Prosjektskisse – Gruppe 9

Hovedprosjekt i data/informasjonsteknologi ved Høgskolen i Oslo, våren 2014

Tittel: Analyse av IP/domenerep i sikkerhetsovervåkning
Sted/Dato: Høgskolen i Oslo og Akershus, Oslo 6.12.2013

Gruppemedlemmmer

- Kristoffer Berdal - s180212
- Sondre Braathen - s181137
- Anders Eckhoff - s181126
- Tommy Nyrud - s180487
- Even Sverdrup Augdal - s181091

Oppdragsgiver

- **Selskap:** mnemonic AS, avdeling MSS
- **Telefon:** +47 232 04 700
- **Adresse:** Wergelandsveien 25, 0167 Oslo
- **Kontaktperson:** Andreas Bråthen

Beskrivelse av oppdragsgiver

mnemonic AS er Nordens størst leverandør innen IT- og informasjonssikkerhet. En av tjenestene de leverer er sikkerhetsovervåkning, hvor de blant annet benytter ryktebasert analyse (IP- og domene) som en kilde for å oppdage sikkerhetshendelser og for å øke tillit til andre datakilder som eksempelvis Intrusion and Detection Systems (IDPS).

Ryktebaserte kilder har lenge vært i utstrakt bruk på mail-systemer for filtrering av kjente spam og phishing avsendere, men har først i de senere år blitt tatt mer i bruk for å oppdage mistenkelig nettverkskommunikasjon og annotere andre sikkerhetsalarmer. En utfordring ved ryktebaserte metoder er at det ofte krever manuell analyse og tolkning av datagrunnlaget. Dette er lite skalerbart når kundeporteføljen og ryktebaserte kilder øker, og mnemonic har derfor behov for å utvikle presentasjonslag som kan gi analytikere et nøyaktig og oversiktlig bilde ved en sikkerhetshendelse.

I dag har mnemonic flere egenproduserte verktøy for å samle inn, analysere og presentere data. Dette er arbeidskrevende, i mindre grad automatisert og skaper rom for feilvurderinger. mnemonic ønsker derfor å utvide deres kunde- og overvåkningsløsning, Argus, med et grensesnitt som presenterer datakilder sammenkoblet på en oversiktlig og verdiskapende måte.

Prosjektbeskrivelse

Oppgaven skal se nærmere på følgende:

- Vurdere datakilder med hovedfokus på ryktebasert analyse og identifisere behov til presentasjonslag basert på tilbakemeldinger fra 2.- og 3.linje analytikere
- Utarbeide forslag til organisering for hvordan kildene bør kobles sammen og presenteres
- Utarbeide mashup av de forslagene og behovene som identifiseres

Det stilles ingen krav til plattform, bruk av verktøy eller hvordan arbeidet presenteres, men det utarbeidede forslaget bør teoretisk sett kunne utvikles og integreres i mnemonics Argus.