Krystian Hofman
Business Development Manager,
Oberig IT

„Nowoczesne rozwiązania w zakresie bezpieczeństwa infrastruktury krytycznej”

- **Wykładniczy wzrost zagrożeń cybernetycznych**
  - Liczba ataków rośnie, a aktorzy zagrożeń (APT, grupy przestępcze) stosują coraz bardziej zaawansowane TTP.
  - Bez systematycznego monitorowania zagrożeń organizacje reagują zbyt późno.
- **Wycieki danych i ich sprzedaż**
  - W darknecie i otwartych źródłach regularnie pojawiają się bazy z danymi uwierzytelniającymi, konfiguracjami technicznymi, adresami IP – co bezpośrednio zagraża klientom.
  - Rozwiązanie Luminar (Cognyte) pozwalają automatycznie wykrywać i reagować na takie wycieki.
- **Rosnąca powierzchnia ataku**
  - Usługi chmurowe, praca zdalna, IoT – wszystko to tworzy nowe wektory ataków.
  - CTI pomaga śledzić aktualne zagrożenia dotyczące konkretnej infrastruktury.
- **Wymogi regulacyjne i ryzyko reputacyjne**
  - W wielu sektorach (finanse, energetyka, administracja publiczna) obowiązują normy bezpieczeństwa i obowiązki raportowe.
  - Opóźnione wykrycie incydentu = bezpośrednie kary + utrata zaufania.
- **Konieczność proaktywności**
  - Klasyczne SOC i SIEM głównie reagują na już znane incydenty.
  - Luminar (Cognyte) jako CTI/DRP pozwala działać z wyprzedzeniem, monitorując przygotowania do ataków i sygnalizując ryzyka zanim dojdzie do ich realizacji.
- **Konieczność ciągłości**
  - Organizacje wiedzą, ile inwestują w cyberbezpieczeństwo, ale nie wiedzą, na ile te inwestycje faktycznie działają. Cymulate daje ciągłą walidację, a nie tylko jednorazowy audyt.
  - Tradycyjne testy penetracyjne są punktowe i statyczne, podczas gdy Cymulate oferuje ciągłą i dynamiczną walidację.
  - Jak organizacjom mierzyć realny poziom odporności na techniki MITRE ATT&CK?
- **Widoczność, kontekst i automatyzacja w jednym miejscu**
  - Dane logów same w sobie nie zwiększają bezpieczeństwa – kluczowa jest analiza i kontekst.
  - Logpoint pozwala łączyć dane z różnych źródeł i automatyzować reakcje, co skraca czas obsługi incydentów.
- **Bezpieczeństwo aplikacji zaczyna się od polityk sieciowych**
  - Infrastruktura IT jest coraz bardziej złożona, a manualne zarządzanie regułami to ryzyko i strata czasu.

- AlgoSec zapewnia widoczność i kontrolę nad zależnościami między aplikacjami a politykami bezpieczeństwa.
- AlgoSec skraca czas audytów zgodności (PCI-DSS, GDPR, NIS2, DORA) z tygodni do godzin.