Taryk Abu-Hassan

„Wykrywanie incydentów oraz działania poincydentalne”

1. Jakie kompetencje powinien mieć incydent handler, jakie działania powinien wykonywać?
2. Jak przygotować się na incydent, by móc wykryć go po kilku godzin po wystąpieniu, jak zastawić pułapki i HoneyPots?
3. Jakie czynności powinny zostać wykonane w celu analizy artefaktów pozostawionych przez atakującego?
4. Jakie czynności powinny zostać wykonane, aby zabezpieczyć organizacje na przyszłość?
5. Analiza powierzchni ataku, czyli w jaki sposób dokonywać analizy po włamaniowej oraz aktualizować katalog ryzyk?