Deloitte.

**Deloitte Security Intelligence Framework**

Etablering, vedligeholdelse og drift af en SIEM intelligence overvågningsplatform

# Udvikling fra reaktiv til proaktiv Cyber Risk Management

Flere og flere organisationer stræber efter at opnå et modenhedsniveau indenfor informationssikkerhed, hvor trusler korreleres og proaktivt styres i et Security Operations Center (SOC) for derigennem kontinuerligt at spore hændelser, registrere mønstre og abnormiteter og gennemføre statistisk analyse, der gør organisationen i stand til proaktivt at overvåge trusler.

Deloitte Security Intelligence Center har de nødvendige kompetencer til at indsamle præcise, relevante og rettidige logs for derigennem dels proaktivt at kunne afværge en svaghed på en kritisk enhed, før en hændelse når at opstå, dels at analysere og hurtigst muligt bringe organisationen tilbage til normal drift, når en hændelse er opstået.

Deloitte Security Intelligence Framework tager udgangspunkt i en risikobaseret og holistisk informationssikkerhedstilgang, som sikrer at logs på tværs af organisationens systemer omdannes til meningsfulde og forretningsorienterede indsigter i forhold til den enkelte kundes Cyber Risk Management-system.

## Mangler ved traditionelle risikostyringssystemer

Mange virksomheder har i dag en grundlæggende reaktiv og deskriptiv sikkerhedstilgang, der består af traditionelle signaturbaserede detektionsmekanismer til styring af sikkerhedsrelaterede hændelser samt trusselsrapportering. Disse mekanismer er alle nødvendige, men hver for sig giver de ikke tilstrækkelig beskyttelse mod nutidens trusselsniveau. Nedenfor ses en beskrivelse af nogle af manglerne ved en traditionel reaktiv tilgang til risikostyring af organisationens it-sikkerhedsdrift.

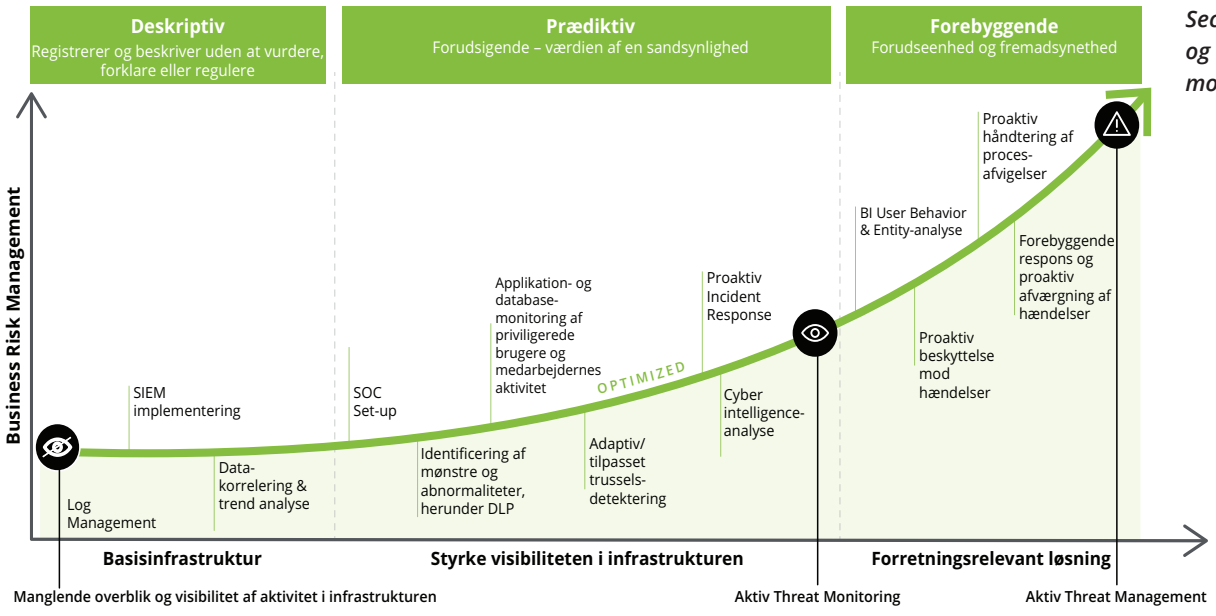
**Ineffektiv prioritering -** Det er nærmest umuligt at beskytte og fortolke alle ustrukturerede og strukturerede data, som strømmer igennem organisationen hver eneste dag. Det er derfor essentielt, at organisationen kan vurdere data ud fra kritikalitet i forhold til virksomhedens risikobaserede prioriteter.

**Manglende forebyggelse og rettidig omhu -** Udover at beskytte data skal organisationer også kunne tolke og reagere på tegn, som tyder på, at kritiske data er udsat for en forhøjet risiko, inden en sikkerhedshændelse indtræffer, hvilket kræver rettidig omhu og en proaktiv risikostyring.

**Manglende overblik og visibilitet -** Når en sikkerhedshændelse indtræffer, er det vigtigt, at sikkerhedsanalytikere har et klart overblik og visibilitet på tværs af hele organisationens infrastruktur for at kunne vurdere hændelsens kritikalitet – lige så vel som det er vigtigt, at sikkerhedsanalytikerne hurtigt kan få overblik over, om sikkerhedshændelsen kan ramme organisationens kritiske data og systemer.

**Upålidelig teknologi skaber falsk tryghed -** Manglende pålidelig teknisk automatisering med udskilning af falske / positiver i systemerne gør, at analytikere har en tendens til at formode, at en alarm ikke er reel, eller at den ikke er vigtig, hvilket i mange tilfælde kan være faretruende.

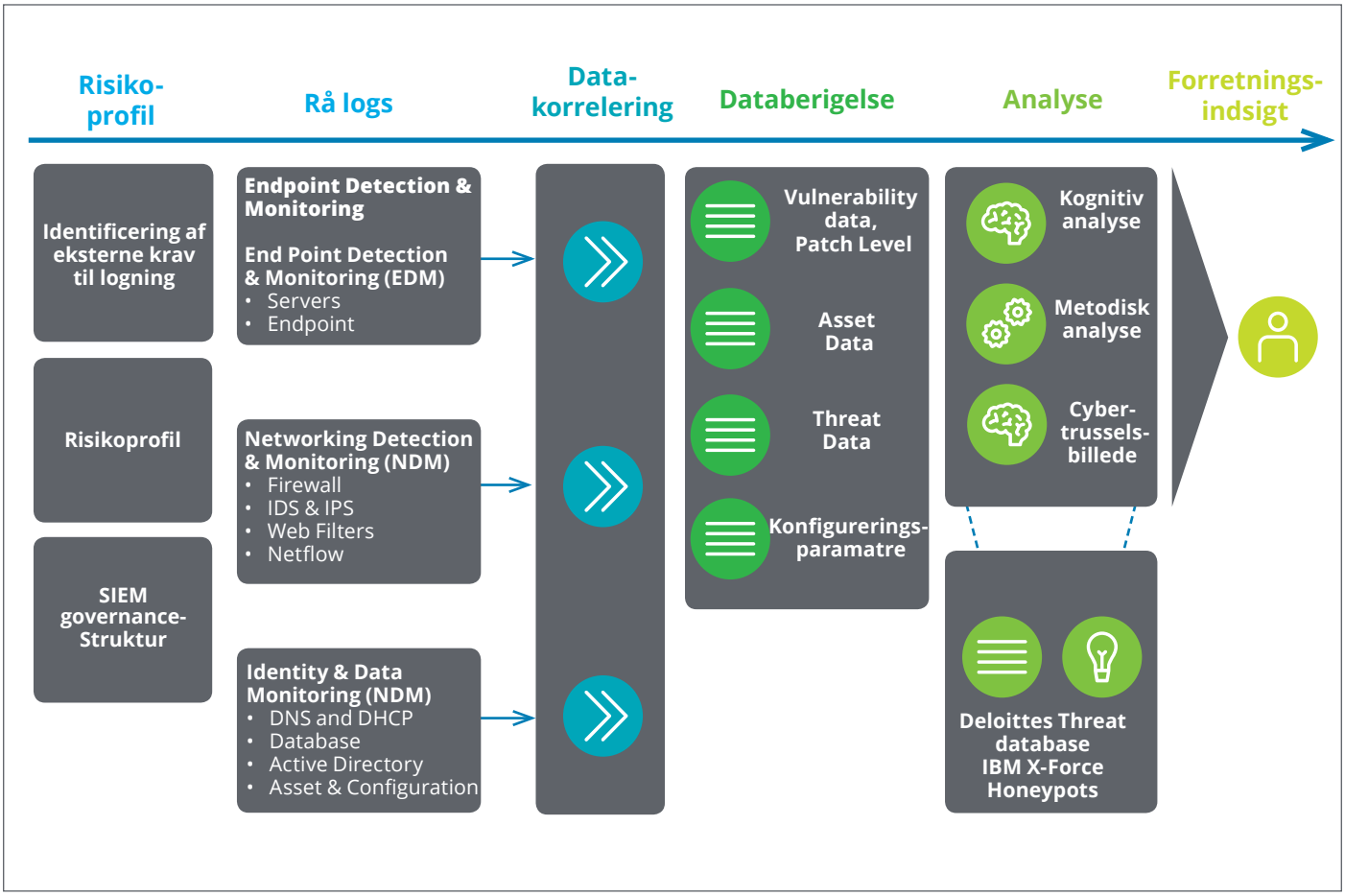
**Manglende ensretning i hele organisationen -** Manglende dokumentation af governance-struktur og kommunikation af organisationens retningslinjer indenfor informationssikkerhed svækker i mange tilfælde organisationens datasikkerhed.




***Security Intelligence og Operations modenhedskurve***

**Deloitte Security Intelligence Framework** leverer en altomfattende overvågningsplatform indeholdende fastlæggelse af behov, udarbejdelse af governancestruktur og drift af en cyberintelligens. Platformen monitorerer og rapporterer et risikobaseret og holistisk billede af den enkelte kundes it-sikkerhedshændelser, overholdelse af compliance-krav samt modenhedsniveau indenfor organisationens Cyber Risk Management.

**Deloitte Security Intelligence Framework**




**Why Deloitte Managed Security Servies**

- Deloitte sikrer en proaktiv udvikling af den enkelte kundes Security Intelligence Framework med udgangspunkt i innovative teknologier.
- Deloitte sikrer skabelse af ny visibilitet af organisationens daglige it-sikkerhedshændelser, herunder overblik over nye mønstre og sammenhænge i organisationens it-infrastruktur.
- Via Deloittes mere end 20 globale Service Operation Centres, (SOC) leverer vi den nyeste cyberviden i realtid til vores kunder.
- Deloitte leverer it-sikkerhedsovervågning med værdiskabende forretningsindsigt i denenkelte organisations risikostyringssystemer.

Deloitte.

Om Deloitte
Deloitte leverer ydelser indenfor Revision, Skat, Consulting og Financial Advisory til både offentlige og private virksomheder i en lang række brancher. Vores globale netværk med medlemsfirmaer i mere end 150 lande sikrer, at vi kan stille stærke kompetencer til rådighed og yde service af højeste kvalitet, når vi skal hjælpe vores kunder med at løse deres mest komplekse forretningsmæssige udfordringer. Deloittes ca. 200.000 medarbejdere arbejder målrettet efter at sætte den højeste standard.

Deloitte Touche Tohmatsu Limited
Deloitte er en betegnelse for Deloitte Touche Tohmatsu Limited, der er et britisk selskab med begrænset ansvar, og dets netværk af medlemsfirmaer. Hvert medlemsfirma udgør en separat og uafhængig juridisk enhed. Vi henviser til www.deloitte.com/about for en udførlig beskrivelse af den juridiske struktur i Deloitte Touche Tohmatsu Limited og dets medlemsfirmaer.