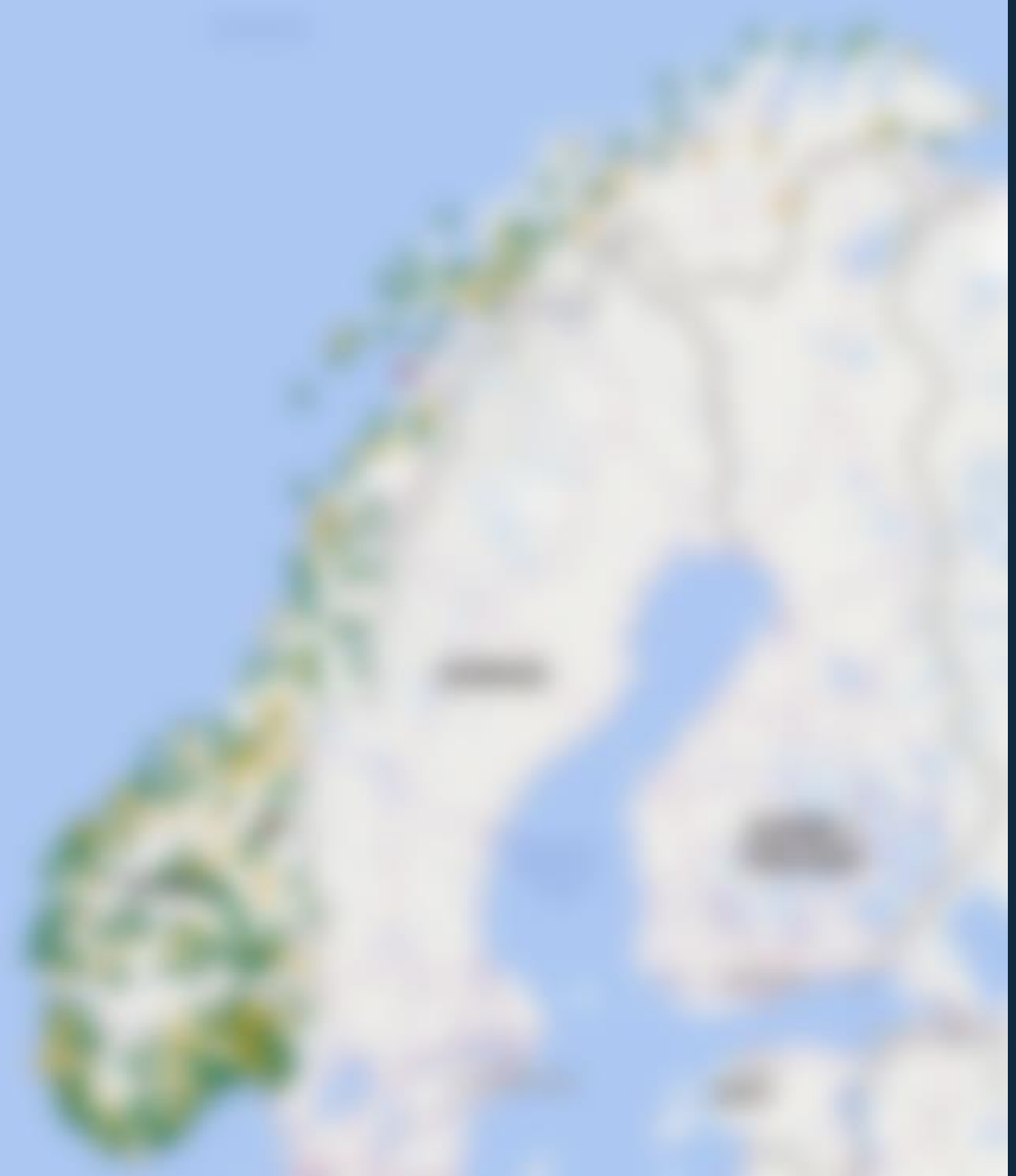


CYBER-X

DFØ/MPS,

Sikkerhetsfestivalen 27. august

André Årnes, Per Jakobsen

Per Jakobsen

DFØ #mps, Seniorrådgiver Cybersikkerhet

Per Jakobsen er tidligere IT-leder med bakgrunn innen informasjonssikkerhet og personvern. Han har tidligere hatt ulike lederstillinger i IT-bransjen innen infrastruktur, web hosting,IT drift og utvikling, men har nå rollen som seniorrådgiver på markedsplassen for skytjenester. Der fokuserer han spesielt på cybersikkerhet i skytjenester. Per bidro til anskaffelsen av en public cloud skytjeneste i Narvik kommune som første offentlige virksomhet i Norge. Dette resulterte i en prinsippavgjørelse hos Datatilsynet om lovlig bruk av skytjenester I offentlig sektor. Per har en sterk interesse for- og fokuserer på skykontrakter for verktøy og tjenester innen sikkerhet og personvern og hvordan disse kan bidra til bedre sikkerhet og personvern ved bruk i offentlig forvaltning.

André Årnes

Partner Cyber Security @ WLC og Professor II @ NTNU

André Årnes er medeier og partner i White Label Consultancy og Professor II ved NTNU. Han har tidligere hatt rollen som SVP og Group Chief Security Officer (CISO/CSO) i Telenor Group (2015 – 2022), som CIO i Telenor Global Shared Services og som spesialetterforsker innen Digital Forensics og datakriminalitet ved Kripos / Økokrim. André har en sterk faglig interesse for sikkerhet, med fokus på sikkerhetsledelse og digital etterforskning. Han har redigert to akademiske lærebøker innen fletet. «Digital Forensics» (Wiley, 2018) og «Cyber Investigations (Wiley, 2022). Han har siden 2022 bistått DFØ og Markedsplassen for Skytjenester som strategisk sikkerhetsrådgiver.

Markedsplassen for skytjenester skal bidra til styrking av sikkerhet i det offentlige Norge gjennom veiledning, digitale tjenester og skykontrakter.

Agenda

Markedsplassen for Skytjenester (MPS)

- Mandat
- Forretningsområder

CyberX – cybersikkerhet og personvern for offentlig sektor

- Utprøvingsprosjekter
- Portefølje
- Referansearkitektur

Lansering av ny avtale for Cyber Risk Score tjeneste

- Signering av ny avtale
- Bakgrunn
- Hvordan ta i bruk tjenesten?

Markedsplassen for Skytjenester (MPS)

Norwegian agency for public and financial management

Markedsplassen er opprettet på bakgrunn av Nasjonal strategi for bruk av skytjenester

Eies av Finansdepartementet. Styres av DFD

Tildelingsbrev fra Finansdepartementet

Veiledning, anskaffelse, informasjonssikkerhet og oversikt over markedet

Fullmakt til å inngå statlige fellesavtaler ved kgl. res. av 3. september 2021

#MPS | Forretningsområder

CIPS
Cloud Infrastructure and Platform Servces

FinOps
Financial Operations

CyberX
Cyber Security & Data Protection

Cloud R&A
Cloud Research & Advisory

Digital
Digital web services

Balanserte vilkår
Pris/kostnad
Effektive avrop
Kostnads-optimalisering, klima og miljø
Cybersikkerhet og GDPR
Fleksibilitet

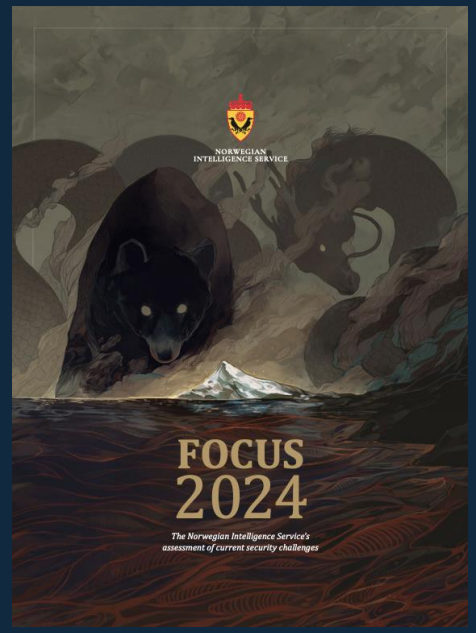
CyberX - Cybersikkerhet og personvern for offentlig sektor

Norwegian agency for public and financial management

Norsk offentlig sektor utsettes for et stadig mer utfordrende trusselbilde og det er behov for en strategisk og risikobasert satsning på cybersikkerhet basert på målbare fakta og informerte beslutninger

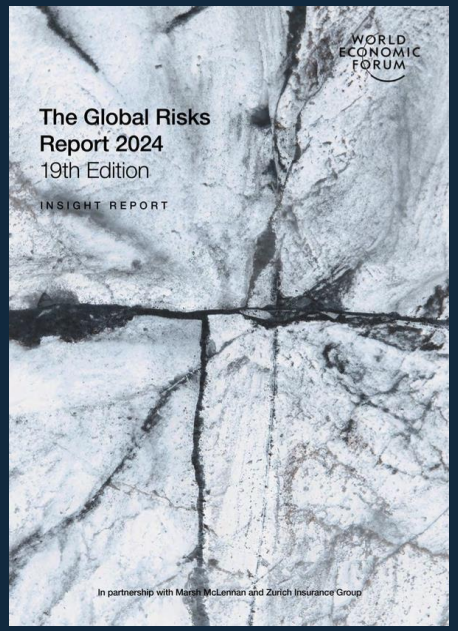
| Demokratiet er under press | Spionasje og cyberoperasjoner | Innsidere | Påvirkningsoperasjoner | Kritisk infrastruktur og verdier må sikres | Anskaffelser, oppkjøp og investeringer | Droner | Kunstig intelligens | Nye sårbarheter vokser frem | Sikkerheten I cyberdomenet må styrkes |

| Statlig etterretningsaktivitet | Russland, Kina, Iran og Nord-Korea | Norge er et mål | Kritisk infrastruktur og teknologi | Trusselen i cyberdomenet er dynamisk og I stadig utvikling | Offentlig forvaltning og politiske beslutningstakere er et mål | Digital industri | Verdikjedeangrep | Kunstig intelligens | Digital rekruttering av kilder |

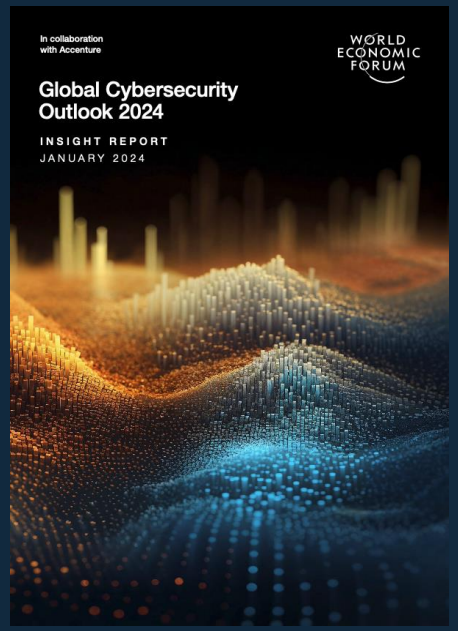


| Endrede sikkerhetspolitiske rammebetingelser | Etterretningstrusselen | Russland | Kina | Utsatte verdikjeder og infrastruktur | Kampen om kunnskap, eierskap og teknologi |

Det globale risikobildet samsvarer med det norske – myndigheter og virksomheter har manglende oversikt og er sårbare for cyberangrep, verdikjedeangrep og desinformasjon



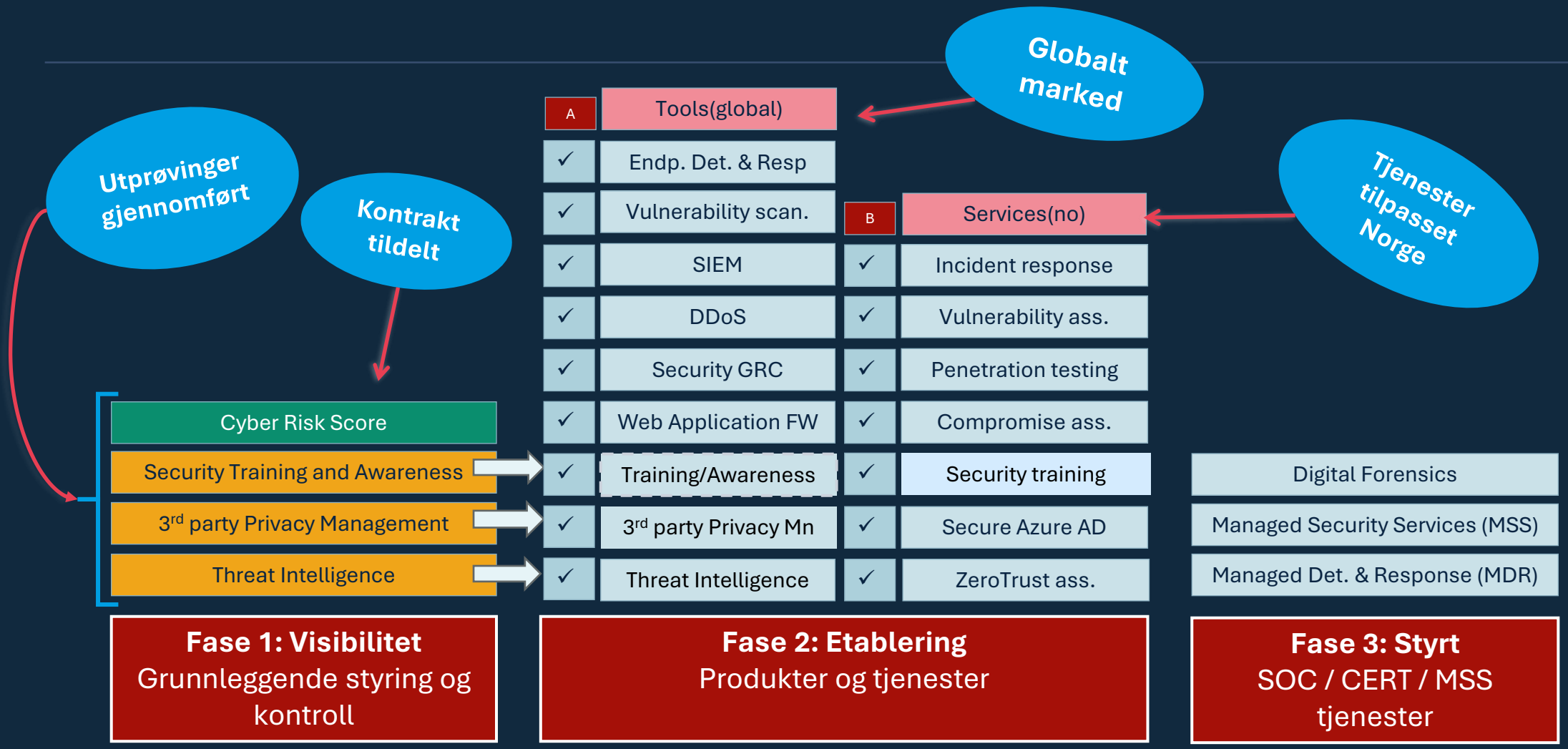
| Misinformasjon og desinformasjon | Cyber insecurity | Uheldige konsekvenser av AI-teknologi | Behov for investering I cybersikkerhet I myndigheter, selskaper og militære |



| Cyber inequality – økende forskjeller mellom organisasjoner | Cyber skill shortage – mangel på kompetanse og ressurser | Sårbare verdikjeder – 54% sier at de har mangelfull innsikt og forståelse |

| Verdikjedeangrep i programvare | Desinformasjonskompanjer | Digital overvåkning (personvern) | Menneskelige feil og legacy-systemer I cyber-fysiske systemer | Målrettede angrep på smart-teknologi | Manglende oversikt over romfartsinfrastruktur | Avanserte hybride trusler | Kompetansermangel | ICT / skytjenester som single-point of feiluraSkill shortage | Misbruk av AI |

#MPS | Portefølje av produkter og tjenester for offentlig sektor



#MPS | Utprøvinger med formål om å få bedre innsikt

Cyber Risk Score

Security Training and Awareness

3rd party Privacy Management

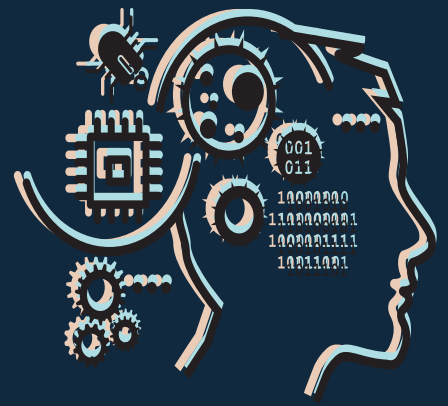
Threat Intelligence

Fase 1: Visibilitet
Grunnleggende styring og kontroll

Cyber Risk Score

Hvilken effekt kan bedre innsikt i egen sårbarhet på internett ha med hensyn på å treffe risikoreduserende tiltak?

Threat Intelligence



Kan bedre kunnskap om **trusselbildet** bidra til raskere og mer målrettet problemløsning innen Cybersikkerhet

Privacy 3rd party

Kan bedre oversikt og innsikt i leverandør-kjedenes personvern bidra til bedre og mindre ressurs-krevende etterlevelse av GDPR for virksomhetene?

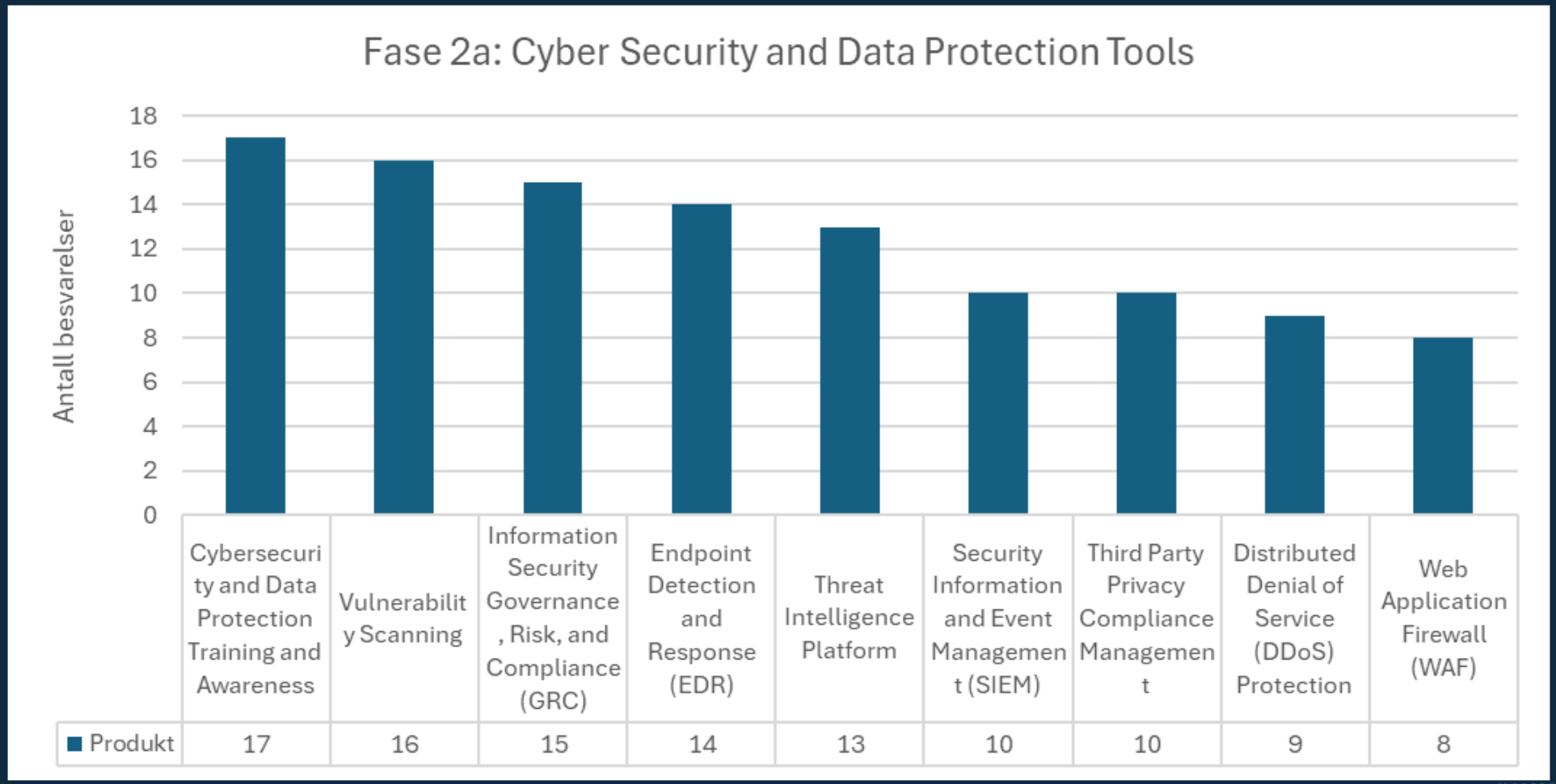
Awareness

Kan bevisstgjøring med kurs innen cybersikkerhet bidra i virksomheten til å bygge kompetanse for en robust sikkerhetskultur?

#MPS | Markedsundersøkelse gjennomført sommeren 2024

A	Tools(global)
✓	Endp. Det. & Resp
✓	Vulnerability scan.
✓	SIEM
✓	DDoS
✓	Security GRC
✓	Web Application FW
✓	Training/Awareness
✓	3rd party Privacy Mn
✓	Threat Intelligence

Fase 2: Etablering
Produkter og tjenester



#MPS | Prinsipper for porteføljе av produkter og tjenester for offentlig sektor

- ✅ Skybaserte. Produkter og tjenester skal være skybaserte og må støtte anvendelse av skytjenester, men også støtte hybrid og on-site infrastruktur.
- ✅ Automatisert. Produkter og tjenester skal tilrettelegge for en høy grad av automatisering.
- ✅ Nasjonal situasjonsforståelse. Produkter og tjenester bør tilrettelegge for aggregert informasjon for sentrale funksjoner (f.eks. NSM og CERTer).
- ✅ Flere leverandører. Målbildet er, hvor det er relevant, å etablere avtaler med flere leverandører innenfor kategoriene og dermed tilrettelegge for fleksibilitet med hensyn på ulike modenhetsnivå.
- ✅ Grunnleggende sikkerhetskrav. Alle produkter og tjenester skal oppfylle sikkerhetskrav basert på for eksempel ISO 27001, NIST CSF 2.0, NSM Grunnprinsipper 2.1, samt lovpålagte krav og andre relevante standarder.

#MPS | Referansearkitektur for sikkerhet i anskaffelser for skytjenester v0.9

Prinsipielle krav	**Overordnede krav til kontraktsmessige forhold**
Basiskrav	**Obligatoriske krav til cybersikkerhet**
Tilleggskrav	**Leverandørens forslag til cybersikkerhetsarkitektur basert på kundens behov**

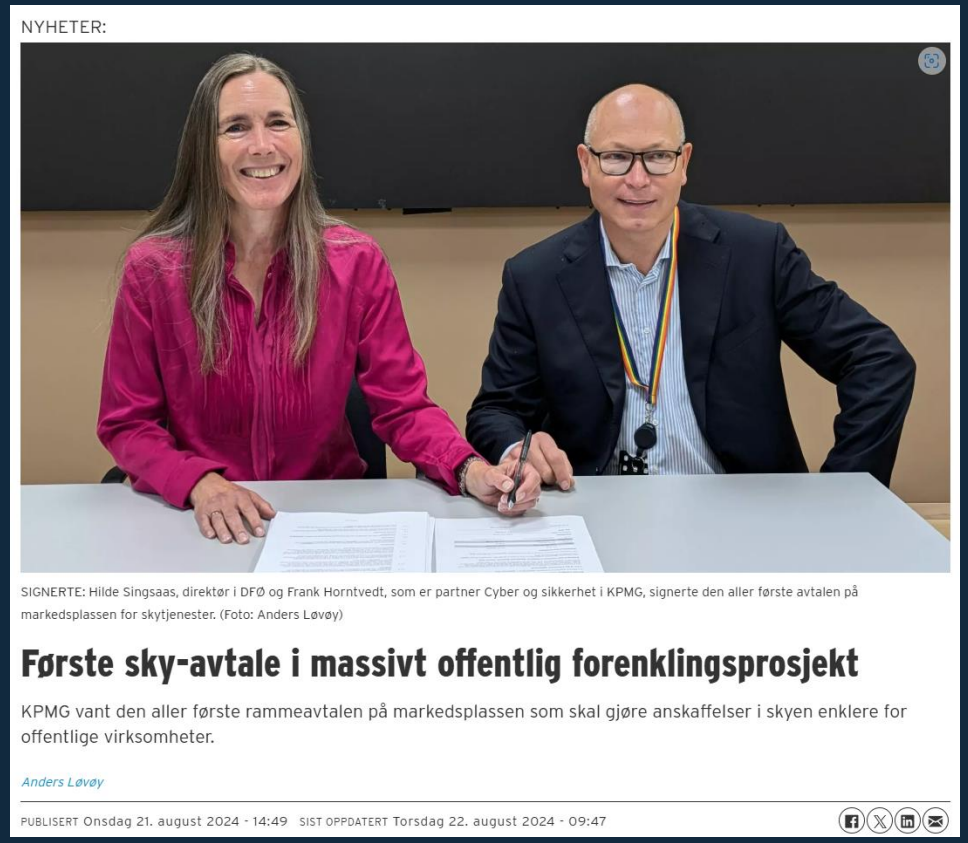
#mps

Cyber Risk Score

Norwegian agency for public and financial management

Cyber Risk Score – avtalen signert onsdag 21. August 2024

- Cyber Risk Score tildelt KPMG/MasterCard med tjenesten RiskRecon
- Rammeavtale med formål å måle og styrke informasjonssikkerhet i offentlig sektor.
- Tjenesten tilrettelegger for:
  - Nasjonal situasjonsforståelse
  - Virksomhetsstyring
  - Operativ bruk
- Ambisjonen er at alle skal med!



NYHETER:

SIGNERTE: Hilde Singsaas, direktør i DFØ og Frank Horntvedt, som er partner Cyber og sikkerhet i KPMG, signerte den aller første avtalen på markedsplassen for skytjenester. (Foto: Anders Løvøy)

Første sky-avtale i massivt offentlig forenklingsprosjekt

KPMG vant den aller første rammeavtalen på markedsplassen som skal gjøre anskaffelser i skyen enklere for offentlige virksomheter.

Anders Løvøy

PUBLISERT Onsdag 21. august 2024 - 14:49 SIST OPPDATERT Torsdag 22. august 2024 - 09:47

Kilde: Computerworld, 21.08.2024

#MPS| Erfaring fra Ringerike kommune om utprøvingen av Cyber Risk Score

Voldsom interesse for nytt skyprogram: – Kjipt å være flagget rødt når naboen er grønn, mener IT-sjef

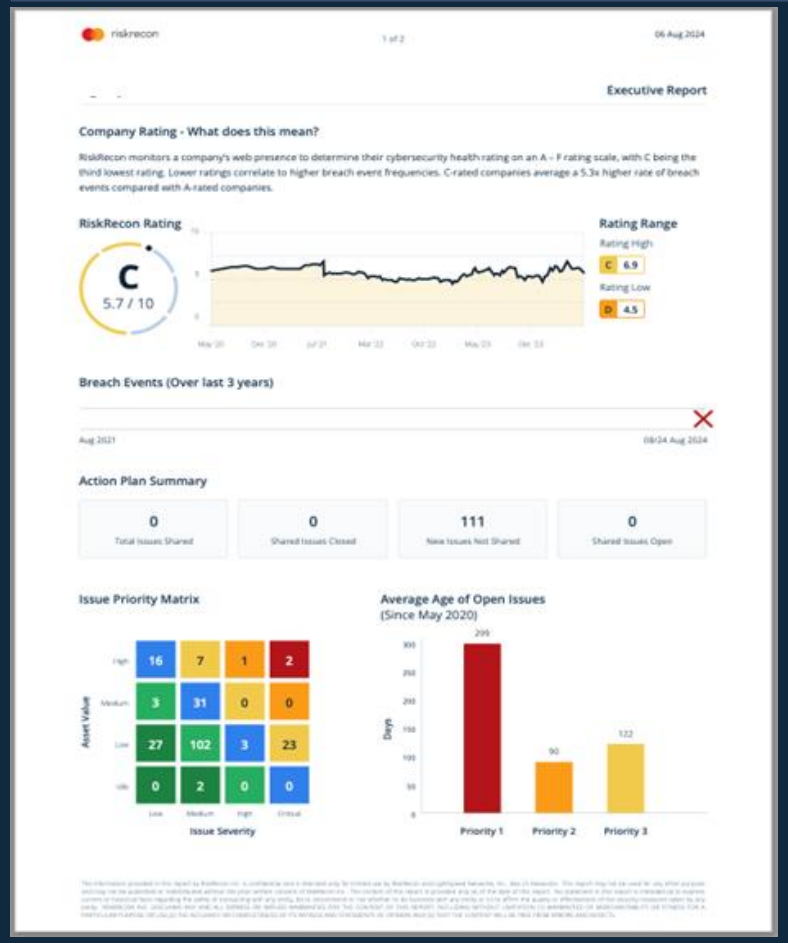
Markedsplassen for skytjenester (MPS) er er i gang med å sjekke interessen for en ny skytjeneste som kartlegger cyberriskofaktorer i offentlig og statlig sektor. Styreleder i offentlig sikkerhetsforening mener programmet er et «must».

Torkjell Dahl er IT-sjef i Ringerike kommune. Her sammen med informasjonssikkerhetsansvarlig Axel Sjøberger. I tillegg til å være IT-sjef, er Dahl styreleder i sikkerhetsorganisasjonen KiNS, som har over 300 kommuner, fylkeskommuner og interkommunale selskaper som medlemmer. *Foto: Espen Ødegård, Ringerikes Blad*

Kilde: Digi.no

Cyber Risk Score gir en helhetlig vurdering av sikkerhetsnivået sett fra internett og hjelper virksomheten med å prioritere tiltak for å beskytte seg mot potensielle trusler.

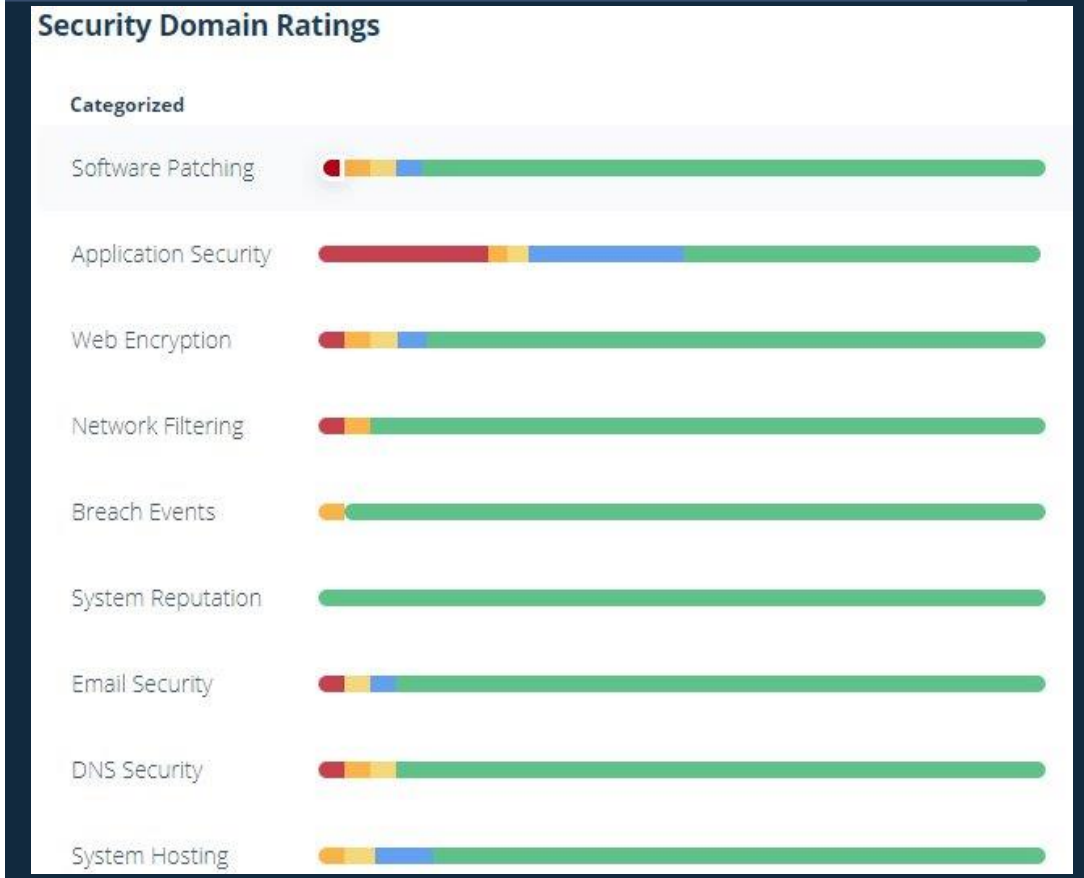
Hva gjør tjenesten for virksomhetene



- Kartlegger virksomhetens systemer, risiko og sårbarhet på Internett
- Beregner en risikoscore som kan følges opp over tid og sammenlignes med andre
- Verktøy for oppfølging av identifiserte risiko og sårbarheter
- Funksjonalitet for dashboards, varsling og rapporter for virksomhetsledelse og operativt bruk hos IT og sikkerhet
- Oppfølging av leverandører og tredjeparter med tilsvarende funksjonalitet som virksomheten selv
- Merk at verktøyet krever en systematisk tilnærming, og det er bare et av flere verktøy i verktøykassa!

Oversikt over statlige virksomheter

Oversikt over kommuner og fylkeskommuner

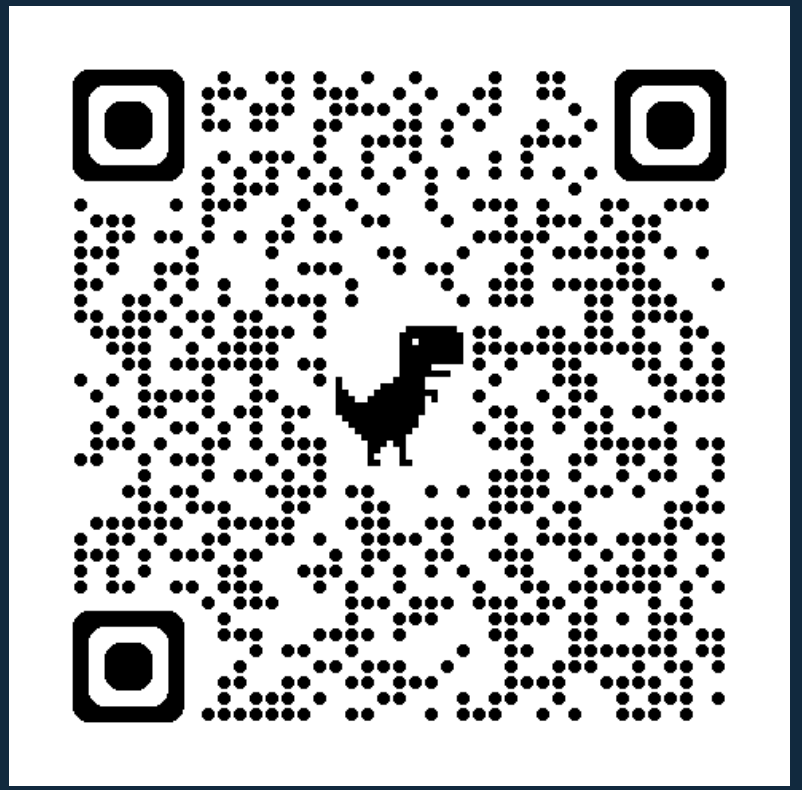


Hvordan ta i bruk Cyber Risk Score?

Nærmere informasjon om avtalen:

Cyber Risk Score - Informasjon om avtalen

Alle statlige virksomheter som er omfattet av DFØs fullmakt kan gjøre avrop.



Takk for oss :)

Følg oss på markedsplassens skyforum, **18.09.2024**

Markedsplassen.anskaffelser.no

Vedlegg

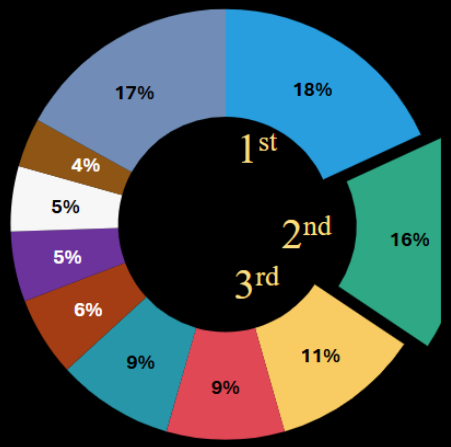
Informasjon om Cyber Risk Score – RiskRecon

Norwegian agency for public and financial management

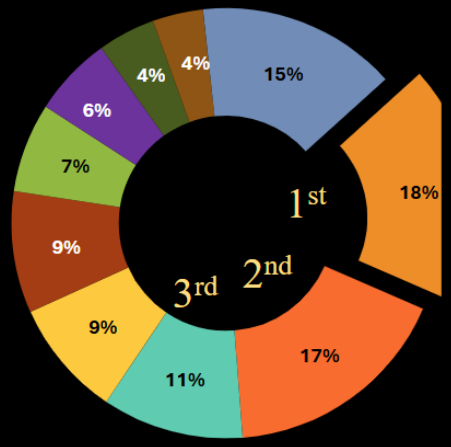
Public industry is the most targted industry in Norway, while ranking second in Europe

Events per Industry

Europe



Norway



Technology | Services | Research | Transportation
Public | Media | Healthcare | Other
Financial | Industrial | Education

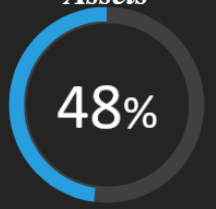
***Industries below 4% grouped under «Other» category**

- *Communication, Energy, Retail, Entertainment, Hospitality, Pharmaceuticals*

Source: Mastercard Cyber Insights Data. Based on data for the period Jan 2024 – Aug 2024

Most popular Assets, Actors and Methods for Public Industry

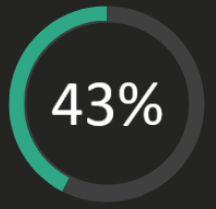
Assets



of events targeting **Physical Assets** and **Business Systems**

European average: 36%

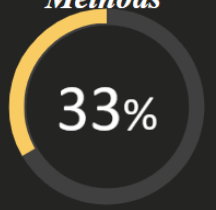
Actors



of events were attributed to **Cyber Terrorist** and **Black Hat**

European average: 26%

Methods



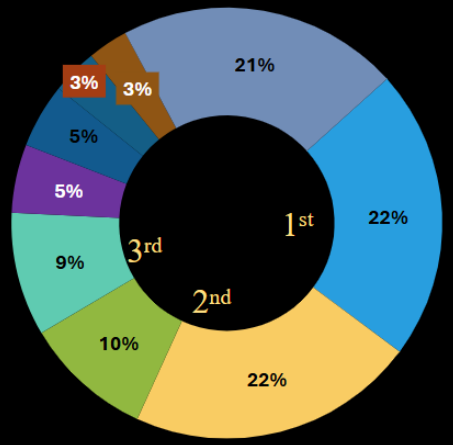
of attacks were performed through **Malware** and **Email Phishing**

European average: 32%

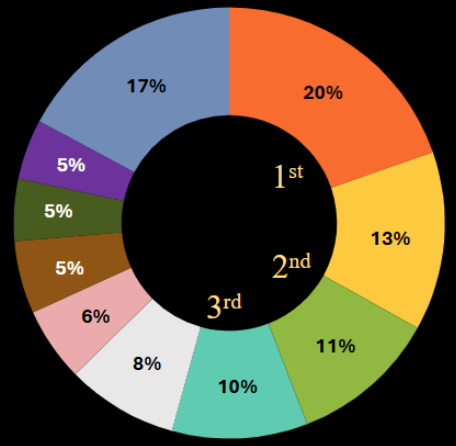
While there is no change in the ranking of the top **three** attacks, **web application** attacks are more prevalent in Norway than in Europe

Attack Methods – All Industries

Europe



Norway



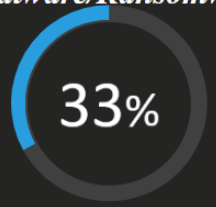
Malware
Ransomware
Reconnaissance
Email Phishing
Denial of Service
Pretexting
Command & Control
Supply Chain Attack
Web Application Attack
Mobile Devie Attack
Other

*** «Other» category contains;**
- *Credential Access, Network Attack, Physical Attack, Persistence, Privilege Escalation, Injection, Adversary in the Middle, Legitimate Tool*

Source: Mastercard Cyber Insights Data. Based on data for the period Jan 2024 – Aug 2024

Most common Tactics, Techniques, and Procedures

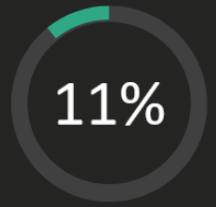
Malware/Ransomware



of events mostly targeting **Government Agencies, Software,** and **Construction and Engineering**

European average: 44%

Reconnaissance



of events mostly targeting **Professional Services, Software,** and **Advertising**

European average: 10%

Email Phishing

of events mostly targeting **Government Agencies, Software,** and **Construction and Engineering**

European average: 9%

FEATURES – OWN ENTERPRISE

Monitor the security performance of the IT assets in your organization

Better Manage Your IT and Security Profile

- RiskRecon provides continuous IT profiling and security analytics, offering detailed visibility into your Internet-connected systems, including their configurations and compliance with security requirements, and enabling teams to identify issues, prioritize responses, and act efficiently.

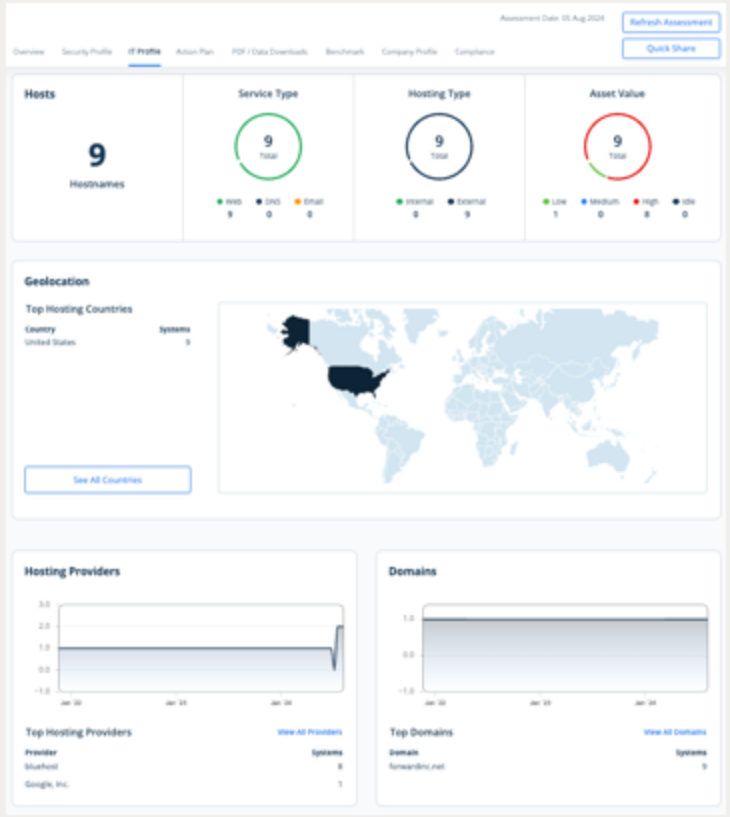
Discover and Monitor Your Internet Assets

- RiskRecon offers comprehensive, continuously updated visibility into all Internet-connected assets, helping IT and security teams discover and protect shadow and forgotten IT assets, both on their network and in the cloud, using advanced Internet asset hunting analytics.

Know the Risk Profile of Your Internet Assets

- RiskRecon provides continuous insight into the risk profile of each Internet asset, helping risk analysts and security teams identify where sensitive data and functionalities are exposed, prioritize risk management efforts, and comply with regulations like GDPR and CCPA.

Did you know?
Companies with good cybersecurity hygiene have **35X** lower frequency of destructive ransomware events.



riskrecon by Mastercard

Easily understand the security posture of your internal IT systems

RiskRecon dashboards provides enhanced insights into the risk within a company's portfolio with active information widgets that facilitate viewing additional details and systems linked to their security profile. The dashboard can be custom-tuned to match the needs of a client and is filterable based on the needs of an organization.

Features of the RiskRecon dashboard:

- **Real-Time Monitoring**
  - Continuous surveillance of security incidents and vulnerabilities.
- **Customizable Views**
  - Tailored dashboards for different roles and teams.
- **Comprehensive Data Integration**
  - Aggregates data from multiple sources for a unified view.
- **Visual Analytics**
  - Intuitive charts, graphs, and heatmaps for easy data interpretation.
- **Automated Alerts & Notifications**
  - Immediate alerts for critical issues and anomalies.

Did you know?
Companies with cyber risk rating of 'F' are **4x** more likely to experience a data loss event according to RiskRecon analysis.

riskrecon by Mastercard

FEATURES – EXECUTIVE REPORTING

Key Insights for Leadership Teams with RiskRecon Executive Reports

Did you know?
Cyberattacks targeting vulnerabilities have increased **180%** YoY.

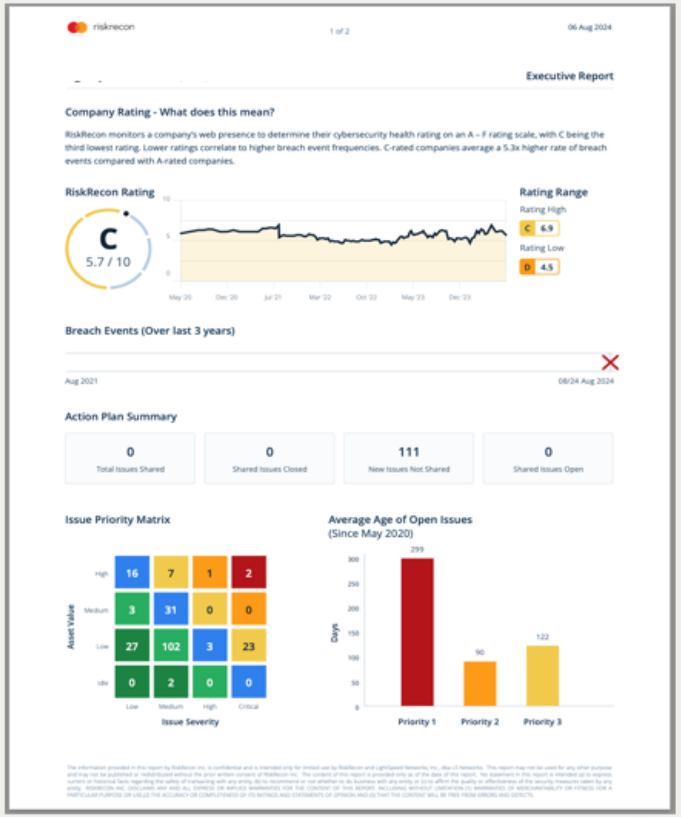
Benefits of RiskRecon Executive Reports

Comprehensive Overviews
- Provides a clear, high-level summary of the organization's cybersecurity posture.
- Highlights critical security risks and areas of concern.

Informed Risk Decisions
- Empowers leadership with data-driven insights to make informed security investments.
- Facilitates alignment on risk tolerance and cybersecurity goals.

Enhanced Visibility
- Offers an aggregated view of cybersecurity performance across all business units.
- Allows tracking of progress and effectiveness of security initiatives.

Strategic Planning
- Assists in resource allocation and strategic planning for cybersecurity improvements.
- Helps in aligning cybersecurity efforts with overall business objectives.



riskrecon by

FEATURES – PRIORITY MATRIX

Optimize Your IT Resources and Take Strategic Action

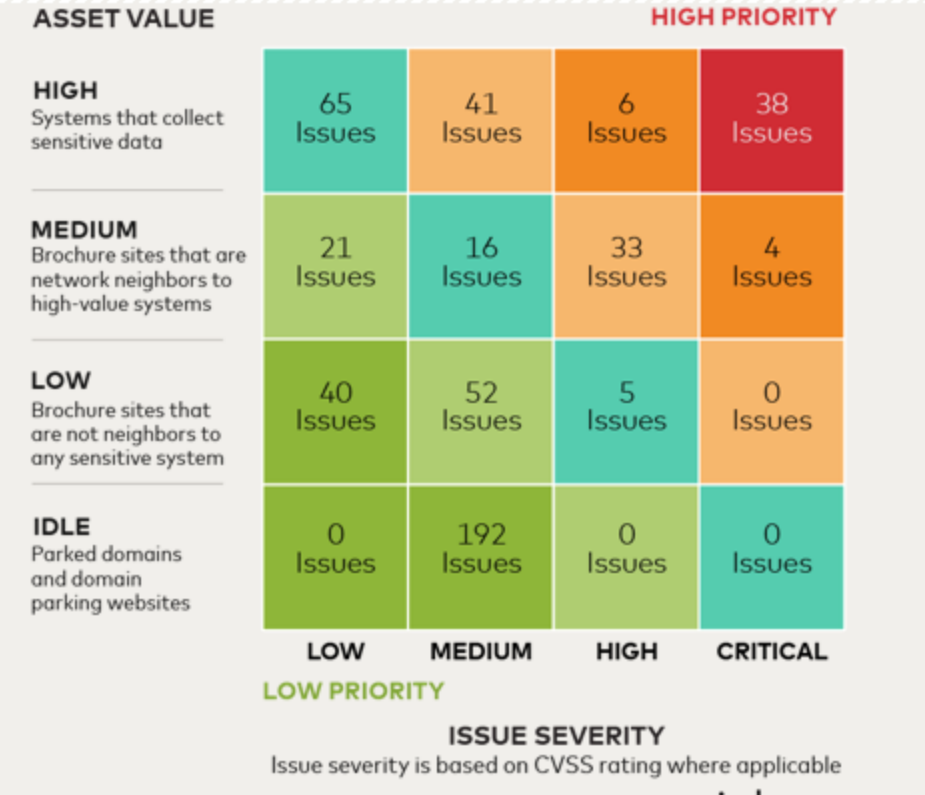
Deep Asset Discovery

- Our asset discovery process integrates analyst-assisted machine learning models tailored for each monitored company, ensuring accurate attribution of company assets amid evolving shifts over time.

Automated Risk Prioritization

- RiskRecon automatically prioritizes every finding based on issue severity and asset value. The value at risk for each system is determined by discovering:
  - Authentication
  - transaction capabilities
  - data types collected, such as:
    - email addresses
    - credit card numbers
    - names

Did you know?
41B connected devices in 2023 with an **18%** higher growth rate than 2022.



riskrecon by

Keep your organization secure with detailed, customizable action plans

Automated, Custom Action Plans

- Automatically create action plans tuned to your risk priorities. Our assessments have a share-ready action plan containing only the issues that violate your risk policy.

Collaboration and Data Sharing

- Customized viewing and reports that includes findings, evidence, recommendations for solving the issues - built according to client's risk policies with no time limit or added costs.

Leverage the Power of Machine Learning

- RiskRecon's machine learning technology identifies issues within a vendors' ecosystem and builds its reports based on issue severity and the sensitivity in which the systems exist.

Third-party Risk Remediation

- RiskRecon's actions plans can be shared with vendors who have access to critical company data; to help ensure the security of your business is not impacted by a third-party.

Did you know?
The average cost of a third-party data breach is **€1.3M**.

riskrecon by