IBM sprendimai kibernetinių incidentų valdymui

Evaldas Valūnas
Grupės vadovas, Saugumo sprendimų kompetencijos centras, Atea

Kibernetinio saugumo rizikos valdymo priemonės

Rizikos analizės ir informacinių sistemų saugumo politika:

- Randori Recon (ASM)
- IBM Guardium Vulnerability assessment
- IBM Guardium Data Discover and Classification
- IBM QRadar UBA

Pagrindinis duomenų saugumo iššūkis - nustatyti, kas turi prieigą ir ką gali daryti. Įmonėms reikia realiuoju laiku stebėti vietinių ir debesijos duomenų šaltinių veiklą, kad svarbūs duomenys išliktų apsaugoti.

ATEA IBM Platinum Partner

Kibernetinio saugumo rizikos valdymo priemonės

Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas:

- IBM IAM
- IBM Verify
- IBM Trusteer
- IBM QRadar XDR
- IBM Cognos

Vidaus auditas nuolat stebi vidaus verslo praktikų nuoseklumą, jo tikslas yra užtikrinti organizacijos politikų ir procedūrų laikymąsi ir įspėti vadovybę apie politikų laikymosi spragas.

ATEA IBM Platinum Partner

Kibernetinio saugumo rizikos valdymo priemonės

Kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimai:

- IBM Verify
- IBM Trusteer

Sprendimai padeda aptikti sukčiavimą, autentifikuoti naudotojus ir nustatyti tapatybės patikimumą visame daugiakanaliame naudotojų judėjime.

ATEA IBM Platinum Partner

Kibernetinio saugumo rizikos valdymo priemonės

Pagrindinė kibernetinės higienos praktika ir kibernetinio saugumo mokymai:

- IBM PL – Cyber Range
- X-Force - Cyber Range*

"Cyber Range" sprendimas sukuria simuliacijas, kurios padeda organizacijoms atlikti realius pažeidimo scenarijus, padedančius užtikrinti, kad galite reaguoti ir atsigauti po kibernetinių incidentų organizacijos mastu.

ATEA IBM Platinum Partner

* „Enterprise“ dydžio klientams

Kibernetinio saugumo rizikos valdymo priemonės

Kriptografija ir šifravimo naudojimo politikos ir procedūros:

- IBM Security Guardium
  Data Encryption (GDE)
- IBM Cloud - Hyper Protect Crypto Services
  Unified Key Orchestrator (multicloud)

Kriptografija yra viena iš svarbiausių priemonių, kurią įmonės naudoja siekdamos apsaugoti sistemas, kuriose saugomas svarbiausias turtas – duomenys, nesvarbu ar jie yra saugomi ar judantys.

ATEA IBM Platinum Partner

Kibernetinio saugumo rizikos valdymo priemonės

Politikos ir procedūros, kibernetinio saugumo rizikos valdymo veiksmingumui įvertinti:

- IBM QRadar SOAR
- IBM Open Pages
- IBM Guardium Data Protection
- IBM PL – Cyber Range

Vidaus auditas nuolat stebi vidaus verslo praktikų nuoseklumą, jo tikslas yra užtikrinti organizacijos politikų ir procedūrų laikymąsi ir įspėti vadovybę apie politikų laikymosi spragas.

ATEA IBM Platinum Partner

Kibernetinio saugumo rizikos valdymo priemonės

Tinklų ir informacinių sistemų įsigijimas:

- IBM CloudPak for Security
  - Qradar QNI, Forensic
  - IBM QRadar SOAR
  - OT/IoT security
  - IBM QRadar XDR
- MaaS360
- IBM Verify (IAM)
- Randori (ASM)
- ReaQta
- IBM X-Force Red*
- IBM Research - IBM Beyond Presence

* „Enterprise“ dydžio klientams

Platinum Partner

Kibernetinio saugumo rizikos valdymo priemonės

Tiekimo grandinės saugumas:

- IBM X-Force
- IBM Security Supply Chain Cyber Risk Management Services
- IBM Cloud Security - Dev/Sec/Ops
- RedHat (ACS)

Užtikrina didesnį visų tiekimo grandinės veiksmų matomumą.
Suteikia beveik realiuoju laiku operacijų matomumą ir galimybę imtis veiksmų anksčiau.

ATEA IBM Platinum Partner

Kibernetinio saugumo rizikos valdymo priemonės

Veiklos tęstinumas, krizių valdymas:

- IBM QRadar SOAR
  - CSIRT integracija
  - (automatizacija, incidentų raportavimo sistema)
  - SOC >> CSIRT
- IBM Storage (safe guarded copies)
- IBM Cloud - backup
- IBM PL – Cyber Range mSOC

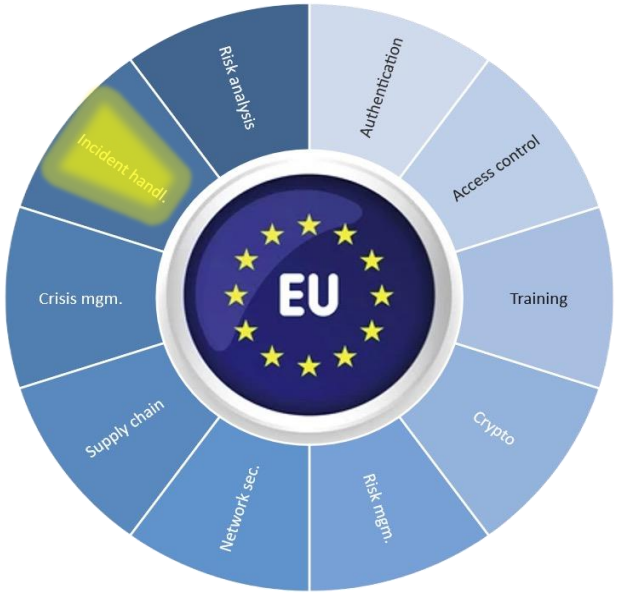
Reaguoti į kibernetinius incidentus yra visos įmonės pareiga.
Paprastai valdydama įvykius ir užduotis, jūsų komanda gali sklandžiai vadovauti tyrimo ir reagavimo veiksmams.

ATEA IBM Platinum Partner

Kibernetinio saugumo rizikos valdymo priemonės

Incidentų valdymas:

- IBM Security QRadar SIEM
- IBM Security QRadar SOAR



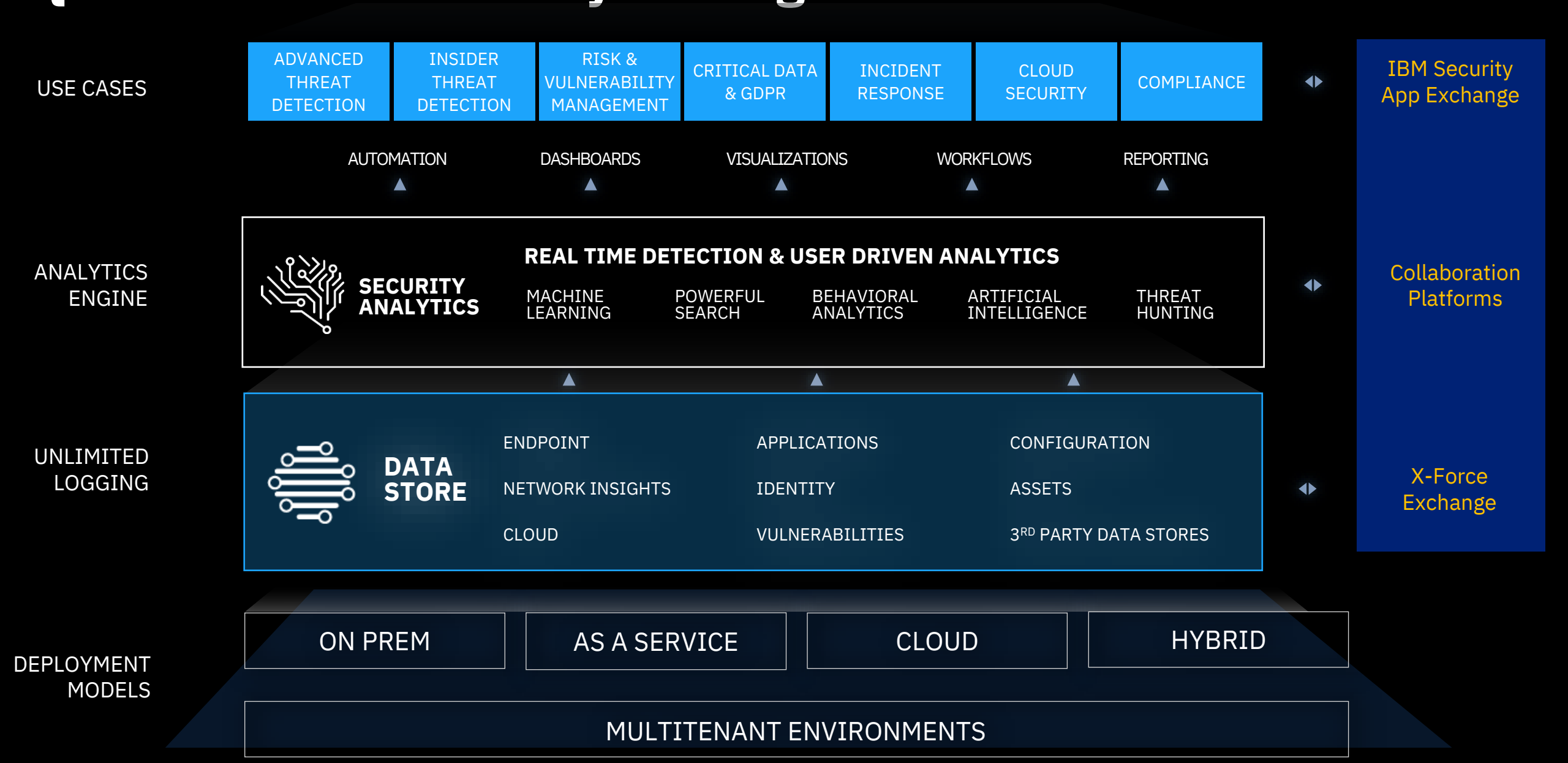
Svarbu ne problema, o tai, kaip ją sprendžiate.

ATEA IBM Platinum Partner

IBM QRadar SIEM

ATEA

QRadar SIEM - Security Intelligence Platform



Extensible functional architecture

Cognitive analytics

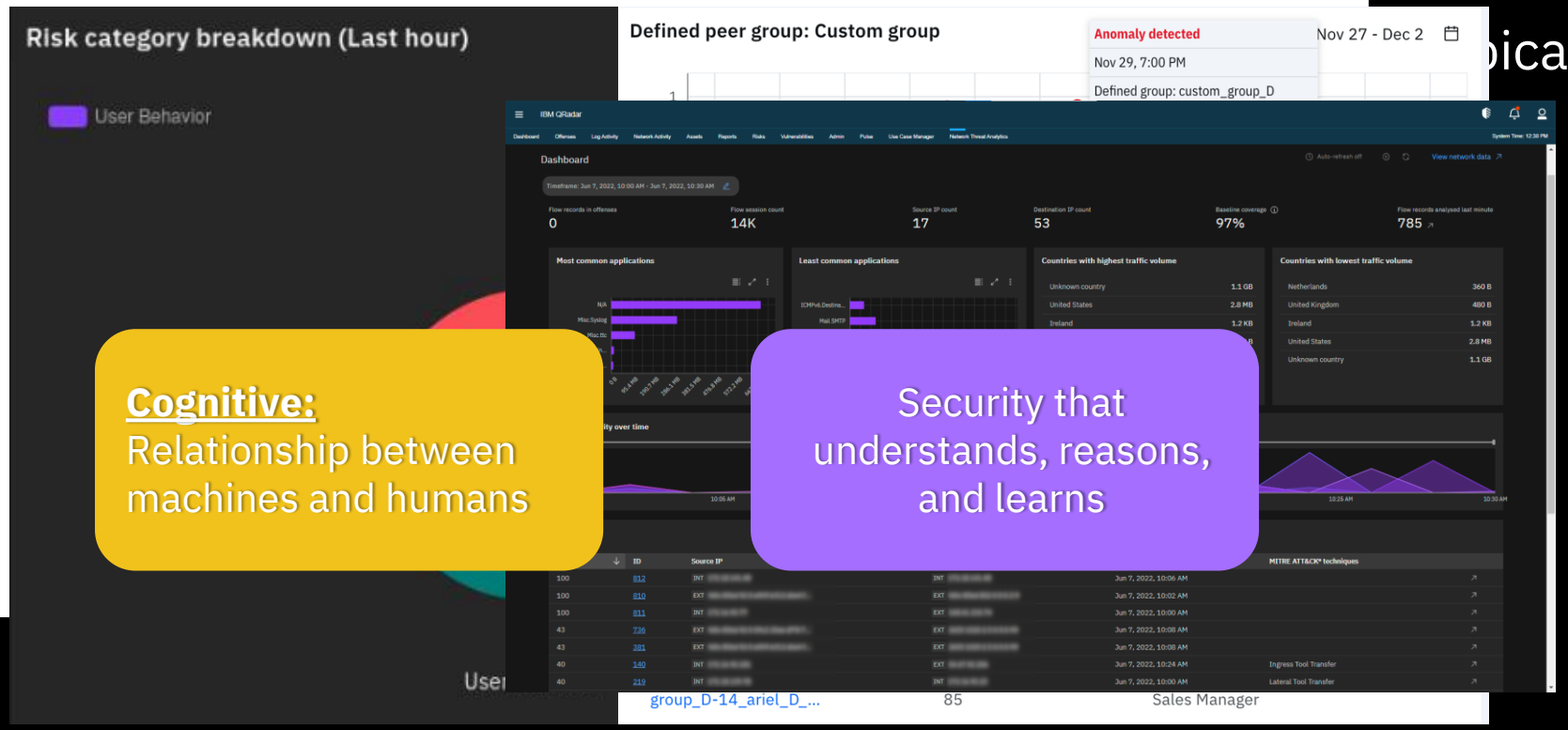
– **QRadar Us**

– **Machine Le**
based on ob

– **Network Th**
observed re

es offenses

ically



Digital everything:
Technology must handle and respond to data

Cognitive:
Relationship between machines and humans

Security that understands, reasons, and learns

Extensible functional architecture

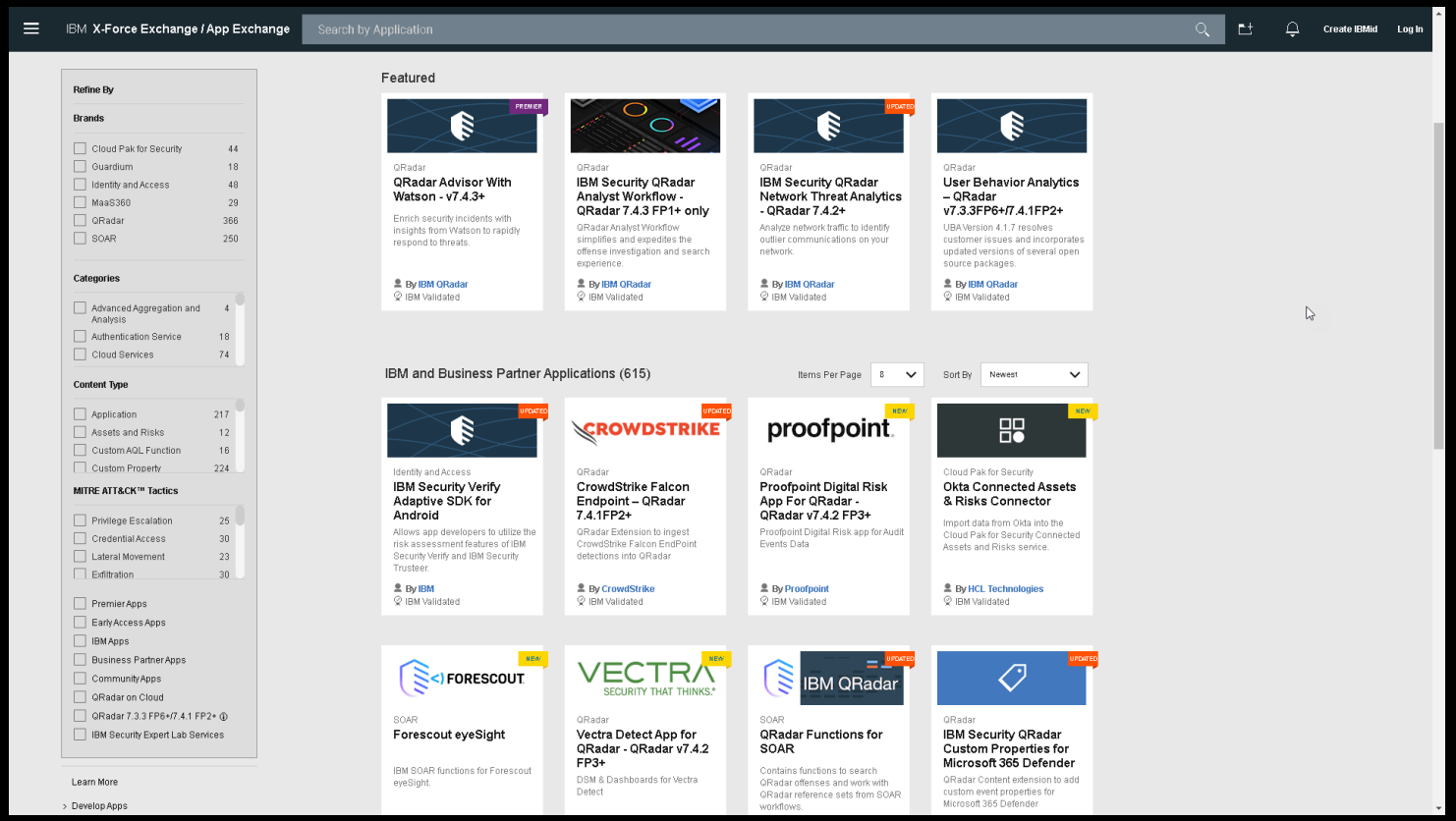
Open ecosystem

– **IBM Security App Exchange** provides access to apps from leading security partners

– Out-of-the-box integrations for 500+ third-party security products

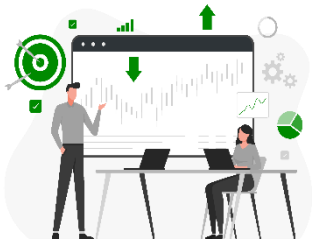
– Open APIs allow for custom integrations and apps

Apps are categorized by the type of service:
– Cloud
– Compliance
– Endpoints
– Data
– Identity
– Malware
– Mobile
– Threat detection
– System management



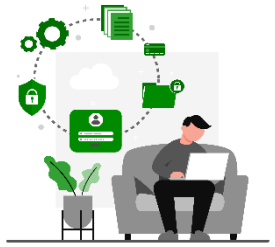
SOC kaip paslauga

SOC paslauga 24x7



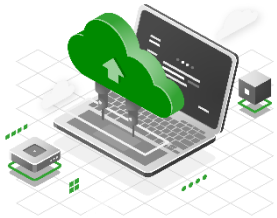
Projekto vald.

- Pradinis susitikimas
- Lūkesčiai
- Paslaugos informacija
- Patikslinimai
- Projekto planas
- Projekto susitikimai



Duomenys

Surenka saugumo žurnalus ir naudotojų elgseną iš vietinių, hibridinių ir debesijos sprendimų



SIEM

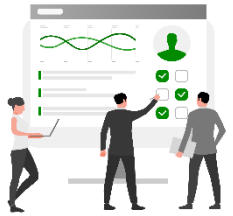
Visų neįprastų įvykių ir veiksmų stebėsena ir aptikimas realiuoju laiku

SOC

Analitikai stebi pavojaus signalus, vertina grėsmes ir imasi neatidėliotinų veiksmų 24/7/365

HyperCare

2 savaitės aktyvios priežiūros po paslaugos paleidimo



CSA

Periodiniai susitikimai su klientais, ataskaitų teikimas, patobulinimai ir atnaujinimai

Projekto valdymas

Turite klausimų apie TIS2 direktyvos taikymą Jūsų organizacijai ?

Susisiekime:

evaldas.valunas@atea.lt

+370 682 55171


Kuriame Lietuvą su IT
ATEA