|  |  |
| --- | --- |
| **Scenario** | **8 – Nettverkssegmenteringsfeil** |
| Øvingsform | Spilløvelse |
| Modenhetskrav | Middels |
| Forventet tidsbruk | Forberedelse: 40 timerGjennomføring: 2-6 timerEvaluering: 2 timer |
| Beskrivelse av scenario | * I brannmuren mellom IT og OT-nettverkene hos en kraftprodusent er det en feilkonfigurasjon som tillater uhindret trafikk for enkelte protokoller, inkludert RPC og SMB.
* En angriper har fått fotfeste i IT-nettet og beveger seg lateral over til OT ved hjelp av PsExec og får et cmd.exe-shell på en SCADA-server.
* Dette oppdages når angriperen kjører flere rekognoseringskommandoer fra SCADA-serveren, og dette trigger en antivirus-alert som sendes på e-post til IT Helpdesk. Helpdesk varsler varsler driftskontroll 3 timer etter ticket ble laget. ​
 |
| Egnede øvingsmål | * Øve på beslutninger under usikkerhet
* Utvikle samhandling mellom IT og OT
* Øve på bruk av planverk
* Etablere felles situasjonsforståelse
 |
| Egnede roller for øvende | * Innsatsleder
* Loggfører
* Kommunikasjonsansvarlig
* Teknisk personell (IT og OT)
 |
| Roller i spillstab | * Scenarioleder
* IT og IT-sikkerhet
* Automasjonsavdeling
* OT-leverandør
 |
| Øvingsmomenter | 1. Alert om mistenkelig aktivitet
2. Avblåses først som støy
3. Tydelige indikatorer på kompromitterte systemer
4. Årsak viser seg å være feilkonfigurasjon
 |