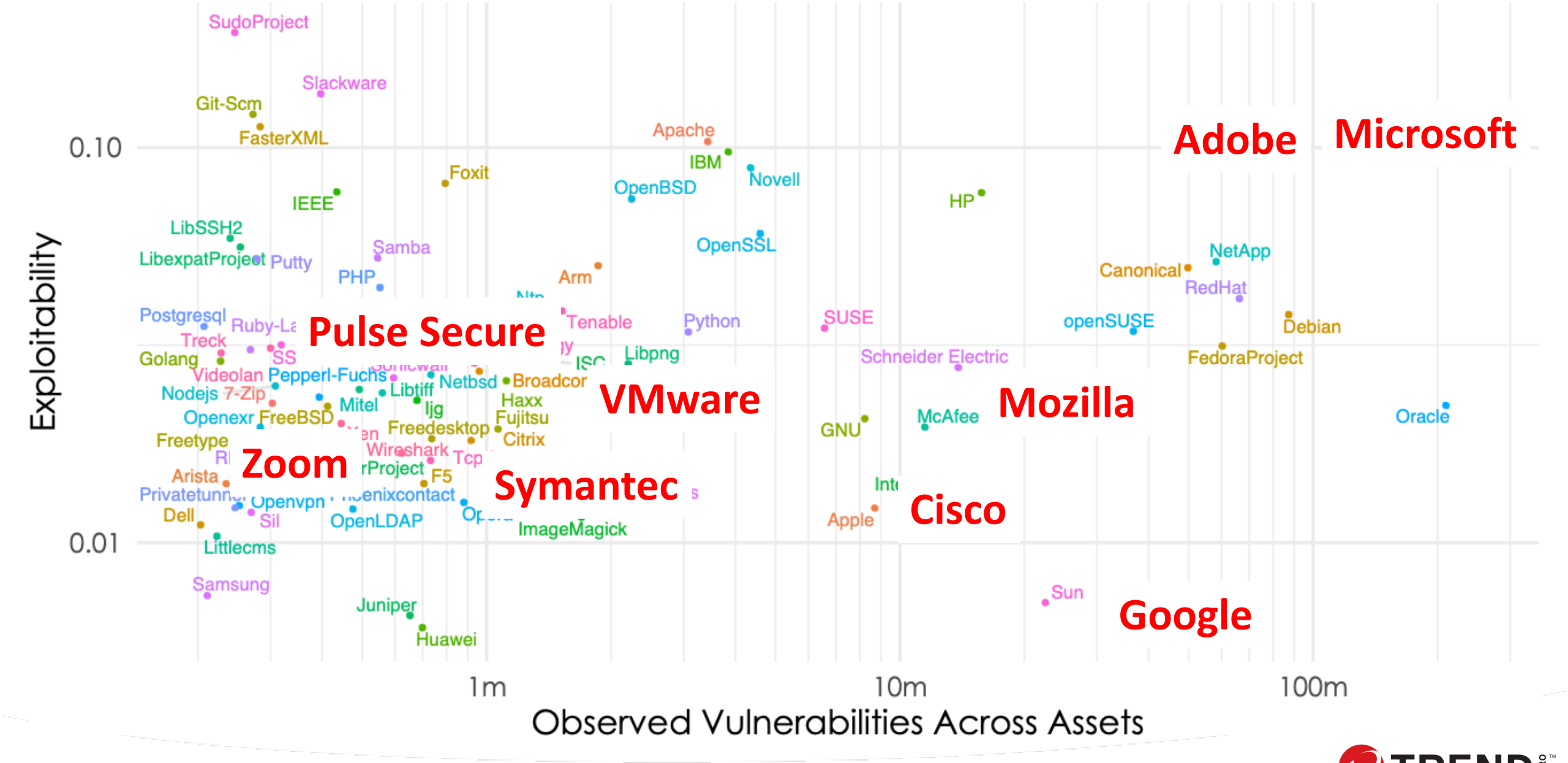
# En reise i nulldags sårbarheter og sårbarheter…og hva du kan gjøre for å beskytte deg mot disse!

Niels Fredrik Berthelsen

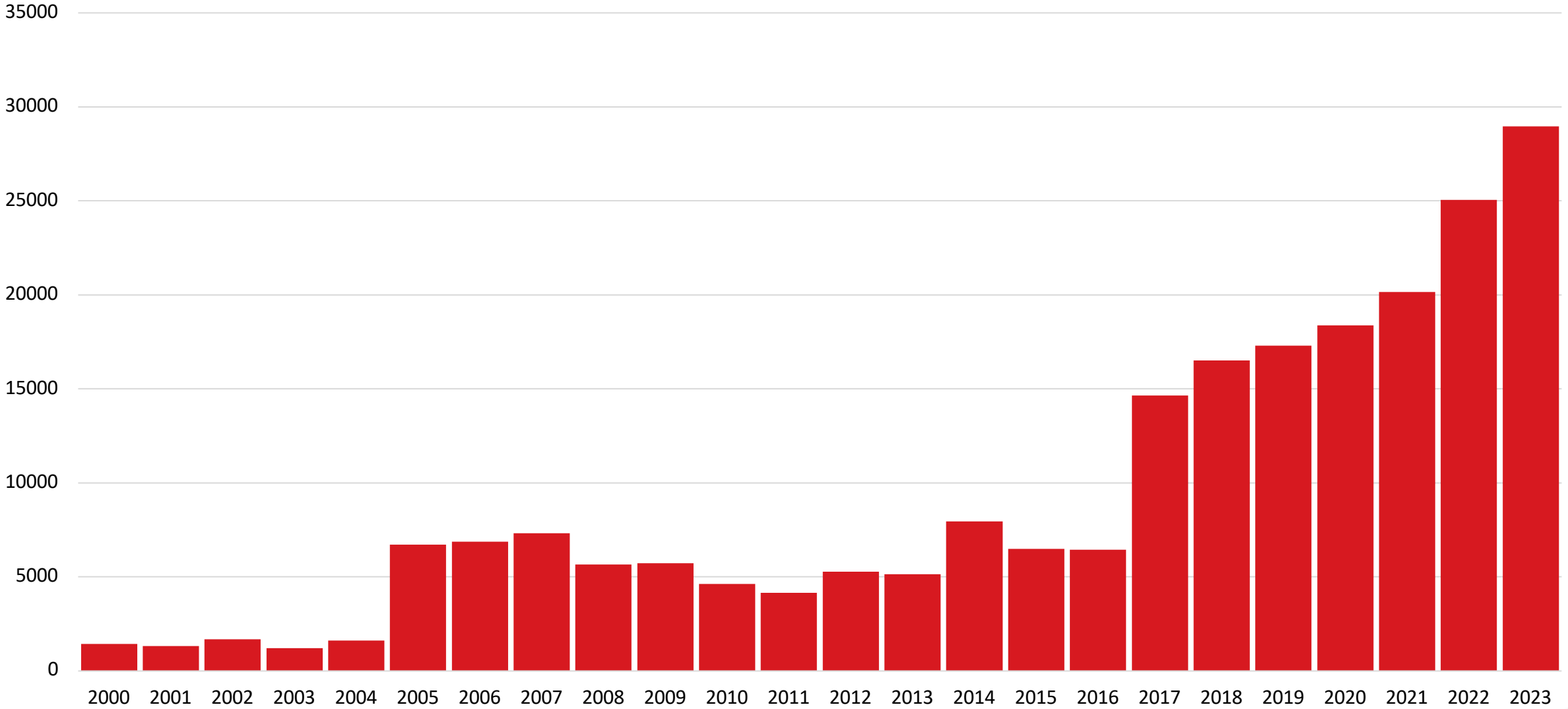
TREND MICRO™



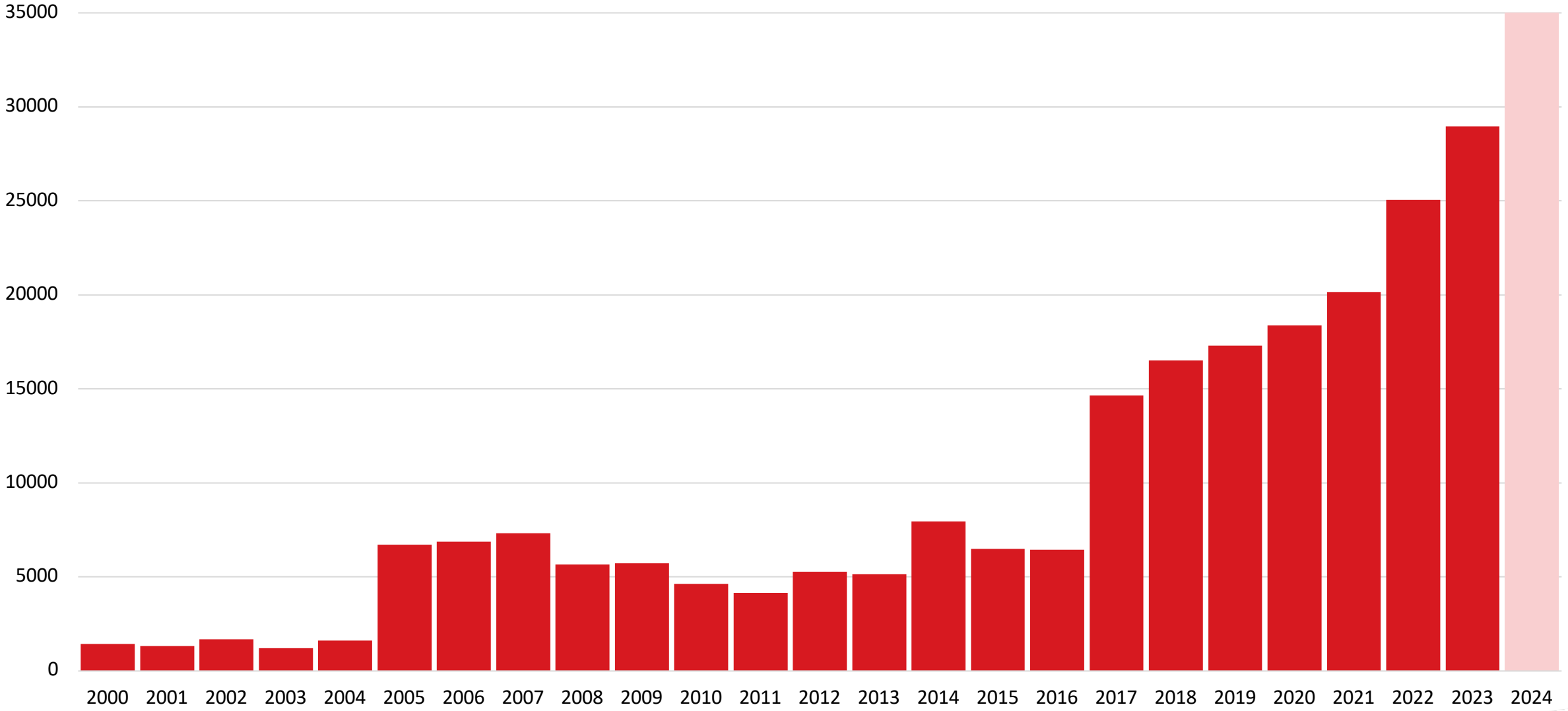


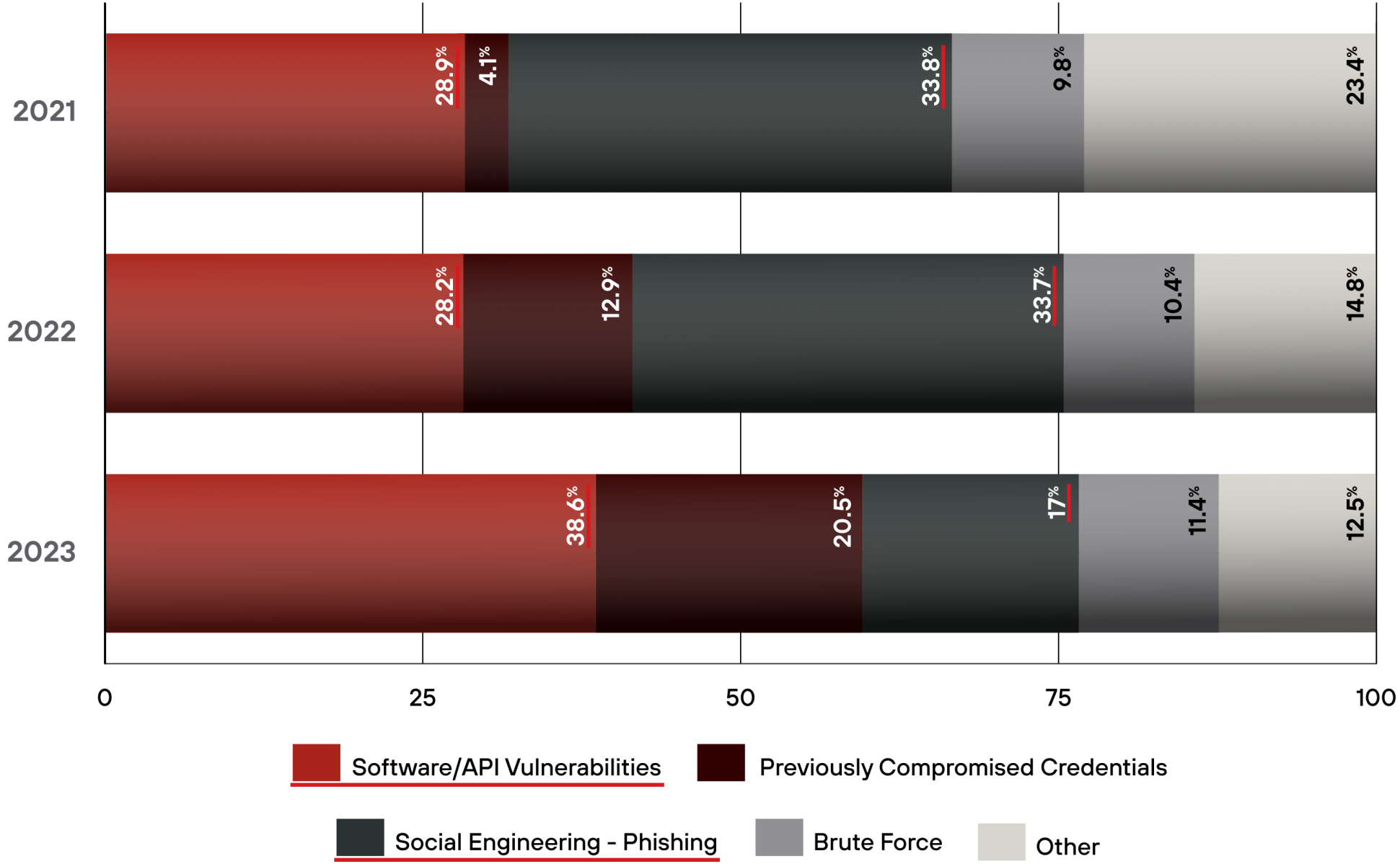

Kenna Security. (2022). *P2P Volume 8: Measuring and Minimizing Exploitability*.

# Antall sårbarheter per år

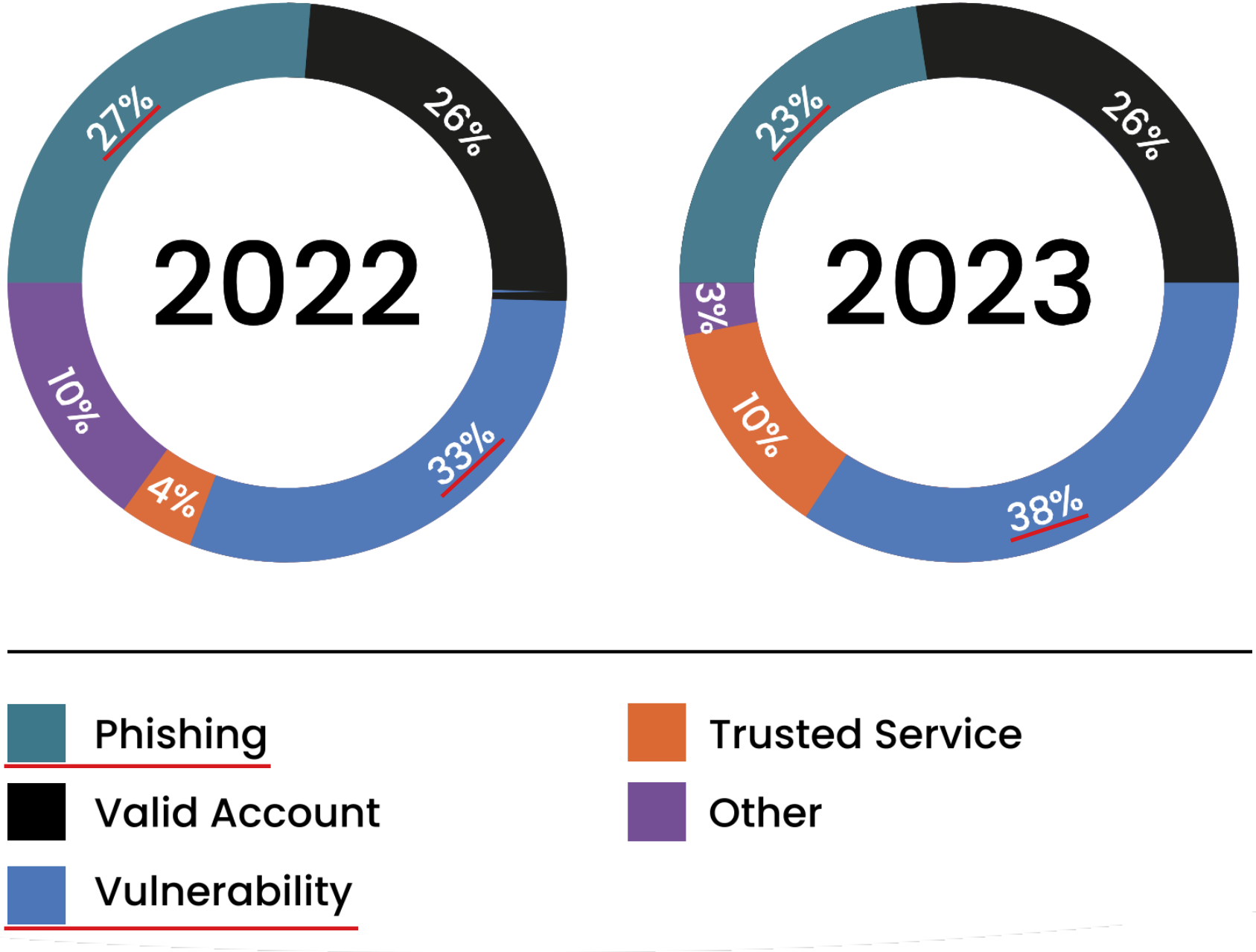


# Antall sårbarheter per år



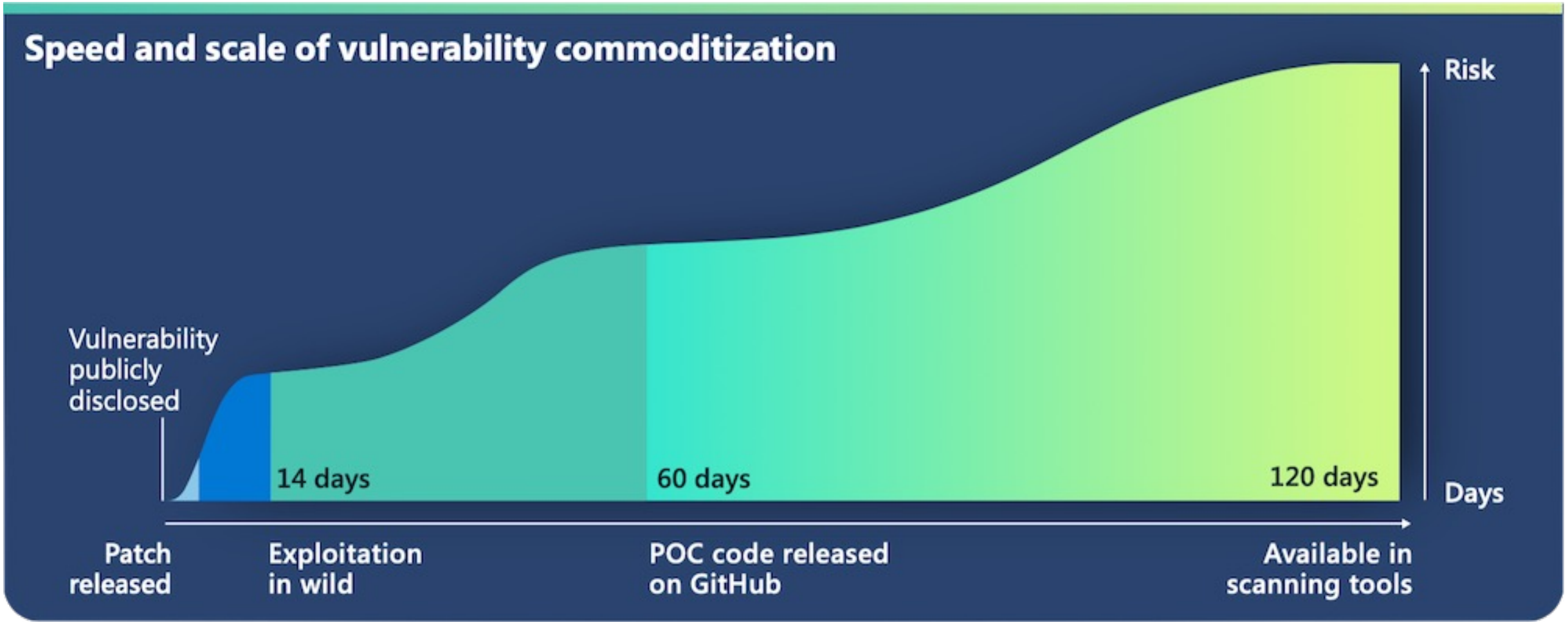



Palo Alto Networks. (2024). *Incident Response Report 2024*.




Truesec. (2024). Threat Intelligence Report 2024.

# Når treffer dritten vifta…?




Microsoft. (2022). *Microsoft Digital Defense Report 2022*.

# Hva er en nulldags sårbarhet?

## En SW-bug som er ukjent for produsenten

Produsenten har hatt “null dager” til å respondere

## Utnyttelse av disse er en sjeldenhet

Nasjonalstater, avanserte trusselaktører og andre tunge aktører er angripere

## De er vanlige

Og verdien av de kan vareriere fra noen hundre til millioner av dollar

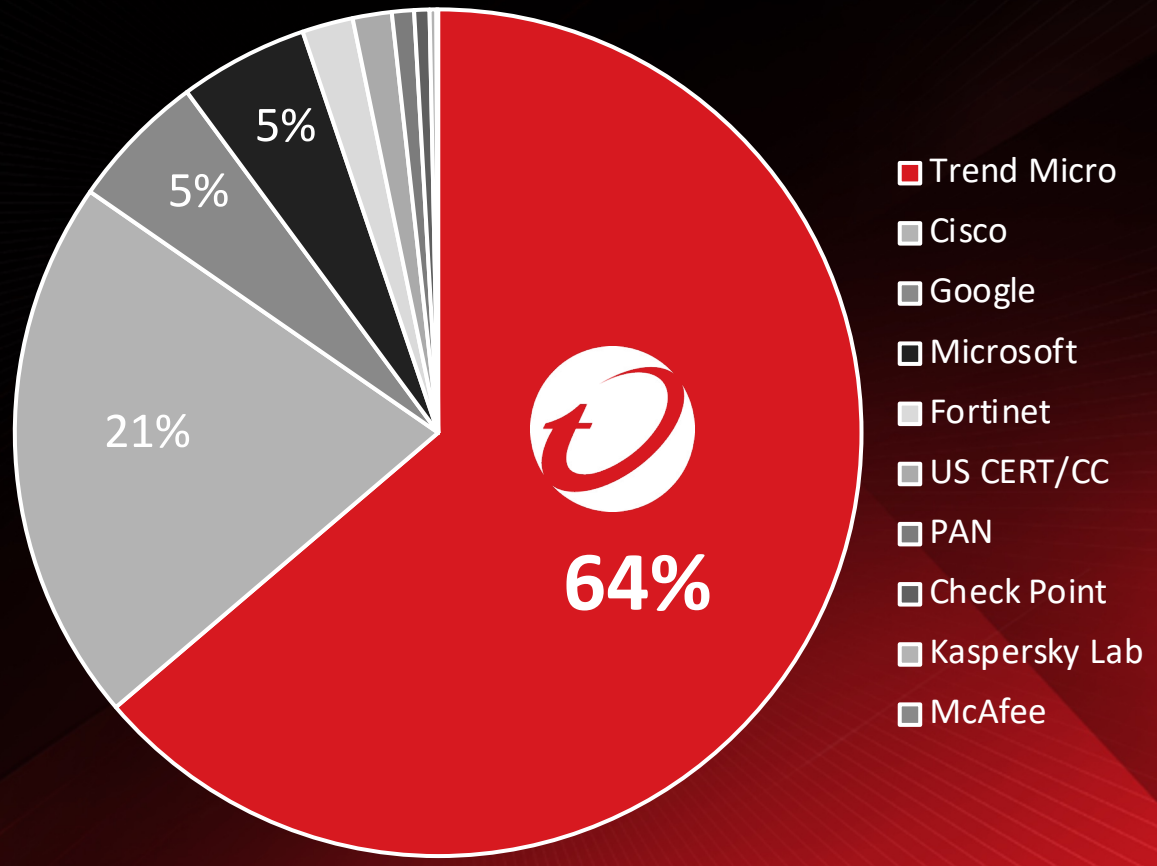
 

# Zero Day Initiative

ZERO DAY INITIATIVE

## #1 Public Vulnerability Disclosure Market

*Quantifying the Public Vulnerability Market, Omdia, May 2022*




*«Å utnytte en nulldagssårbarhet krever store ressurser, enten angriperen finner svakhetene selv, eller kjøper dem. Sårbarhetene kan koste flere titalls millioner kroner»*

Albert-Hoff – leder for Nasjonalt Cybersikkerhetssenter



TREND MICRO

# The Zero Day Initiative

Verdens største produsent-agnostiske bug bounty program

Innkjøper av Zero Days fra uavhengige forskere over hele verden

*Skaper filter for Trend Micro sine produkter

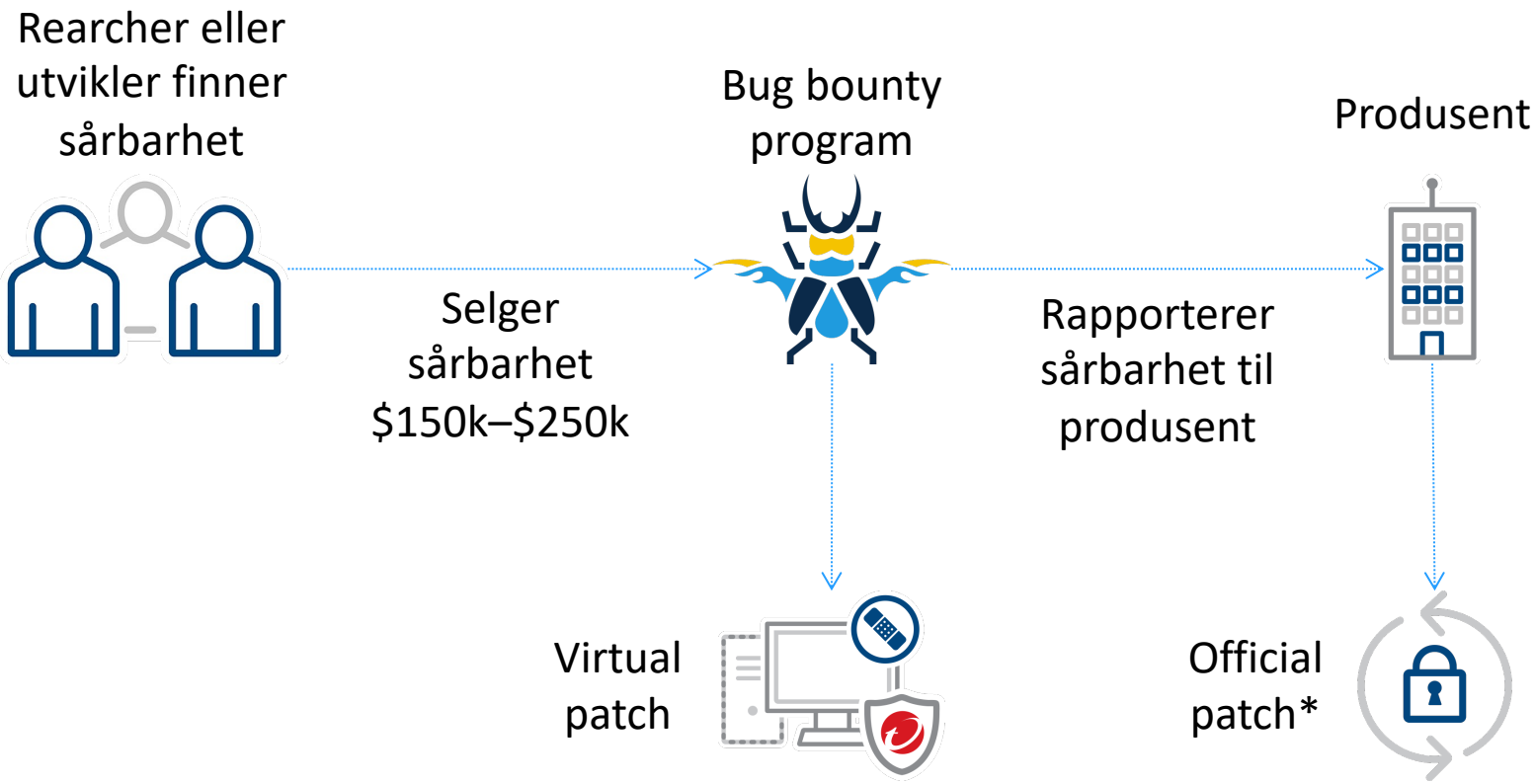
# Sårbarheter kan selges på en rekke måter

Bug bounty programmer

Meglere(eller statlige aktører)

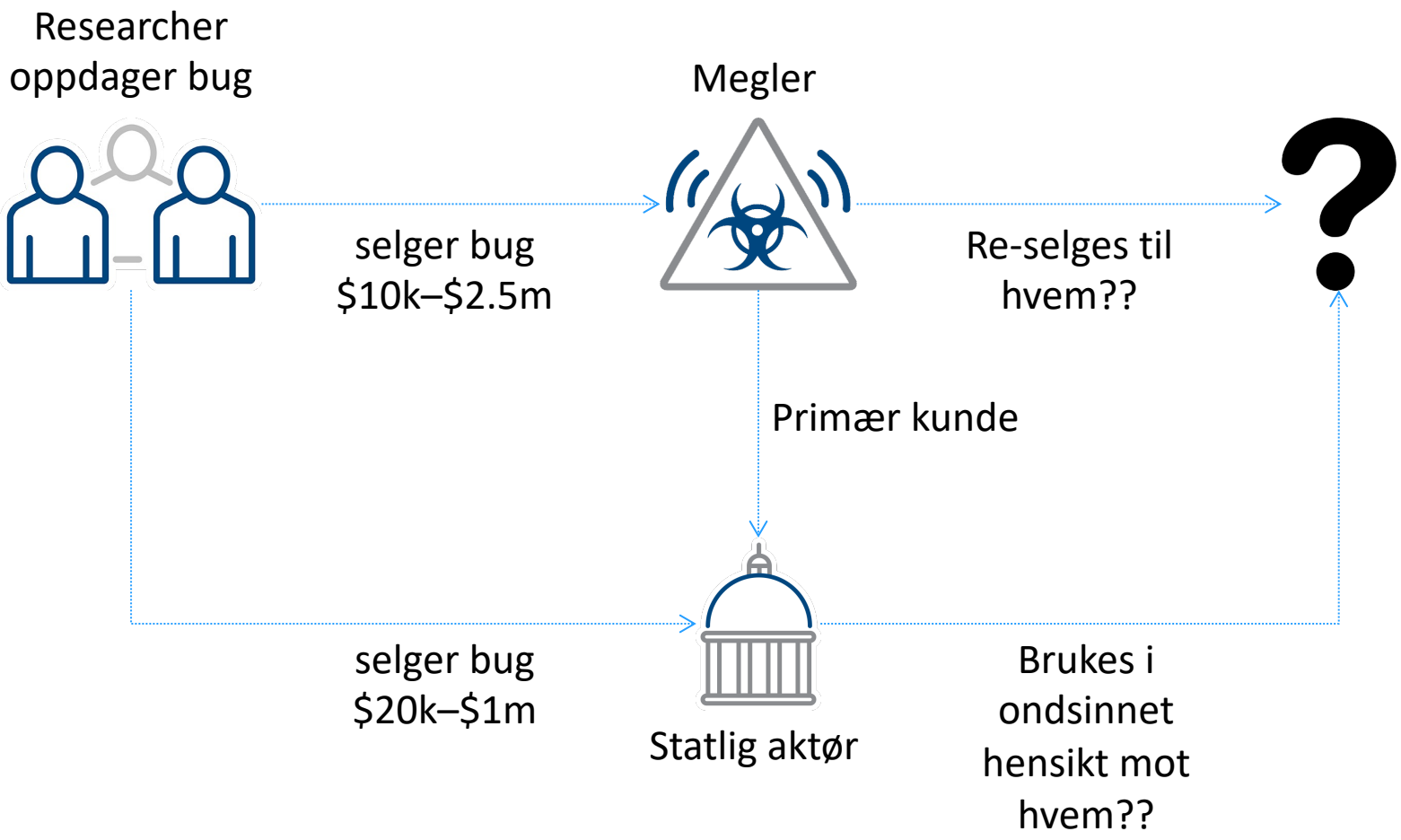

Kriminelle/dark web

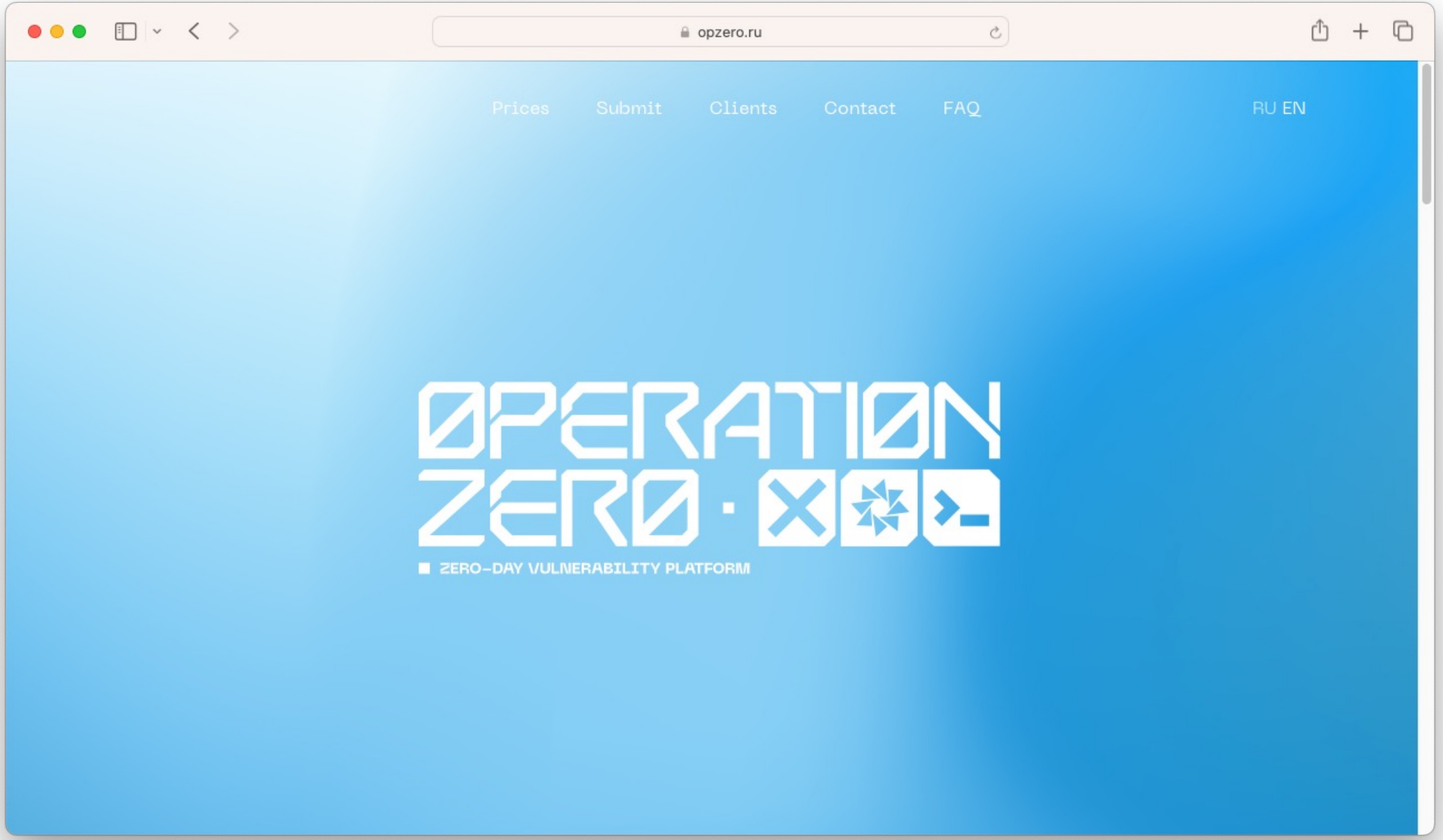
# Hvordan selge til ZDI eller et annet bug bounty program?

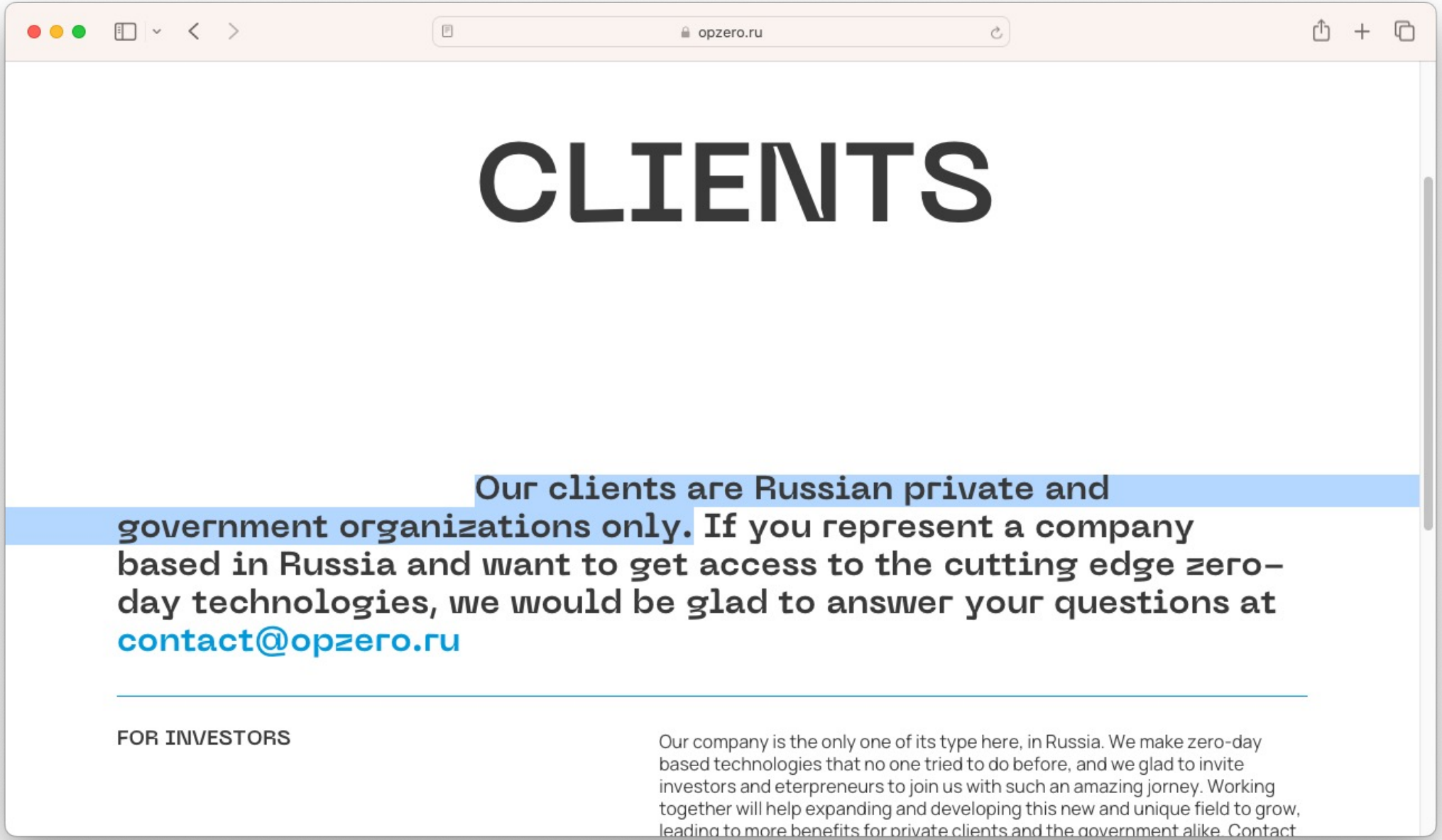


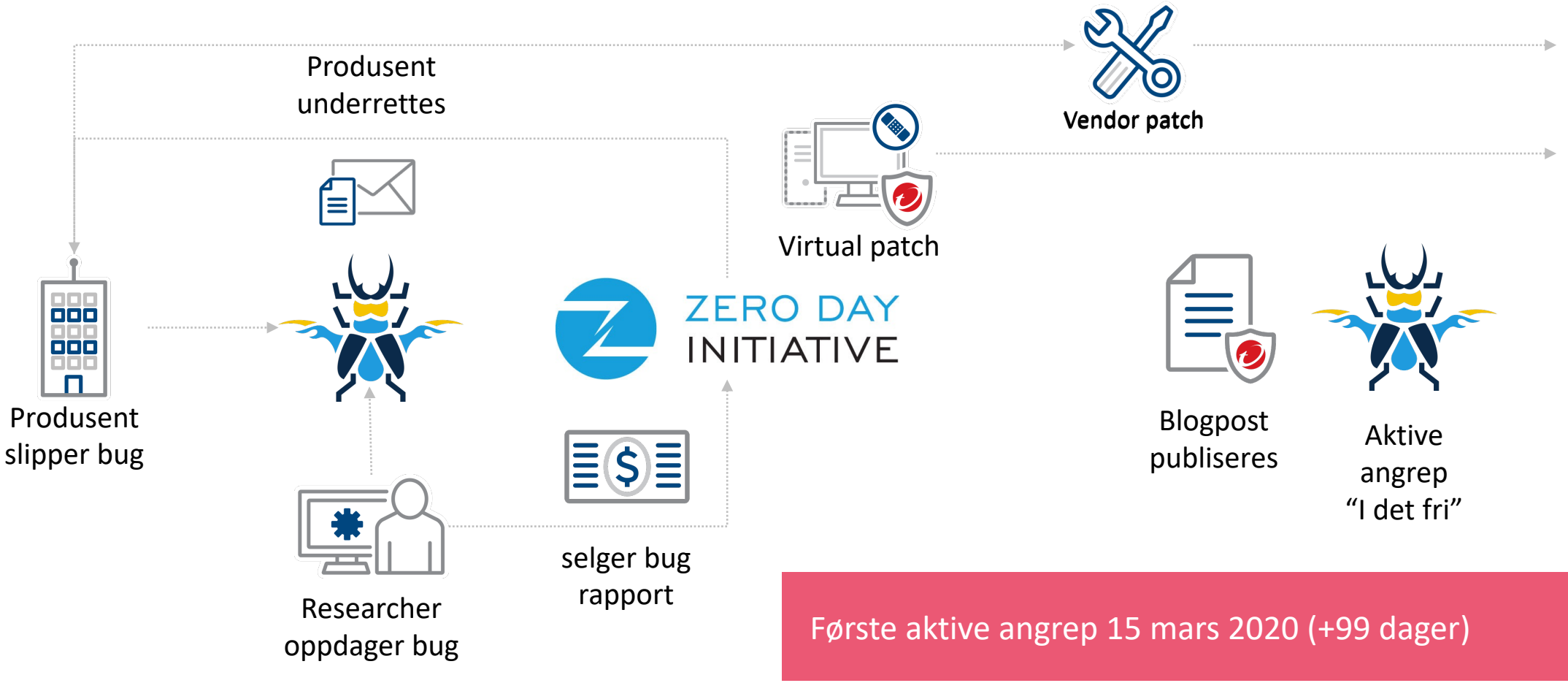
# Å selge til en megler av sårbarheter




opzero.ru
Prices
Submit
Clients
Contact
FAQ
RU EN
OPERATION
ZERO
ZERO-DAY VULNERABILITY PLATFORM


opzero.ru
CLIENTS
Our clients are Russian private and government organizations only. If you represent a company based in Russia and want to get access to the cutting edge zero-day technologies, we would be glad to answer your questions at contact@opzero.ru
FOR INVESTORS
Our company is the only one of its type here, in Russia. We make zero-day based technologies that no one tried to do before, and we glad to invite investors and eterpreneurs to join us with such an amazing jorney. Working together will help expanding and developing this new and unique field to grow, leading to more benefits for private clients and the government alike. Contact

# Case Study—**CVE-2020-0688***

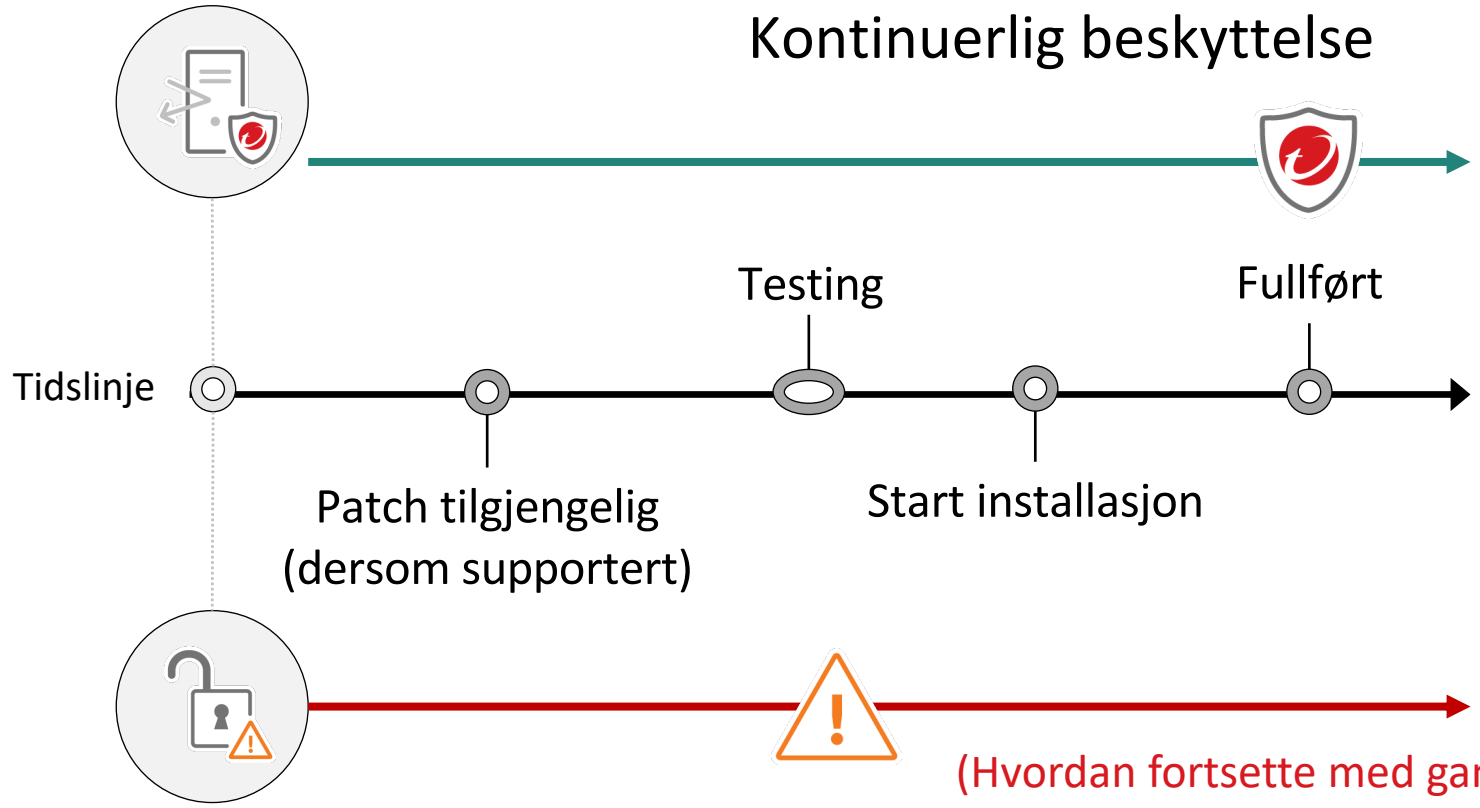



Første aktive angrep 15 mars 2020 (+99 dager)

*Exchange server 2010/13/16/19

# Hvordan > Virtuell patching = beskyttelse mot nulldags sårbarheter/sårbarheter

Virtuell patch tilgjengelig ----→




(Hvordan fortsette med gammalt ræl du ikke blir kvitt….(eller gammal moro du vil ha med videre ☺)

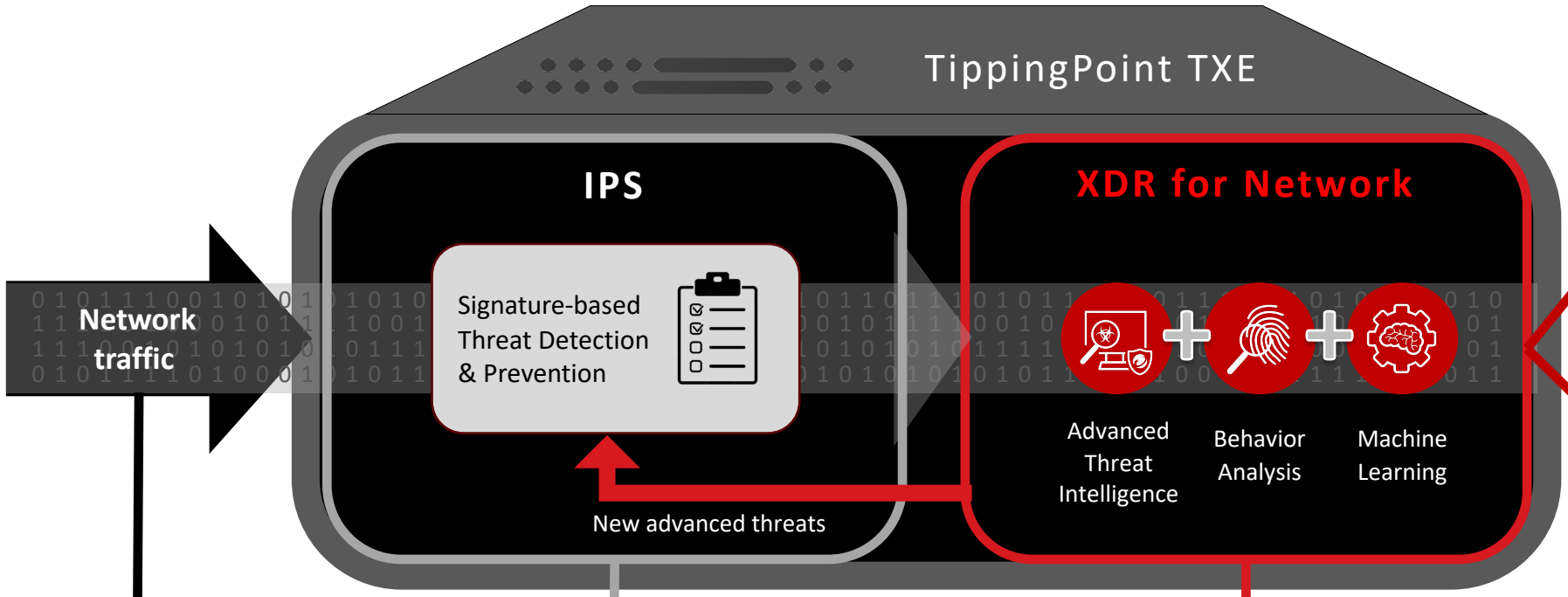
# Hvordan >>>>>> Trend Micro TippingPoint

- The IPS is a “flat” network device
  - Transparant (lag 2)
  - Does not establish connections
  - Does not set up HTTP connections
  - Does not take part in network routing decisions
  - Does not modify frames as they pass through it

# Hva er TippingPoint

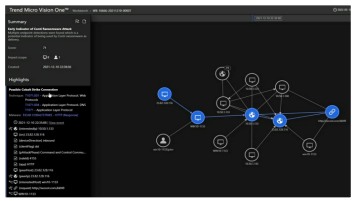
- Kan installereres uten redesign av nettverket eller nedetid
- Sjekker all trafikk som går gjennom den “by default”
  - Trenger minimal config
  - Kan kjøres inn I oppsett I løpet av en 1 dag

# Arkitektur




Network visualization and triage based on historic telemetry and IOCs

Cross-layer correlation for visibility into overall attack surface across a full ATT&CK framework



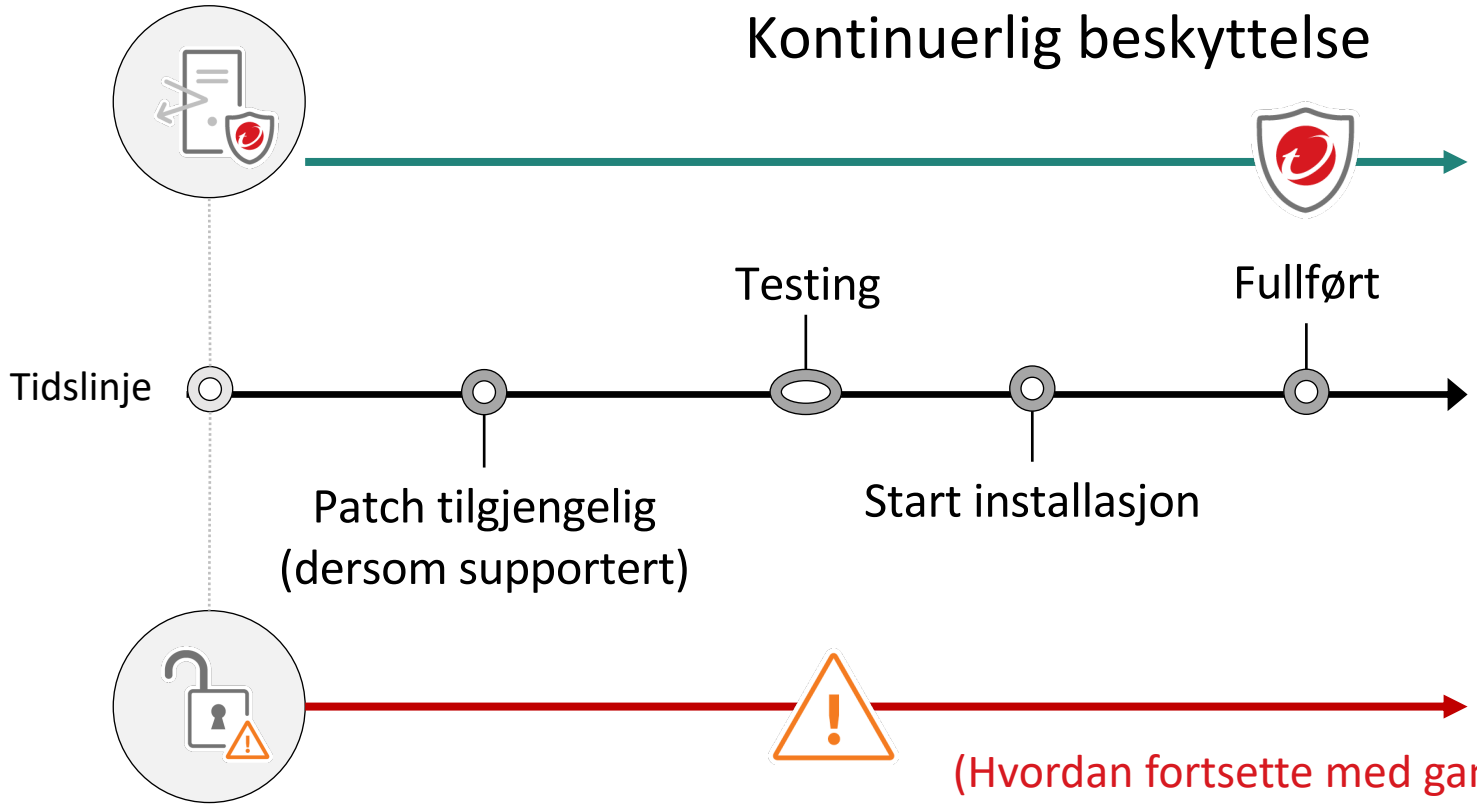
High performance network defense

Detect and block known vulnerabilities ,malware, C&C, and lateral movement techniques

Detect network anomaly and unknown & advanced persistent threats

# Hvordan >>>>>>> First Price og Eldorado-utgaven = XDR, MDR

Virtuell patch tilgjengelig ----→




(Hvordan fortsette med gammalt ræl du ikke blir kvitt….(eller gammal moro du vil ha med videre ☺)

# Hva bør du gjøre, ikke gjøre eller håpe på…?

## Ingenting. Gå videre I livet og glem det

Aksepter risikoen og gå videre I livet. Knapt nok et bra alternativ, men et alternativ!

## Fiks problemet. Patch det

Gitt at det finnes en patch tilgjengelig da…

## Alternative metoder

Open source, “compensation control”, mer tilfeldig virtuell patching

## Ikke råd til at personlig data, helsejournaler eller strøm, VVA og fiber tas ut

**Trend Micro Tippingpoint** for kritisk infrastruktur og nulldags sårbarheter og **XDR** for virtuell patching av sårbarheter

+47 99483521

niels_berthelsen@trendmicro.com

www.zerodayinitiative.com