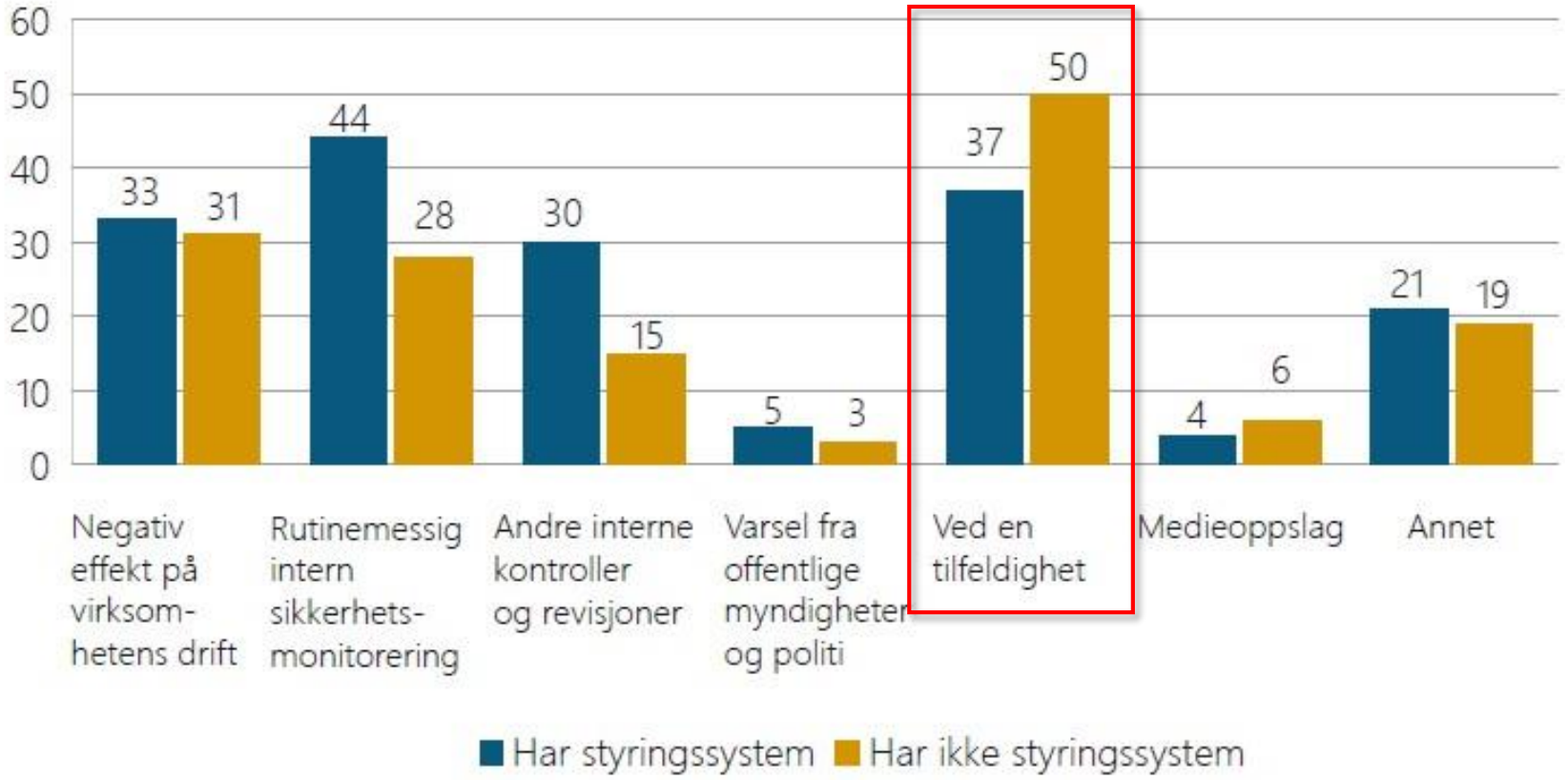
*Spørsmål: Var noen av følgende faktorer årsak til at sikkerhetsbruddet **oppsto**?*



Blant de som har opplevd hendelser er det 67 prosent som mener årsaken var tilfeldigheter eller uflaks, mens over halvparten også tilskriver sikkerhetsbruddet menneskelige feil.

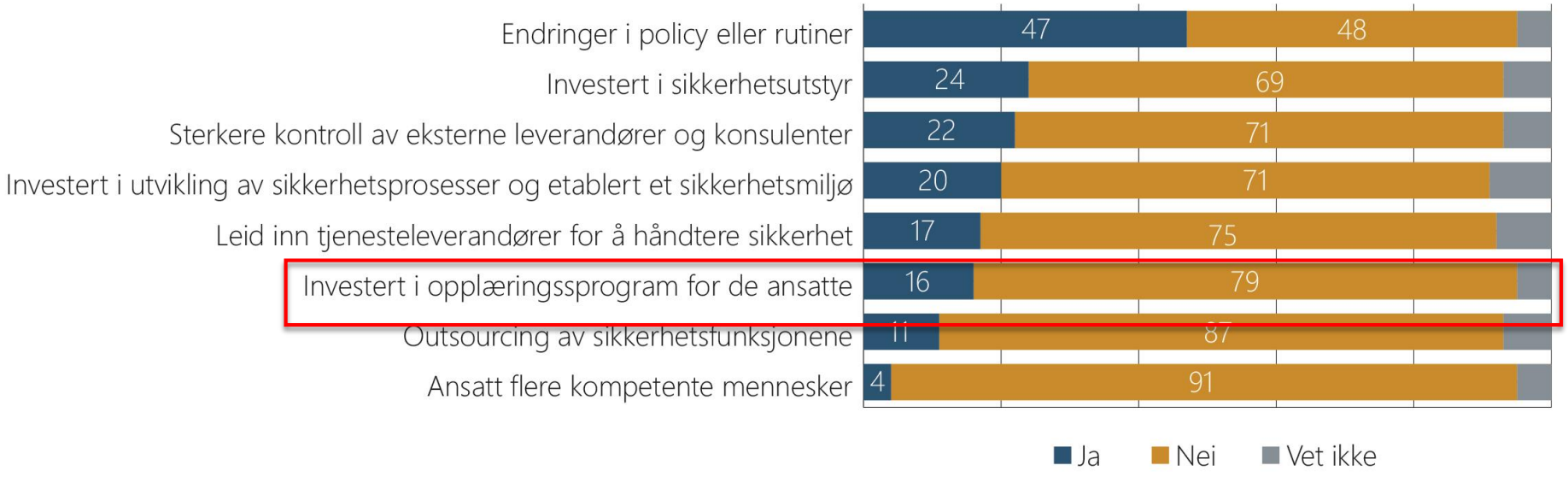
Dette er en nedgang fra 2016.

Årsaker


60
50
40
30
20
10
0
33
31
44
28
30
15
5
3
37
50
4
6
21
19
Negativ effekt på virksom-hetens drift
Rutinemessig intern sikkerhets-monitorering
Andre interne kontroller og revisjoner
Varsel fra offentlige myndigheter og politi
Ved en tilfeldighet
Medieoppslag
Annet
Har styringssystem
Har ikke styringssystem

Følger og håndtering

Spørsmål: Som et resultat av hendelsen, ble noen av følgende endringer gjort i organisasjonen?



De store virksomhetene har i større grad investert i opplæring for de ansatte. Virksomheter som har et styringssystem for informasjonssikkerhet har i større grad enn andre investert i utvikling av sikkerhetsprosesser og etablert et sikkerhetsmiljø.

Dette til tross for at menneskelige feil oppgis til én av hovedårsakene til at hendelsen oppstod.

Næringslivets sikkerhetsråd

PROTECT

Defense-in-Depth

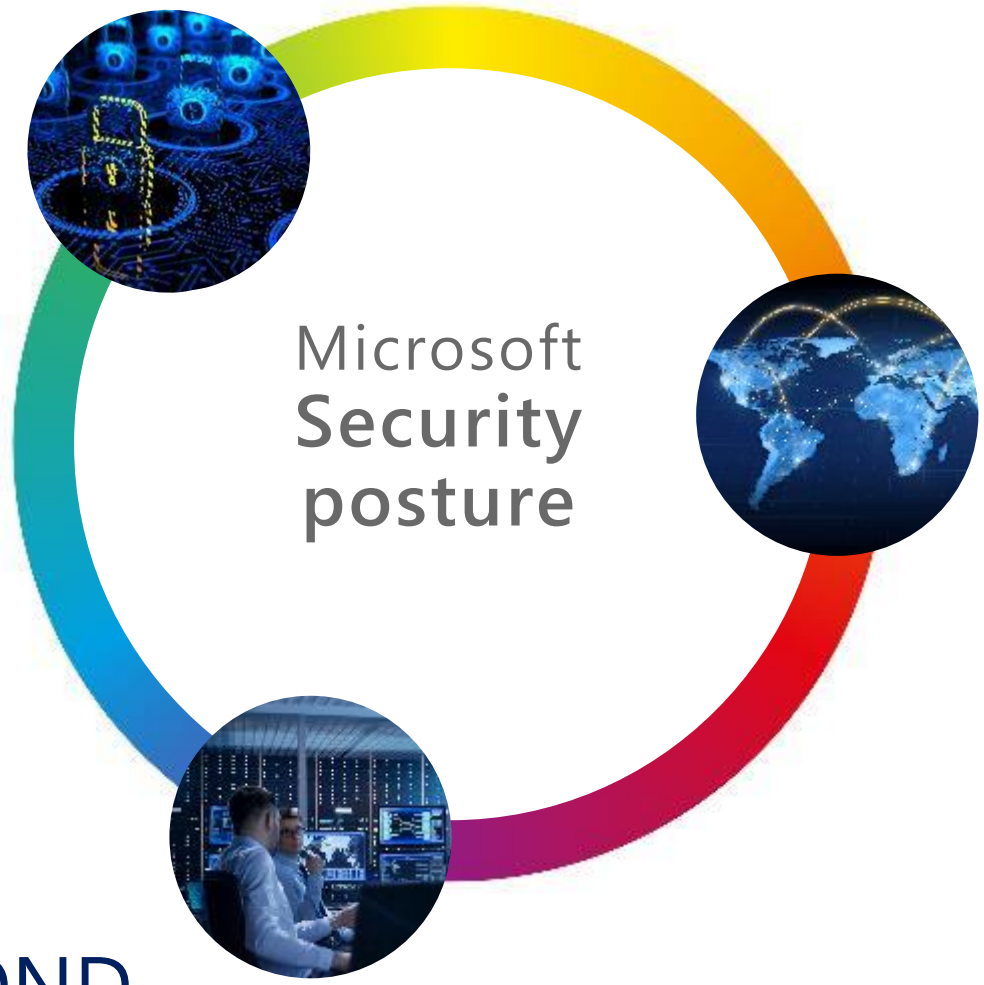
Monitoring and controls

Identity and Access management

Proper hygiene

Security Development Lifecycle

Data encryption



DETECT

Extensive signal fabric

Cloud scale intelligence

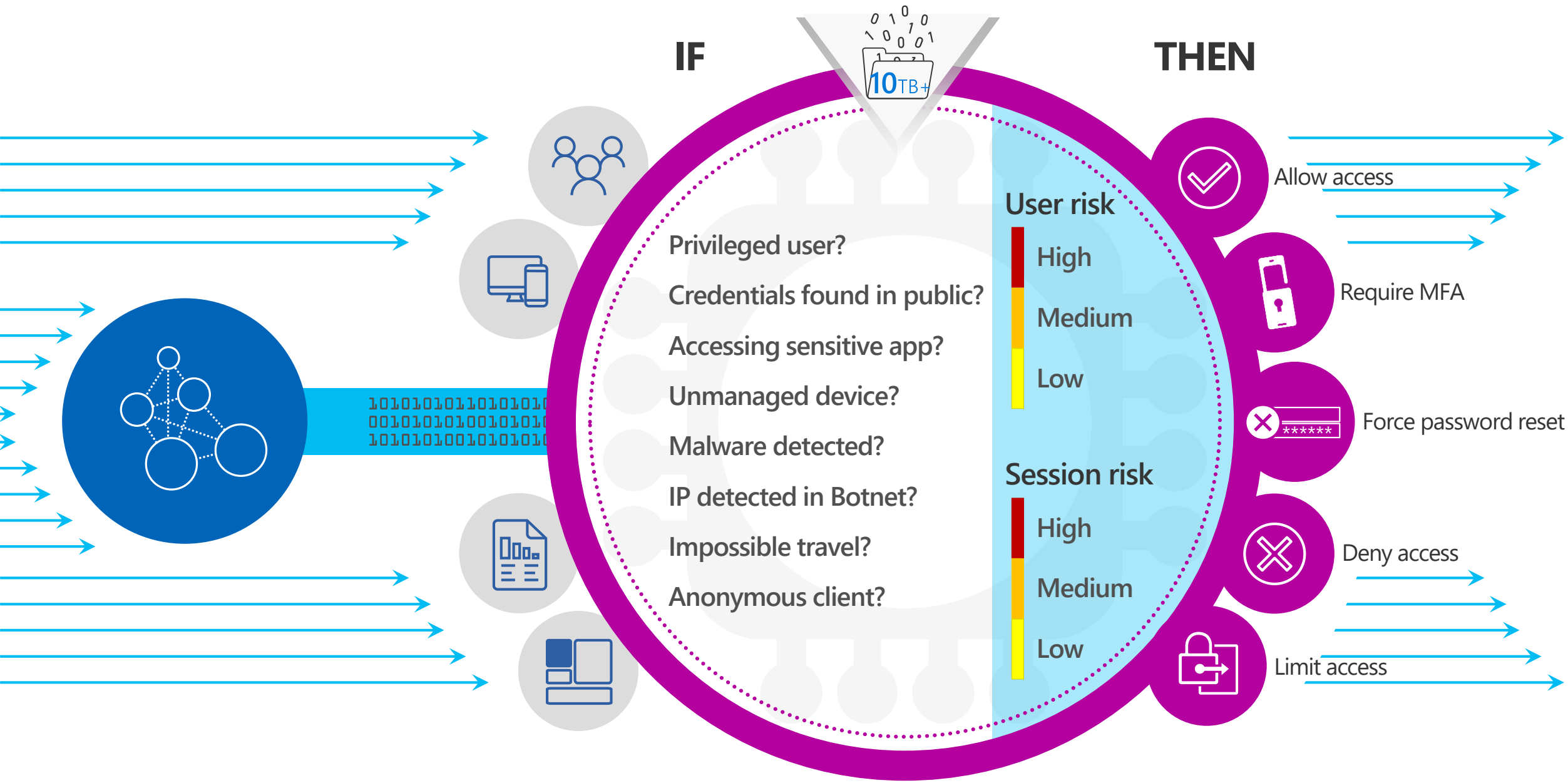
Machine learning

Behavioral monitoring

RESPOND

Closing the gap between discovery and action

CLOUD-POWERED CONDITIONAL ACCESS




Thank You!
Microsoft
@oseierstad