

# 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.

# 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.

# Kibernetinio saugumo rizikos valdymo priemonės

Kelių veiksmų 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.

# 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.

# 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.

# 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.

# 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





# 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 didesnę visų tiekimo grandinės veiksmų matomumą.

Suteikia beveik realiuoju laiku operacijų matomumą ir galimybę imtis veiksmų anksčiau.

# 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 veiksams.



# Kibernetinio saugumo rizikos valdymo priemonės

Incidentų valdymas:

- IBM Security QRadar SIEM
- IBM Security QRadar SOAR



Svarbu ne problema, o tai, kaip ją sprendžiate.

An aerial, high-angle photograph of a modern office lounge. The space features several grey modular sofas with blue cushions and small white round tables. Three groups of business professionals are visible: one group of three people (two men and one woman) is gathered around a table, looking at a tablet and a large document; another group of three people (one woman and two men) is standing and talking; and a third group of three people (two men and one woman) is standing together, with one man holding a tablet. The floor is a light grey tile. The overall atmosphere is professional and collaborative.

# IBM QRadar SIEM

ATEA

# QRadar SIEM - Security Intelligence Platform

USE CASES

ADVANCED THREAT DETECTION	INSIDER THREAT DETECTION	RISK & VULNERABILITY MANAGEMENT	CRITICAL DATA & GDPR	INCIDENT RESPONSE	CLOUD SECURITY	COMPLIANCE
---------------------------	--------------------------	---------------------------------	----------------------	-------------------	----------------	------------

AUTOMATION      DASHBOARDS      VISUALIZATIONS      WORKFLOWS      REPORTING

ANALYTICS ENGINE



**SECURITY ANALYTICS**

**REAL TIME DETECTION & USER DRIVEN ANALYTICS**

MACHINE LEARNING	POWERFUL SEARCH	BEHAVIORAL ANALYTICS	ARTIFICIAL INTELLIGENCE	THREAT HUNTING
------------------	-----------------	----------------------	-------------------------	----------------

UNLIMITED LOGGING



**DATA STORE**

ENDPOINT	APPLICATIONS	CONFIGURATION
NETWORK INSIGHTS	IDENTITY	ASSETS
CLOUD	VULNERABILITIES	3 <sup>RD</sup> PARTY DATA STORES

DEPLOYMENT MODELS

ON PREM	AS A SERVICE	CLOUD	HYBRID
---------	--------------	-------	--------

MULTITENANT ENVIRONMENTS

IBM Security App Exchange

Collaboration Platforms

X-Force Exchange

# Extensible functional architecture

## Cognitive analytics



– QRadar Us

– Machine Le  
based on o

– Network T  
observed re

es offenses

ically

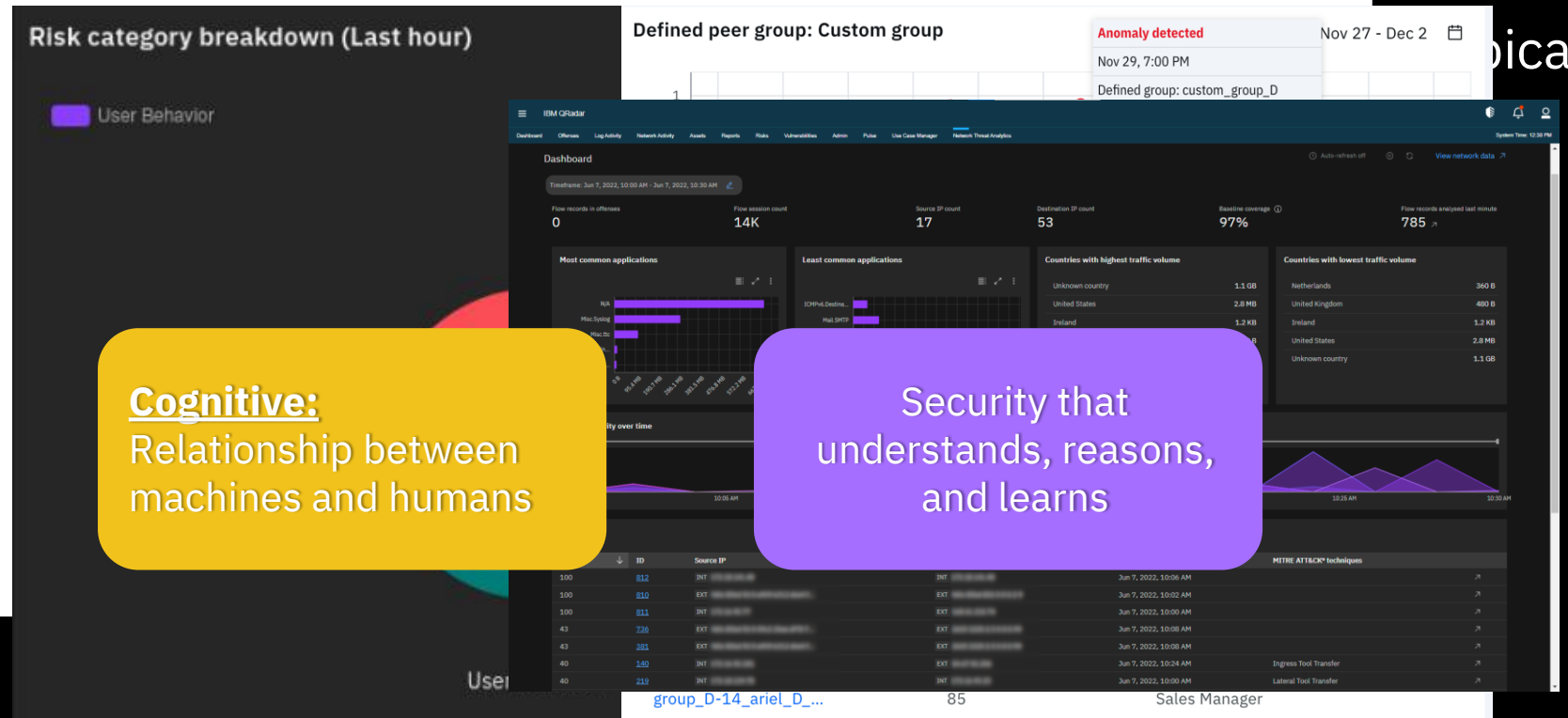
### Digital everything:

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

The screenshot displays the IBM X-Force Exchange / App Exchange interface. The top navigation bar includes the title "IBM X-Force Exchange / App Exchange", a search bar, and user options like "Create IBMid" and "Log In".

**Refine By**

- Brands:**
  - Cloud Pak for Security: 44
  - Guardium: 18
  - Identity and Access: 48
  - Maas360: 29
  - QRadar: 366
  - SOAR: 250
- Categories:**
  - Advanced Aggregation and Analysis: 4
  - Authentication Service: 18
  - Cloud Services: 74
- Content Type:**
  - Application: 217
  - Assets and Risks: 12
  - Custom AQL Function: 16
  - Custom Property: 224
- MITRE ATT&CK™ Tactics:**
  - Privilege Escalation: 25
  - Credential Access: 30
  - Lateral Movement: 23
  - Exfiltration: 30
- Other filters:**
  - Premier Apps
  - Early Access Apps
  - IBM Apps
  - Business Partner Apps
  - Community Apps
  - QRadar on Cloud
  - QRadar 7.3.3 FP6+ / 7.4.1 FP2+ (4)
  - IBM Security Expert Lab Services

**Featured**

- QRadar QRadar Advisor With Watson - v7.4.3+** (Updated): Enrich security incidents with insights from Watson to rapidly respond to threats. By IBM QRadar, IBM Validated.
- QRadar IBM Security QRadar Analyst Workflow - QRadar 7.4.3 FP1+ only** (Updated): QRadar Analyst Workflow simplifies and expedites the offense investigation and search experience. By IBM QRadar, IBM Validated.
- QRadar IBM Security QRadar Network Threat Analytics - QRadar 7.4.2+** (Updated): Analyze network traffic to identify outlier communications on your network. By IBM QRadar, IBM Validated.
- QRadar User Behavior Analytics - QRadar v7.3.3FP6+/7.4.1FP2+** (Updated): UBA Version 4.1.7 resolves customer issues and incorporates updated versions of several open source packages. By IBM QRadar, IBM Validated.

**IBM and Business Partner Applications (615)**

Items Per Page: 8 | Sort By: Newest

- Identity and Access IBM Security Verify Adaptive SDK for Android** (Updated): Allows app developers to utilize the risk assessment features of IBM Security Verify and IBM Security Trusteer. By IBM, IBM Validated.
- CrowdStrike Falcon Endpoint - QRadar 7.4.1FP2+** (Updated): QRadar Extension to ingest CrowdStrike Falcon on Endpoint detections into QRadar. By CrowdStrike, IBM Validated.
- proofpoint Proofpoint Digital Risk App For QRadar - QRadar v7.4.2 FP3+** (New): Proofpoint Digital Risk app for Audit Events Data. By Proofpoint, IBM Validated.
- Cloud Pak for Security Okta Connected Assets & Risks Connector** (New): Import data from Okta into the Cloud Pak for Security Connected Assets and Risks service. By HCL Technologies, IBM Validated.
- SOAR Forescout eyeSight** (New): IBM SOAR functions for Forescout eyeSight. By Forescout, IBM Validated.
- QRadar Vectra Detect App for QRadar - QRadar v7.4.2 FP3+** (New): DSI & Dashboards for Vectra Detect. By Vectra, IBM Validated.
- SOAR QRadar Functions for SOAR** (Updated): Contains functions to search QRadar offenses and work with QRadar reference sets from SOAR workflows. By IBM, IBM Validated.
- QRadar IBM Security QRadar Custom Properties for Microsoft 365 Defender** (Updated): QRadar Content extension to add custom event properties for Microsoft 365 Defender. By IBM, IBM Validated.

Learn More > Develop Apps

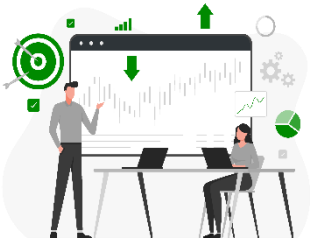
An aerial, high-angle view of a modern office lounge. The space features a large, modular grey sofa with several bright blue ottomans. Small, round white tables are scattered around the seating area. In the foreground, three people (two men and one woman) are gathered around a table, looking at a tablet and a large sheet of paper. In the background, another group of three people (two men and one woman) are standing and talking. The floor is a light grey tile. The overall atmosphere is professional and collaborative.

# SOC kaip paslauga

ATEA



# 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 stebėseną ir aptikimą realiuoju laiku



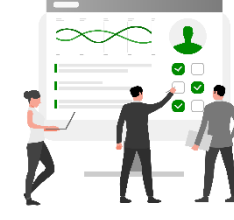
## SOC

Analitikai stebi pavojaus signalus, vertina grėsmes ir imasi neatidėliotųjų 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 ?

---

## Susisiekiame:

[evaldas.valunas@atea.lt](mailto:evaldas.valunas@atea.lt)

+370 682 55171



ATEA



# Kuriame Lietuvą su IT

ATEA