

## HVA ER «VULNERABILITY MANAGEMENT»

Sårbarhetshåndtering er den pågående praksisen med å identifisere, prioritere og utbedre sårbarheter.

Det kan også beskrives som en proaktiv og systematisk respons på sårbarheter i ditt IT-miljø. Implementering av sårbarhetshåndtering er avgjørende for organisasjoner som ønsker å øke datasikkerhet og minimere angrepsflaten.

## HVORDAN FUNGERER DET

### 1. OPPDAGELSE

**Forstå hvilke fysiske og logiske enheter som finnes** i IT-miljøet, både fysiske og virtuelle nettverk, skynettnettverk eller andre potensielle angrepsflater som kan utnyttes i et dataangrep.

**Kartlegg enheter** og opprett en database for å skanne etter sårbarheter.

**Bruk «threat hunting» informasjon**, sårbarhetsdata og skannere for å lage en oversikt for patching.

### 2. EVALUERING

**Finn ut hvor du skal bruke ressurser på datasikkerhet** for å redusere potensielle risikoer. Sårbarhetene blir rangert fra høyeste til laveste risiko, avhengig av flere faktorer.

### 3. HÅNTERING

**Fokuser på sårbarheter som utsetter organisasjonen** for de største risikoene - inkludert utbedring av kritiske sårbarheter og eliminering av falske positiver.

### 4. RAPPORTERING

**Sørg for klar internt kommunikasjon via rapportering.** Informasjon om sårbarheter bør være forståelig nok til å kunne tolkes av alle i organisasjonen.

## PROAKTIV TRUSSELJAKT

Å skape et robust sikkerhetsforsvar krever at du tar initiativ. Bruk proaktive sikkerhetstiltak for å finne sikkerhetshull før de utnyttes. Sårbarhetshåndtering krever en kontinuerlig tilnærming til IT-sikkerhet på tvers av organisasjonen.

Vårt «Vulnerability Management» produkt bidrar til proaktiv trusseljakt i din organisasjon!



### CLOUD SCANNING

Skyskanning gir innsyn i skytjenester og deres sikkerhetskonfigurasjoner



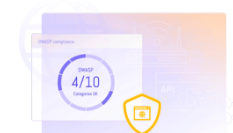
### NETWORK SCANNING

System- og nettverkskanning dekker hele IT-infrastrukturen



### API SCANNING

Sikre REST, GraphQL og SOAP endepunkter med API-scanning.



### WEB APPLICATION SCANNING

Webapp-skanning oppdager svakheter der IT-miljøet er mest sårbart