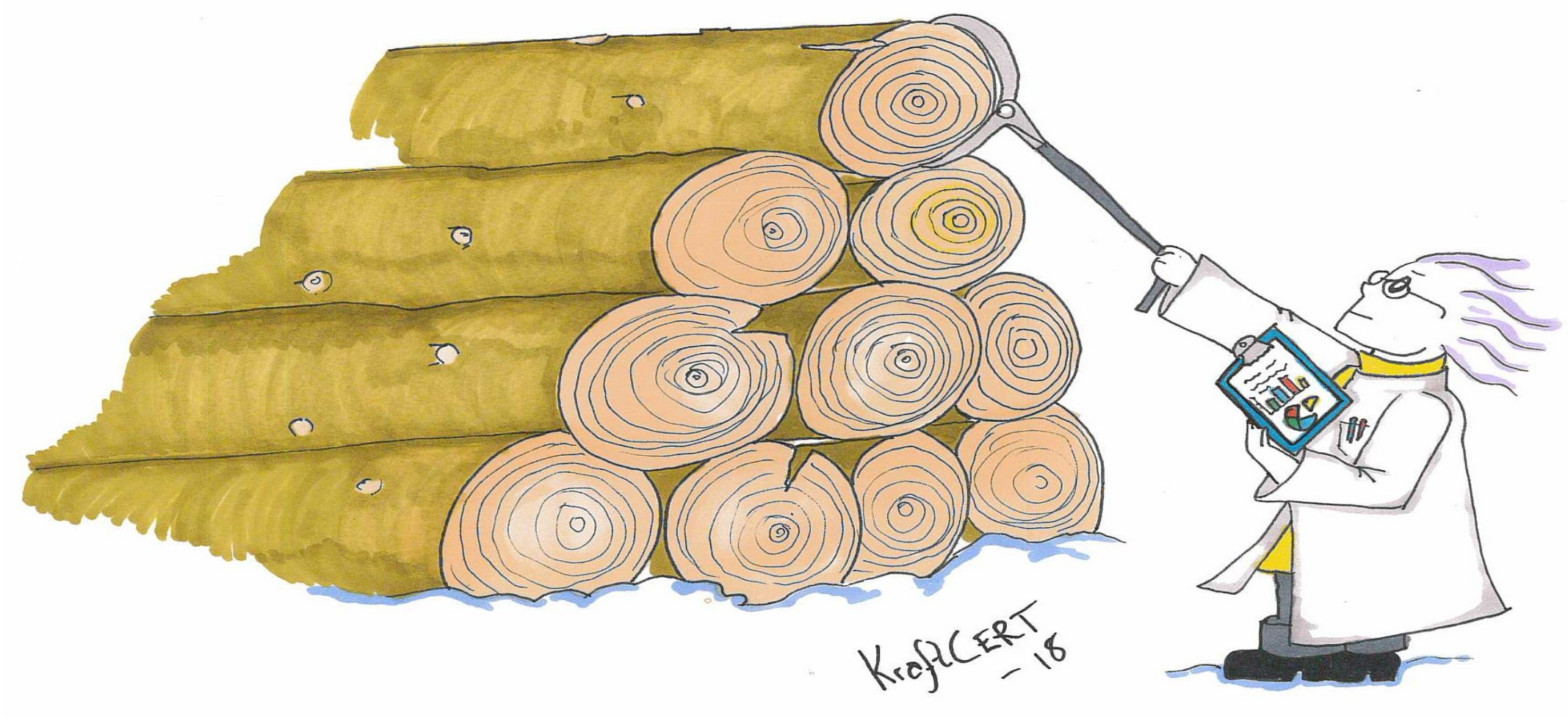
Statistikker, metrikker og rapporter for bedre felles sikkerhet



Kan vi måle sikkerhet?

- Logger er opphav til mye nyttig informasjon
  - Men du verden så mye annet også
- De som gir råd om analyse snakker ut fra et generelt perspektiv
- Logger fra blant annt IDSer, Brannmurer, Netflow, arbeidstasjoner kan gi svært spesifikk og viktige sikkerhetsmetrikker

Kraft CERT

Metrikker må være gjenkjennbart

- Antall portscannere per dag er et eksempel på hva man kan se. Det er mye av det, alle er utsatt for det, og det kan være mange forskjellige hensikter.
- Gode metrikker:
  - Utvetydige og meningsfulle for en forutbestemt hensikt, og lesbar for en sikkerhetsanalytiker
  - Å måle for å få en metrikk bør ikke koste mye, verken i midler eller trafikkforstyrrelse.
  - Målinger skal gjøres med samme metode, med tilstrekkelig intervall mellom målinger, og helst med automatiske metoder.

Kraft CERT

Hver metrikk har sitt publikum

- Antall portscannere per dag er fint for analytikerne, men er av mindre verdi for ledelsen
- Metrikker kan for eksempel tiltenkes
  - Teknikere
  - Operative sikkerhetsanalytikere
  - Strateger
  - Ledelse

Kraft CERT

Metrikker må ha en kontekst

- Antall portscannere per dag gir ingen mening om man ikke vet hva som er normalen. Man må kjenne ***baseline.***
- Kunnskap om omgivelsene:
  - For eksempel: Dersom det er mye falske positiver må man ta dette med i beregningen nå man danner seg et bilde av aktiviteten.
- Av og til gir også andres data en viktig kontekst
  - Trusselbildet blir tydeligere

Kraft CERT

Flere ledd i datainnsamling

- Det blir store mengder data, som stiller høye krav til MINST maskinvare og analytikere (potensielt også finansene)
- Selv om man benytter seg av “sampling” for å dra ut data vil det være formålstjenlig å ha tilgang til de opprinnelige data dersom resultatene fører til grundigere undersøkelser

Feil som oppstår

- IDSer er sensitive til falske positiver, spesielt om der er store mengder falske positiver
- IDSer (eller brannmurer) som blir utsatt for ondsinnet trafikk fra “the usual suspects” kan rapportere dette kontinuerlig, og dette kan forvirre de metrikker man faktisk er ute etter
- Tuning av disse verdiene, kontinuerlig oppfølging

Kraft CERT

Innsamling av data for informasjon

- Man kan korrelere data for å kunne gjenkjenne visse typer angrep
  - Man kan også lage nye egne metrikker for dette
  - Dette er metrikker som kan deles
  - Det er også metrikke som det tjenes penger på
- Blacklist-baserte metrikker er alltid nyttig, med eller uten korrelering
  - C&C, TOR, kjente skadevarekilder, kjente kompromitterte
- Man kan gå dypt å for eksempel logge feil protokoll, feil bruk av en protokoll (f.eks. ulovlige flagg i TCP eller forsøk på å svare på ikke-etablerte sesjoner)
- Man kan benytte slike data i forbindelse med geografisk sperring
- På enkeltmaskiner kan man loggen endringer i executables, men da må man vite hva man har. Det gjelder alt.

Kraft CERT

Innsamlig av data til informasjon II

- Generelt vil man kunne skape metrikker ved å observere status quo (ikke bandet), f.eks
  - Ulovlige enheter på nettverket
  - Ulovlige minnepinner
    - Alle disse kan også snevres inn, særlig for kontekst
  - Variasjon i trafikkvolum
    - Ha oversikt over ordinær datamengde
    - eksfiltrasjon av data
    - illegitim nedlasting av payload
  - Ulovlige innlogginger (kontekst: var det lovlige?)
  - Alerter på suspekt og/eller usannsynlig brukeraktivitet f.eks. innlogging fra flere steder, rare steder eller på rare tider (dette blir dog fort brennbart)
- Hvis man også logger mengde av vanlige data som f.eks. HTTP 4xx eller 200 OK vil dette f.eks kunne være indikasjon på DDoS

Kraft CERT

Trusselbildet

- I dag er det et gap mellom det myndigheter uttrykker om trusselbildet og det som understøttes ved statistiske data eller rapporter.
- Det nasjonale trusselbildet som foreligger for bransjen er ikke-transparent.
- Politiske motiver og vilje til å ta de rette beslutninger på departementsnivå bør være fundert i realistiske metrikker.

Trusselvurdering for bransjen ut fra statistikker og metrikker

- Man må kunne samle relevante data, f.eks. antall portscannere per dag totalt, og bevegelser i hvem som er utsatt for dette.
- Metoden må ha lav kostnad, gjøres på lik måte hver gang og helst være automatisk
- Metoden må ikke ha negative konsekvenser for selskapene, også mht sikkerhetspolicier og GDPR.

Kraft CERT

Trusselvurdering fra metrikker

- Hva er trusselbildet for en enkelt tjeneste hos et selskap?
- Hva er trusselbildet på tvers? Kanskje noen prøver forskjellige angrep på samme tjeneste hos forskjellige selskap.
- Krysskorrelering av data i enkeltselskap gir metrikker for egne trusler
- Krysskorrelering på tvers av selskapene gir metrikker både for enkeltselskap, tuning-data og verdifull informasjon for kritisk infrastruktur

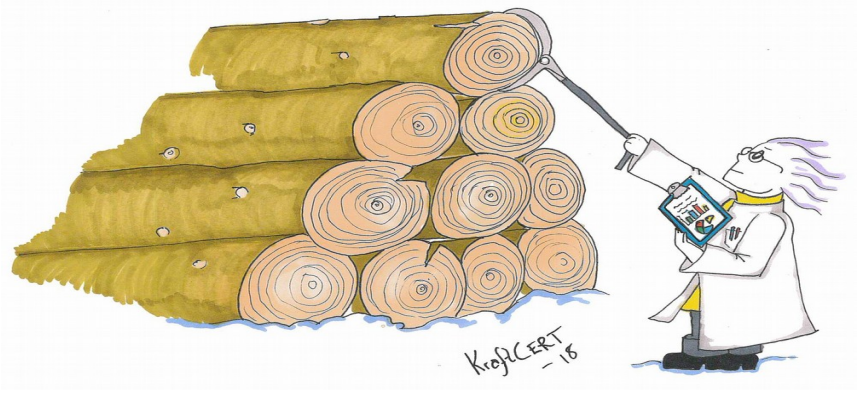
Kraft CERT

Hva kan man se når man ser flere

- Early warning for andre
- Angrep kamuflert som mundan støy
- Angrep kamuflert i andre angrep

Spørsmål? Ta kontakt på cert@kraftcert.no eller margrete.raaum@kraftcert.no

Statistikker, metrikker og rapporter for bedre felles sikkerhet



Kan vi måle sikkerhet?

- Logger er opphav til mye nyttig informasjon
  - Men du verden så mye annet også
- De som gir råd om analyse snakker ut fra et generelt perspektiv
- Logger fra blant annt IDSer, Brannmurer, Netflow, arbeidstasjoner kan gi svært spesifikk og viktige sikkerhetsmetrikker

Kraft CERT

Metrikker må være gjenkjennbart

- Antall portscannere per dag er et eksempel på hva man kan se. Det er mye av det, alle er utsatt for det, og det kan være mange forskjellige hensikter.
- Gode metrikker:
  - Utvetydige og meningsfulle for en forutbestemt hensikt, og lesbar for en sikkerhetsanalytiker
  - Å måle for å få en metrikk bør ikke koste mye, verken i midler eller trafikkforstyrrelse.
  - Målinger skal gjøres med samme metode, med tilstrekkelig intervall mellom målinger, og helst med automatiske metoder.

Hver metrikk har sitt publikum

- Antall portscannere per dag er fint for analytikerne, men er av mindre verdi for ledelsen
- Metrikker kan for eksempel tiltenkes
  - Teknikere
  - Operative sikkerhetsanalytikere
  - Strateger
  - Ledelse

Kraft CERT

Metrikker må ha en kontekst

- Antall portscannere per dag gir ingen mening om man ikke vet hva som er normalen. Man må kjenne ***baseline.***
- Kunnskap om omgivelsene:
  - For eksempel: Dersom det er mye falske positiver må man ta dette med i beregningen nå man danner seg et bilde av aktiviteten.
- Av og til gir også andres data en viktig kontekst
  - Trusselbildet blir tydeligere

Kraft CERT

Flere ledd i datainnsamling

- Det blir store mengder data, som stiller høye krav til MINST maskinvare og analytikere (potensielt også finansene)
- Selv om man benytter seg av “sampling” for å dra ut data vil det være formålstjenlig å ha tilgang til de opprinnelige data dersom resultatene fører til grundigere undersøkelser

Kraft CERT

Feil som oppstår

- IDSer er sensitive til falske positiver, spesielt om der er store mengder falske positiver
- IDSer (eller brannmurer) som blir utsatt for ondsinnet trafikk fra “the usual suspects” kan rapportere dette kontinuerlig, og dette kan forvirre de metrikker man faktisk er ute etter
- Tuning av disse verdiene, kontinuerlig oppfølging

Kraft CERT

Innsamling av data for informasjon

- Man kan korrelere data for å kunne gjenkjenne visse typer angrep
  - Man kan også lage nye egne metrikker for dette
  - Dette er metrikker som kan deles
  - Det er også metrikke som det tjenes penger på
- Blacklist-baserte metrikker er alltid nyttig, med eller uten korrelering
  - C&C, TOR, kjente skadevarekilder, kjente kompromitterte
- Man kan gå dypt å for eksempel logge feil protokoll, feil bruk av en protokoll (f.eks. ulovlige flagg i TCP eller forsøk på å svare på ikke-etablerte sesjoner)
- Man kan benytte slike data i forbindelse med geografisk sperring
- På enkeltmaskiner kan man loggen endringer i executables, men da må man vite hva man har. Det gjelder alt.

Kraft CERT

Innsamlig av data til informasjon II

- Generelt vil man kunne skape metrikker ved å observere status quo (ikke bandet), f.eks
  - Ulovlige enheter på nettverket
  - Ulovlige minnepinner
    - Alle disse kan også snevres inn, særlig for kontekst
  - Variasjon i trafikkvolum
    - Ha oversikt over ordinær datamengde
    - eksfiltrasjon av data
    - illegitim nedlasting av payload
  - Ulovlige innlogginger (kontekst: var det lovlige?)
  - Alerter på suspekt og/eller usannsynlig brukeraktivitet f.eks. innlogging fra flere steder, rare steder eller på rare tider (dette blir dog fort brennbart)
- Hvis man også logger mengde av vanlige data som f.eks. HTTP 4xx eller 200 OK vil dette f.eks kunne være indikasjon på DDoS

Kraft CERT

Trusselbildet

- I dag er det et gap mellom det myndigheter uttrykker om trusselbildet og det som understøttes ved statistiske data eller rapporter.
- Det nasjonale trusselbildet som foreligger for bransjen er ikke-transparent.
- Politiske motiver og vilje til å ta de rette beslutninger på departementsnivå bør være fundert i realistiske metrikker.

Kraft CERT

Trusselvurdering for bransjen ut fra statistikker og metrikker

- Man må kunne samle relevante data, f.eks. antall portscannere per dag totalt, og bevegelser i hvem som er utsatt for dette.
- Metoden må ha lav kostnad, gjøres på lik måte hver gang og helst være automatisk
- Metoden må ikke ha negative konsekvenser for selskapene, også mht sikkerhetspolicier og GDPR.

Trusselvurdering fra metrikker

- Hva er trusselbildet for en enkelt tjeneste hos et selskap?
- Hva er trusselbildet på tvers? Kanskje noen prøver forskjellige angrep på samme tjeneste hos forskjellige selskap.
- Krysskorrelering av data i enkeltselskap gir metrikker for egne trusler
- Krysskorrelering på tvers av selskapene gir metrikker både for enkeltselskap, tuning-data og verdifull informasjon for kritisk infrastruktur

Kraft CERT

Hva kan man se når man ser flere

- Early warning for andre
- Angrep kamuflert som mundan støy
- Angrep kamuflert i andre angrep

Spørsmål? Ta kontakt på cert@kraftcert.no eller margrete.raaum@kraftcert.no