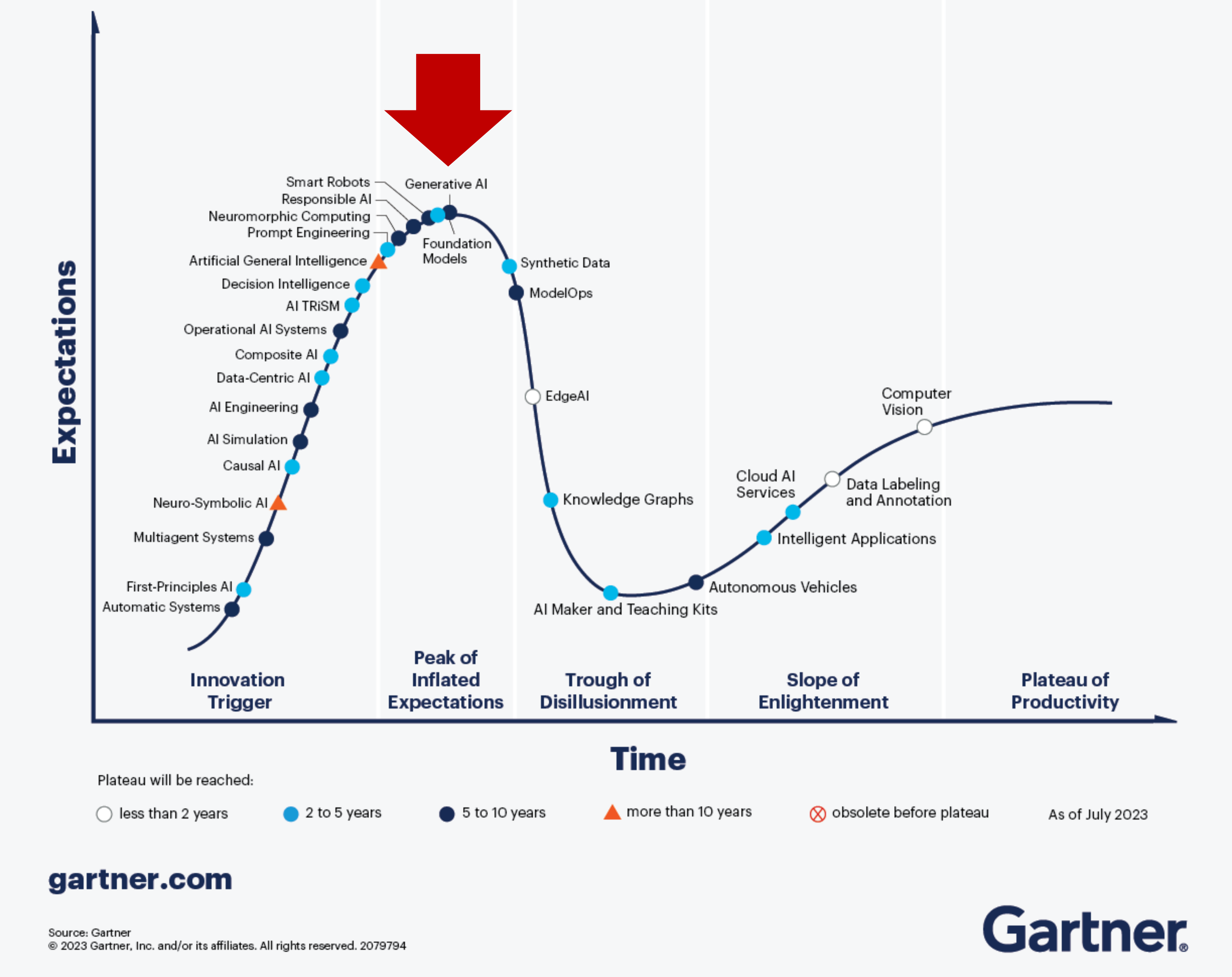
opentext™

AI zkušenosti v Security Analytics

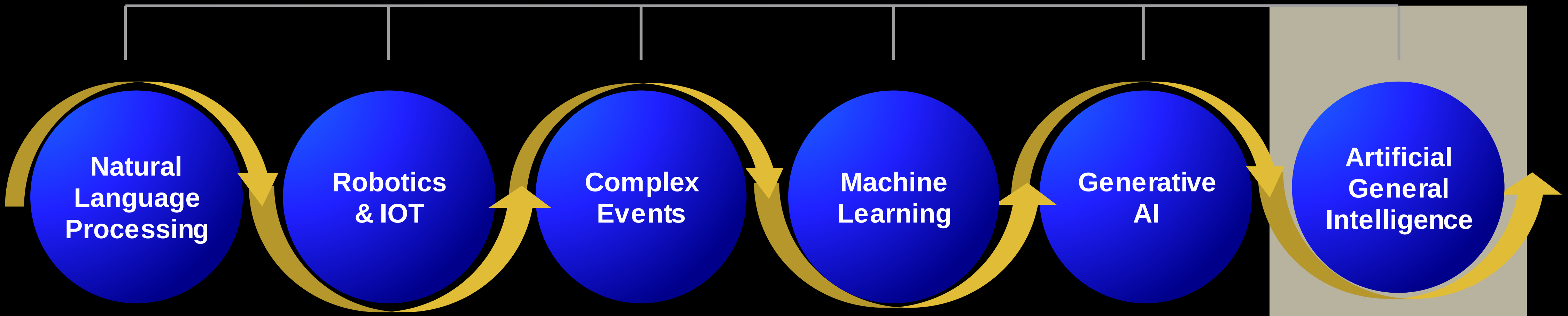
Petr Hněvkovský, CISM, CISA, CISSP, CEH
Sr. Manager | Cybersecurity Solutions Consulting
Duben 2024

Úspěch generativní AI zajistil maximální humbuk!



Source: Gartner
© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. 2079794

Dvě desetiletí inovací AI s více než 371 patenty AI



Natural Language Processing

- Programmed Translation
- Information Extraction

Robotics & IOT

- Process automation
- Optimization
- Expert systems

Complex Events

- Text to Speech
- Speech to Text
- Machine vision
- Image Recognition

Machine Learning

- Predictive Models
- Deep Learning
- Reinforced Learnings

Generative AI

- Prompt-engineering
- Large Language Models
- Vector DB
- API Orchestration

Artificial General Intelligence

- Automating decisions
- Machine made choices
- AI Trust, Risk & Security Management

© 2023 Open Text

Významné AI inovace kybernetické bezpečnosti

2010

BrightCloud první cloudová platforma Threat Inteligence

2014

Interset User and Entity Behavioural Analytics

2019

Fortify Audit Assistant k třídění výsledků testování

2020

ArcSight Recon introduces outlier analytics

2023

Voltage Financial Risk calculator

© 2023 Open Text

Použijte správnou AI pro správný scénář!

AppSec testovací problémy

- Omezení šumu
- Časově náročný proces
- Nedostatek auditorů AppSec
- Opakující se všední kontrola

© 2023 Open Text

Použijte správnou AI pro správný scénář!

AppSec testovací problémy

- Omezení šumu
- Časově náročný proces
- Nedostatek auditorů AppSec
- Opakující se všední kontrola

	Random Forest	ChatGPT
Classification performance	Equal or better	Equal or worst
Parameters	8 million[1]	1.76 trillion[3] (~950,000 larger)
Memory	50 MB[1]	45 GB[2] (~1300 times larger)
Training cost	< $30.67	> $100,000,000 [4]
Training CPUs/GPUs	1-3	~10,000[5]
Prediction speed	milliseconds	seconds

Fortify Audit Assistant první a přelomový od 2019

[1] Based on 10 forests, average of 114 trees, with an average maxDepth of 23. Computed using our default tunings, one forest per language

[2] Estimate from https://updf.com/knowledge/what-is-gpt-4/

[3] https://en.wikipedia.org/wiki/GPT-4 and Sam Altman

[4] Based on >700K FoD data, assuming 3xc5.large AWS instances on running for 12 hours, for 10 languages

[5] https://www.fierceelectronics.com/sensors/chatgpt-runs-10k-nvidia-training-gpus-potential-thousands-more

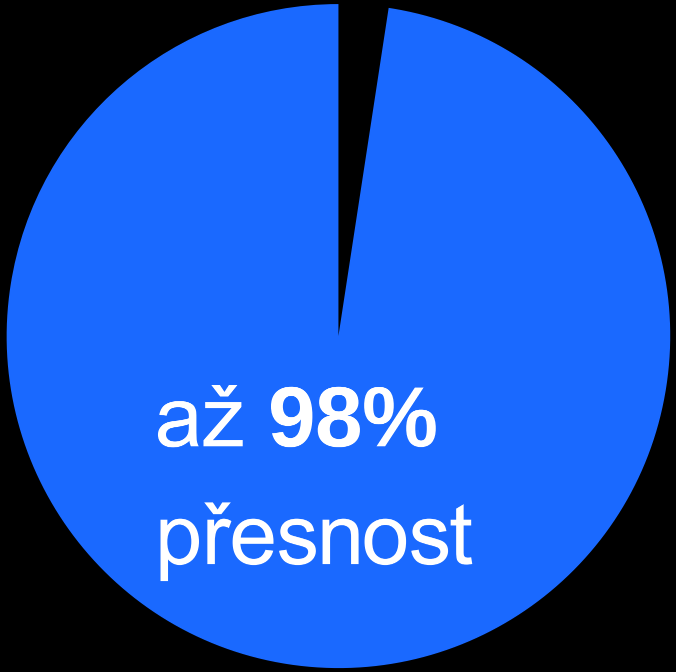
opentext™

© 2023 Open Text

Použijte správnou AI pro správný scénář!

AppSec testovací problémy

- Omezení šumu
- Časově náročný proces
- Nedostatek auditorů AppSec
- Opakující se všední kontrola



Okamžité výsledky

- Prioritizace pro výsledky s velkým dopadem
- Snížení manuálního úsilí
- Granulární označování
- Lidský asistent s AI

Fortify Audit Assistant první a přelomový od 2019

© 2023 Open Text

Poučení se z AI pro vytvoření vhodnějších řešení

Klíčové výzvy SOC 2020

- Nedostatek talentů
- Dlouhá doba expozice
- Rozvoj hrozeb
- Informační přetížení
- Manuální opakující se úkoly

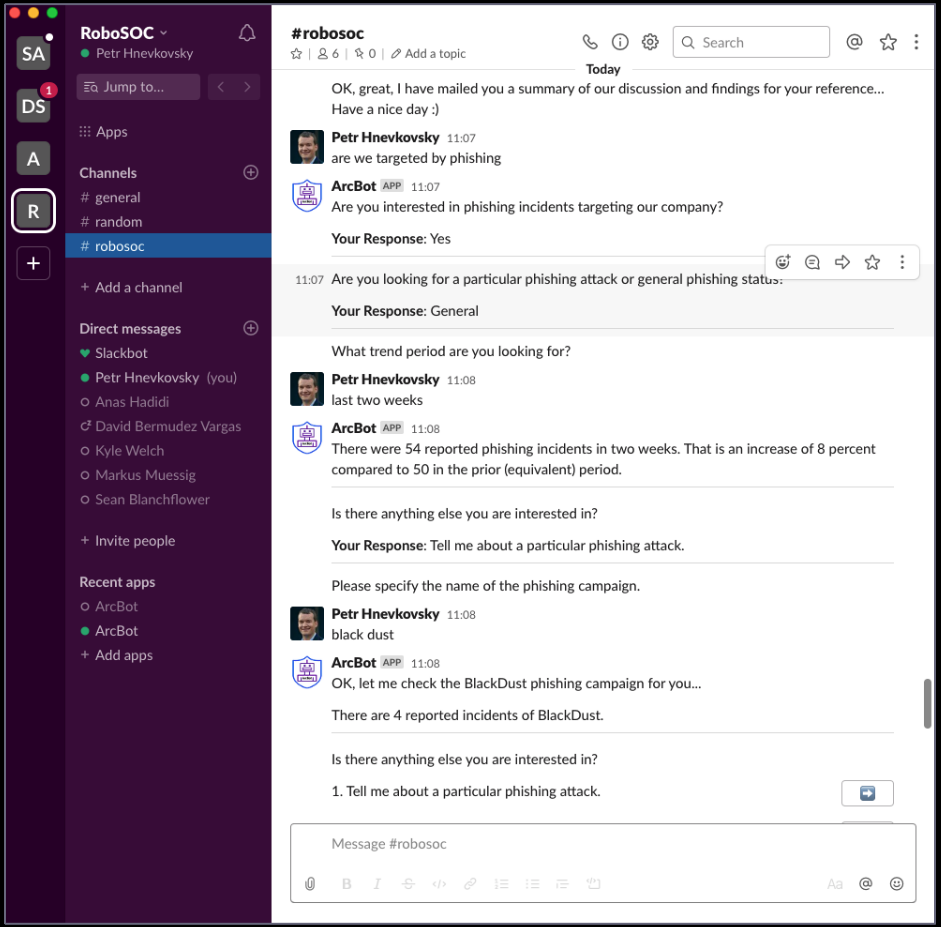
Robotic Driven SOC 1/4

AI and RPA Improving SecOps

RoboSOC Security Guide

© 2023 Open Text

Získejte okamžitý přehled bez technické znalosti



OK, great, I have mailed you a summary of our discussion and findings for your reference... Have a nice day :)

Petr Hnevkovsky 11:07
are we targeted by phishing

ArcBot APP 11:07
Are you interested in phishing incidents targeting our company?

Your Response: Yes

11:07 Are you looking for a particular phishing attack or general phishing status?

Your Response: General

What trend period are you looking for?

Petr Hnevkovsky 11:08
last two weeks

ArcBot APP 11:08
There were 54 reported phishing incidents in two weeks. That is an increase of 8 percent compared to 50 in the prior (equivalent) period.

Is there anything else you are interested in?

Your Response: Tell me about a particular phishing attack.

Please specify the name of the phishing campaign.

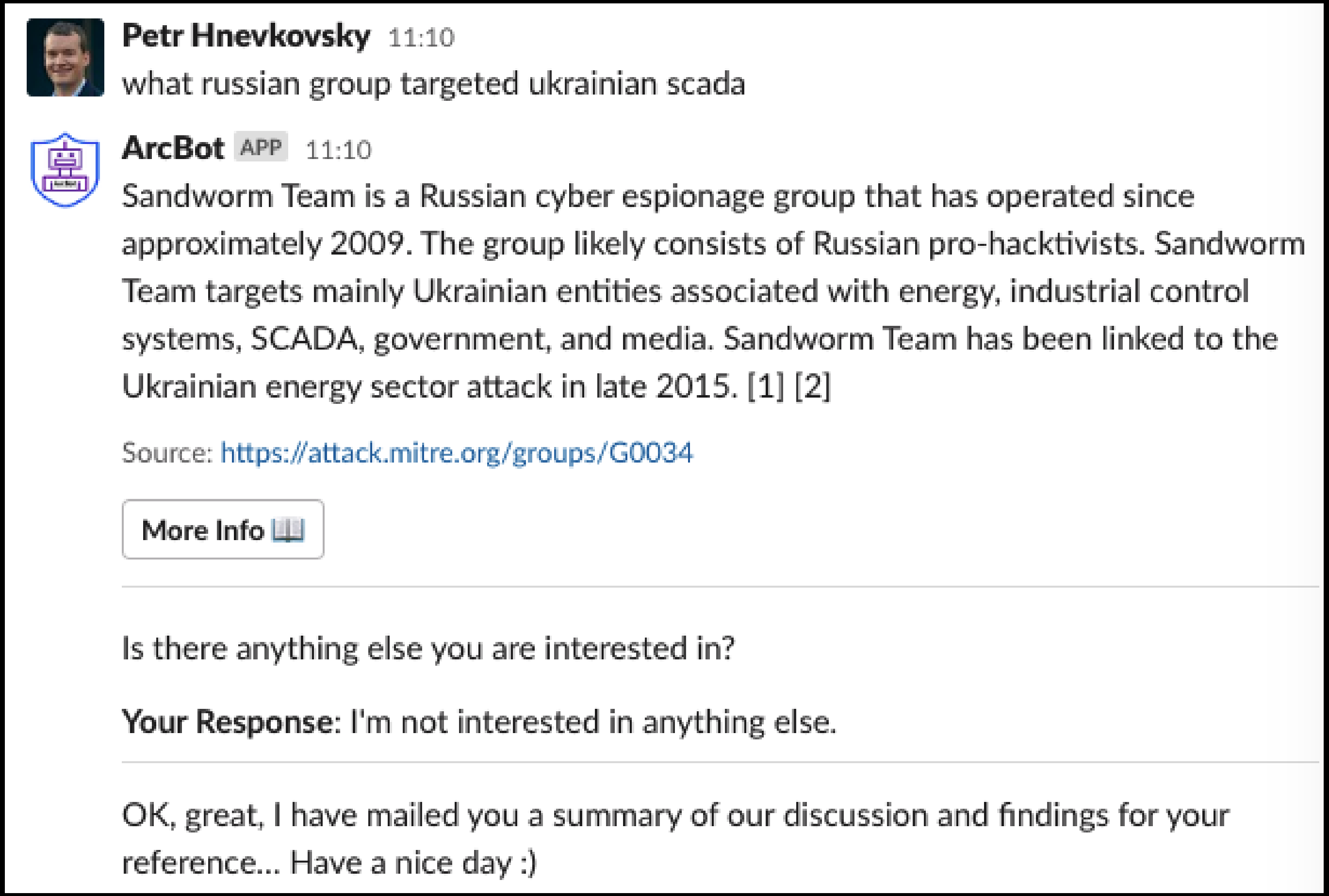
Petr Hnevkovsky 11:08
black dust

ArcBot APP 11:08
OK, let me check the BlackDust phishing campaign for you...

There are 4 reported incidents of BlackDust.

Is there anything else you are interested in?

1. Tell me about a particular phishing attack.



Petr Hnevkovsky 11:10
what russian group targeted ukrainian scada

ArcBot APP 11:10
Sandworm Team is a Russian cyber espionage group that has operated since approximately 2009. The group likely consists of Russian pro-hacktivists. Sandworm Team targets mainly Ukrainian entities associated with energy, industrial control systems, SCADA, government, and media. Sandworm Team has been linked to the Ukrainian energy sector attack in late 2015. [1] [2]

Source: https://attack.mitre.org/groups/G0034

Is there anything else you are interested in?

Your Response: I'm not interested in anything else.

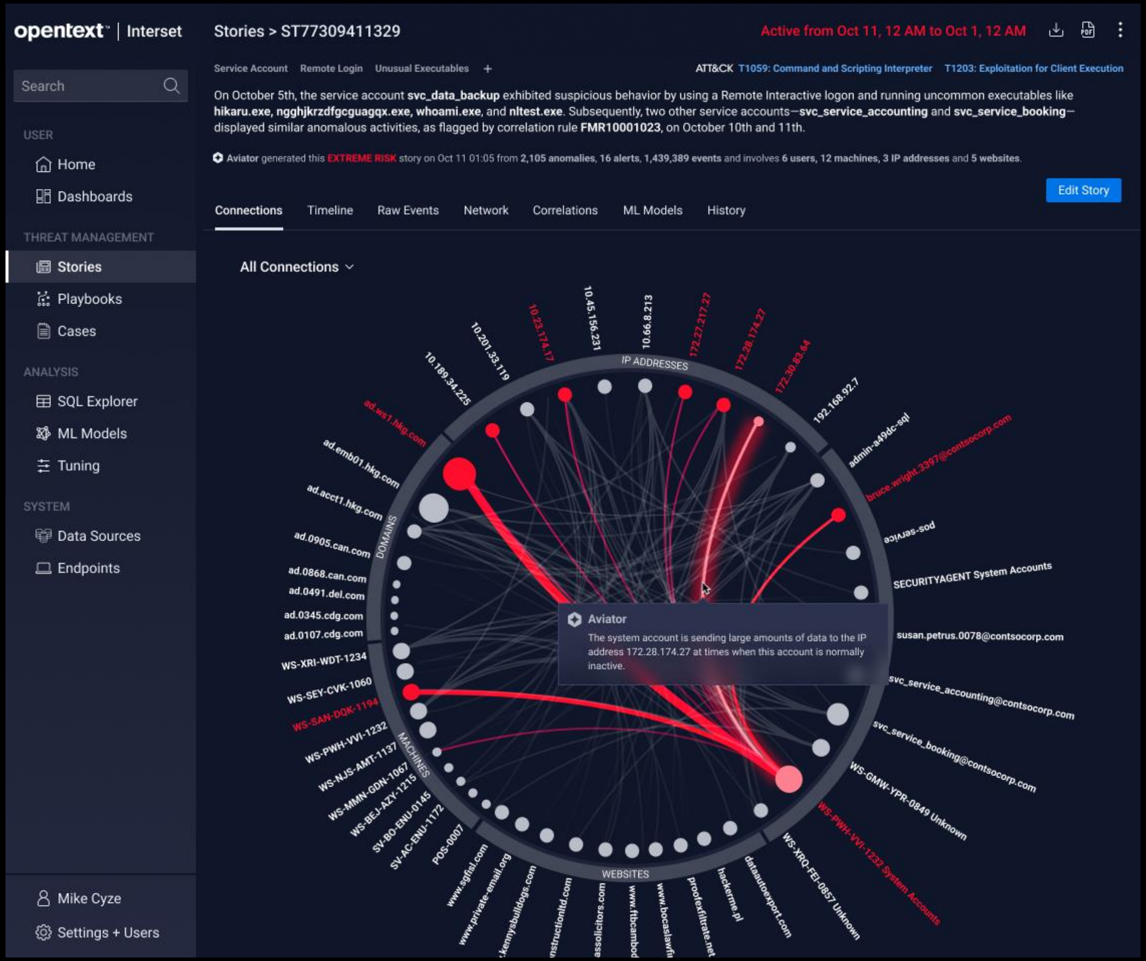
OK, great, I have mailed you a summary of our discussion and findings for your reference... Have a nice day :)

© 2023 Open Text

Vývoj přesných a spolehlivých schopnosti AI a RPA

RoboSOC*

- User & Entity Behaviour Analytics
- Security operations automation response
- Global adversary analytics



Stories > ST77309411329

Active from Oct 11, 12 AM to Oct 1, 12 AM

ATT&CK T1059: Command and Scripting Interpreter T1203: Exploitation for Client Execution

On October 5th, the service account **svc_data_backup** exhibited suspicious behavior by using a Remote Interactive logon and running uncommon executables like **hikaru.exe, ngghjkrzdfgcguagqx.exe, whoami.exe**, and **nltest.exe**. Subsequently, two other service accounts—**svc_service_accounting** and **svc_service_booking**—displayed similar anomalous activities, as flagged by correlation rule **FMR10001023**, on October 10th and 11th.

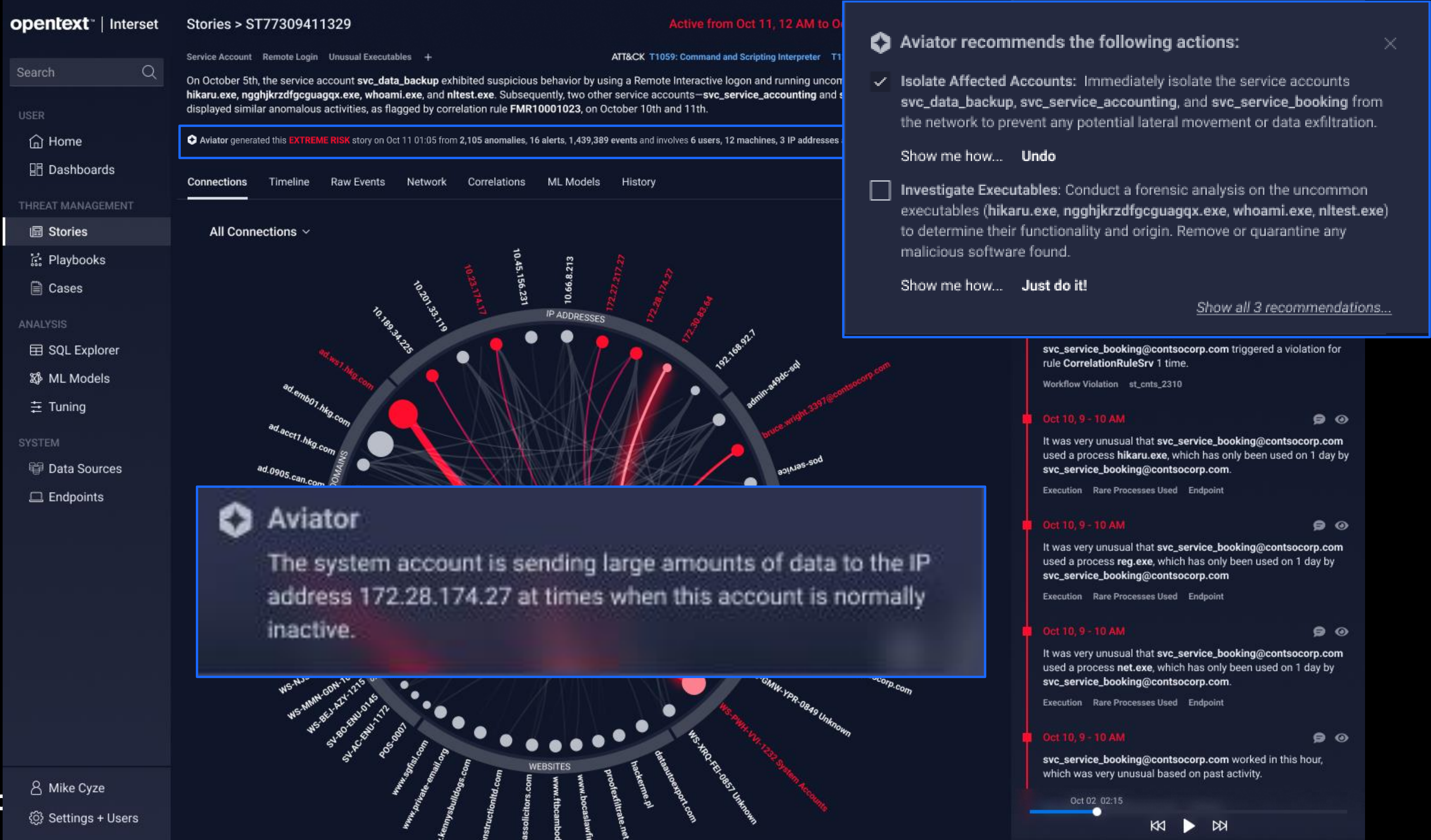
Aviator generated this **EXTREME RISK** story on Oct 11 01:05 from **2,105 anomalies, 16 alerts, 1,439,389 events** and involves **6 users, 12 machines, 3 IP addresses** and **5 websites**.

Aviator

The system account is sending large amounts of data to the IP address 172.28.174.27 at times when this account is normally inactive.

ArcSight Security Analytics

© 2023 Open Text



Stories > ST77309411329

Active from Oct 11, 12 AM to O

On October 5th, the service account **svc_data_backup** exhibited suspicious behavior by using a Remote Interactive logon and running uncom **hikaru.exe, nghjkrzdfgcguagqx.exe, whoami.exe**, and **nltest.exe**. Subsequently, two other service accounts—**svc_service_accounting** and displayed similar anomalous activities, as flagged by correlation rule **FMR10001023**, on October 10th and 11th.

Aviator generated this **EXTREME RISK** story on Oct 11 01:05 from **2,105 anomalies, 16 alerts, 1,439,389 events** and involves **6 users, 12 machines, 3 IP addresses**

Aviator recommends the following actions:

☑ **Isolate Affected Accounts:** Immediately isolate the service accounts **svc_data_backup**, **svc_service_accounting**, and **svc_service_booking** from the network to prevent any potential lateral movement or data exfiltration.

Show me how... **Undo**

☐ **Investigate Executables:** Conduct a forensic analysis on the uncommon executables (**hikaru.exe, ngghjkrzdfgcguagqx.exe, whoami.exe, nltest.exe**) to determine their functionality and origin. Remove or quarantine any malicious software found.

Show me how... **Just do it!**

Show all 3 recommendations...

svc_service_booking@contsocorp.com triggered a violation for rule **CorrelationRuleSrv** 1 time.

Workflow Violation st_cnts_2310

Oct 10, 9 - 10 AM

It was very unusual that **svc_service_booking@contsocorp.com** used a process **hikaru.exe**, which has only been used on 1 day by **svc_service_booking@contsocorp.com**.

Execution Rare Processes Used Endpoint

Oct 10, 9 - 10 AM

It was very unusual that **svc_service_booking@contsocorp.com** used a process **reg.exe**, which has only been used on 1 day by **svc_service_booking@contsocorp.com**

Execution Rare Processes Used Endpoint

Oct 10, 9 - 10 AM

It was very unusual that **svc_service_booking@contsocorp.com** used a process **net.exe**, which has only been used on 1 day by **svc_service_booking@contsocorp.com**.

Execution Rare Processes Used Endpoint

Oct 10, 9 - 10 AM

svc_service_booking@contsocorp.com worked in this hour, which was very unusual based on past activity.

Aviator

The system account is sending large amounts of data to the IP address 172.28.174.27 at times when this account is normally inactive.

Přesná detekce vnitřní hrozby pomocí jednoho zdroje

Snadno pochopitelné a kvalitní zacílení

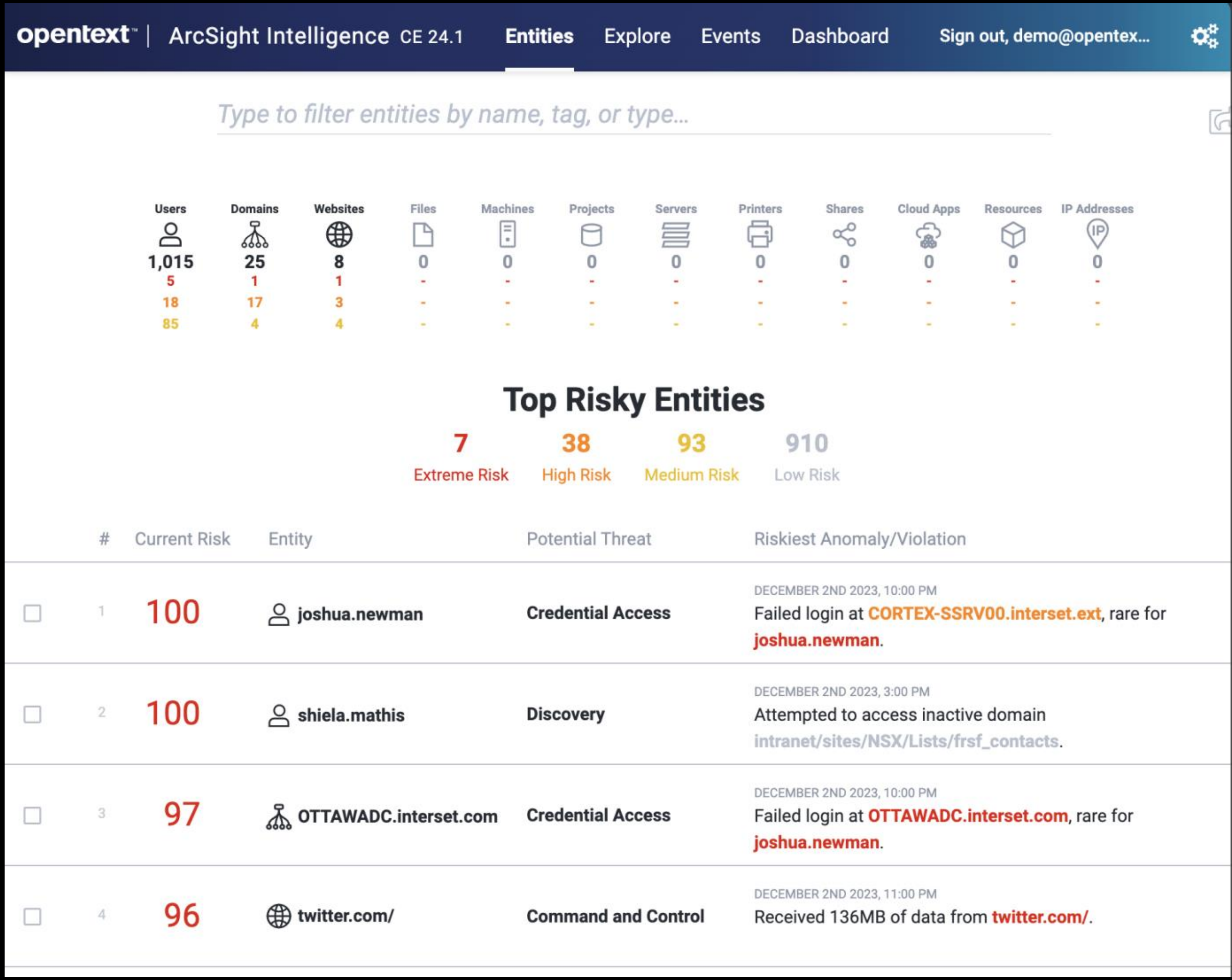
- Podniková špionáž
- Útoky na hesla
- Špatné IT postupy
- Exfiltrace dat

CROWDSTRIKE

MS Defender

SentinelOne

Azure AD


opentext™ | ArcSight Intelligence CE 24.1
Entities
Explore
Events
Dashboard
Sign out, demo@opentex...
Type to filter entities by name, tag, or type...

Users	Domains	Websites	Files	Machines	Projects	Servers	Printers	Shares	Cloud Apps	Resources	IP Addresses
1,015	25	8	0	0	0	0	0	0	0	0	0
5	1	1	-	-	-	-	-	-	-	-	-
18	17	3	-	-	-	-	-	-	-	-	-
85	4	4	-	-	-	-	-	-	-	-	-

Top Risky Entities

7	38	93	910
Extreme Risk	High Risk	Medium Risk	Low Risk

	#	Current Risk	Entity	Potential Threat	Riskiest Anomaly/Violation
☐	1	100	joshua.newman	Credential Access	DECEMBER 2ND 2023, 10:00 PM Failed login at CORTEX-SSRV00.interset.ext, rare for joshua.newman.
☐	2	100	shiela.mathis	Discovery	DECEMBER 2ND 2023, 3:00 PM Attempted to access inactive domain intranet/sites/NSX/Lists/frsf_contacts.
☐	3	97	OTTAWADC.interset.com	Credential Access	DECEMBER 2ND 2023, 10:00 PM Failed login at OTTAWADC.interset.com, rare for joshua.newman.
☐	4	96	twitter.com/	Command and Control	DECEMBER 2ND 2023, 11:00 PM Received 136MB of data from twitter.com/.

© 2023 Open Text

Kognitivní a reaktivní kybernetická obrana (XDR+)

Varovné signály

Dřívější detekce a vyhledávání hrozeb s cílem minimalizovat dobu zdržení.

Signály útočníka ze vzdáleného prostoru

Early warning signals and adversary analytics that indicate an imminent or impending attack.

Signály chování

User behavior analytics to identify insider threats often associated with compromised accounts/credentials.

Korelace

Real-time correlation that provides instant visibility into known threats as well as suspicious patterns.

Síťová detekce

Network telemetry to detect lateral movement, and anomalous traffic and provide forensic playback.

Řízení identit a koncových bodů

Identity account and endpoint blocking, containment, re-imaging, and forensics

MITRE ATT&CK Enterprise Matrix

WoA
WoC

Warnings of Attack
Warnings of Compromise

IoA

Indicators of Attack

IoC

Indicators of Compromise

opentext™

© 2023 Open Text

Kybernetická odolnost

- Ochrana aplikací, dat a identit
- Přesná detekce a automatizovaná reakce

Lidský kapitál

- Virtuální asistenti
- Partnerství mezi lidmi a umělou inteligencí
- 1 + 1 = 3

Digitální transformace

- Aviator podpoří Váš růst
- Umožněte své AI využívat svá data

opentext™

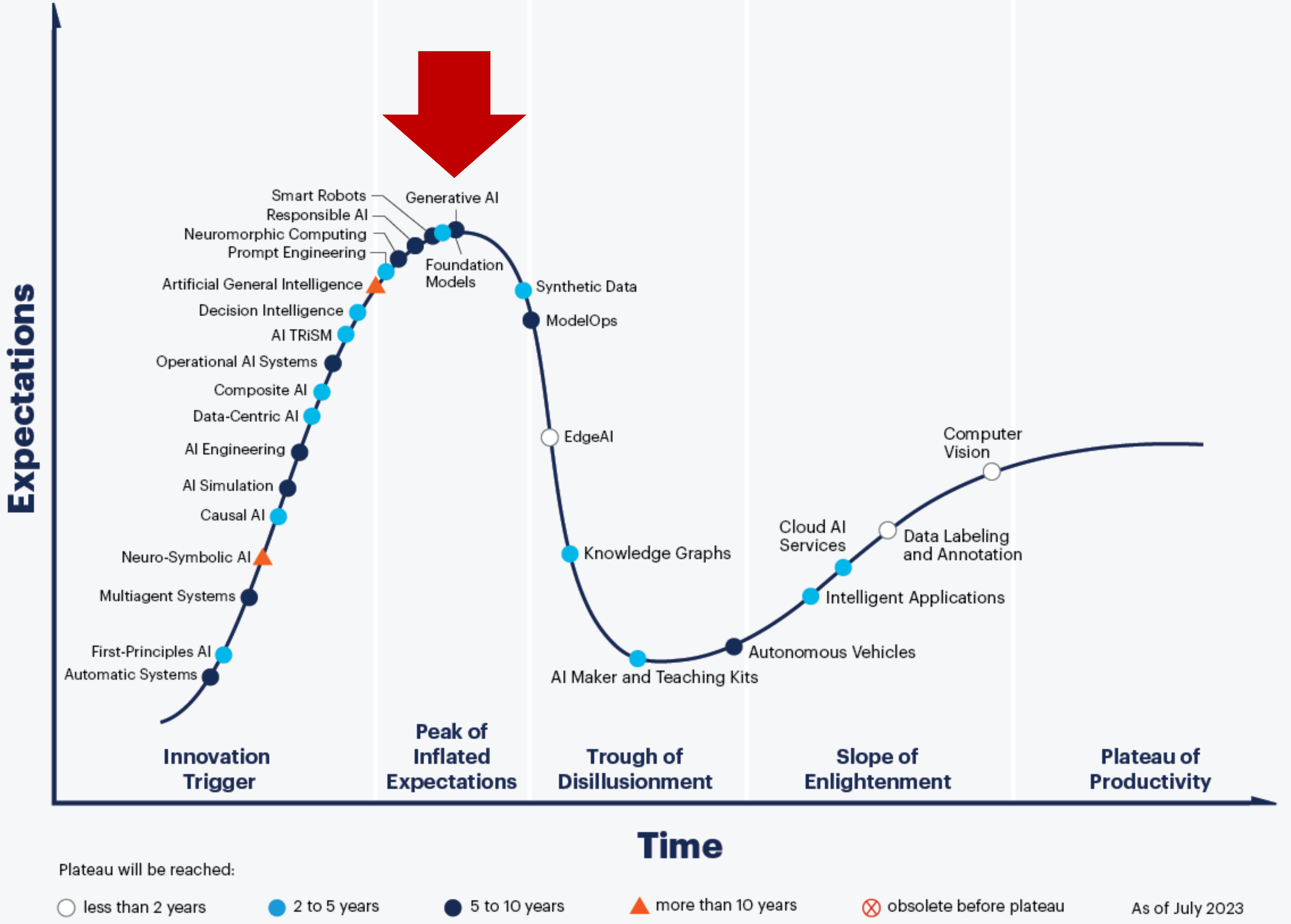
© 2023 Open Text

opentext™

Jak může AI Aviator zabezpečit vaše podnikání?

opentext.ai | phnevkovsky@opentext.com

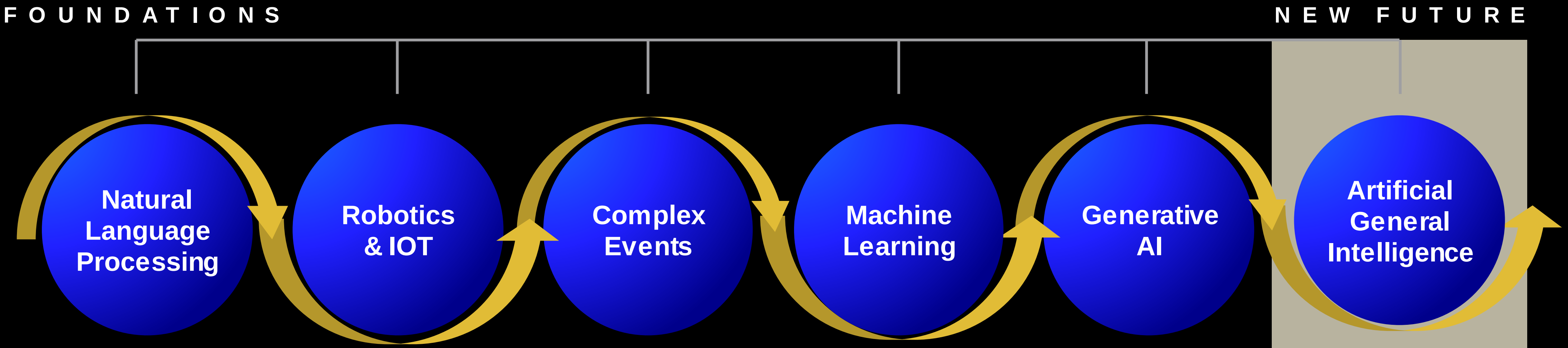
Generative AI achievement unlocked: maximum hype!



gartner.com

Source: Gartner
© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. 2079794

Two decades of AI innovations with 371+ AI patents



Natural Language Processing

- Programmed Translation
- Information Extraction

Robotics & IOT

- Process automation
- Optimization
- Expert systems

Complex Events

- Text to Speech
- Speech to Text
- Machine vision
- Image Recognition

Machine Learning

- Predictive Models
- Deep Learning
- Reinforced Learnings

Generative AI

- Prompt-engineering
- Large Language Models
- Vector DB
- API Orchestration

Artificial General Intelligence

- Automating decisions
- Machine made choices
- AI Trust, Risk & Security Management

© 2023 Open Text

Notable cybersecurity AI innovation milestones

2010

BrightCloud first cloud threat intelligence platform

2014

Interset User and Entity Behavioural Analytics

2019

Fortify Audit Assistant to triage testing results

2020

ArcSight Recon introduces outlier analytics

2023

Voltage Financial Risk calculator

© 2023 Open Text

Use the right AI for the right use case!

AppSec testing burden

- Noise reduction needed
- Time Intensive process
- AppSec auditor shortage
- Repetitive mundane reviews

© 2023 Open Text

Use the right AI for the right use case!

AppSec testing burden

- Noise reduction needed
- Time Intensive process
- AppSec auditor shortage
- Repetitive mundane reviews

	Random Forest	ChatGPT
Classification performance	Equal or better	Equal or worst
Parameters	8 million[1]	1.76 trillion[3] (~950,000 larger)
Memory	50 MB[1]	45 GB[2] (~1300 times larger)
Training cost	< $30.67	> $100,000,000 [4]
Training CPUs/GPUs	1-3	~10,000[5]
Prediction speed	milliseconds	seconds

Fortify Audit Assistant first & ground breaking since 2019

[1] Based on 10 forests, average of 114 trees, with an average maxDepth of 23. Computed using our default tunings, one forest per language

[2] Estimate from https://updf.com/knowledge/what-is-gpt-4/

[3] https://en.wikipedia.org/wiki/GPT-4 and Sam Altman

[4] Based on >700K FoD data, assuming 3xc5.large AWS instances on running for 12 hours, for 10 languages

[5] https://www.fierceelectronics.com/sensors/chatgpt-runs-10k-nvidia-training-gpus-potential-thousands-more

© 2023 Open Text

Use the right AI for the right use case

AppSec testing burden

- Noise reduction needed
- Time Intensive process
- AppSec auditor shortage
- Repetitive mundane reviews

Up to **98%** accuracy

Immediate actionable results

- Prioritization on high impact results
- Reduce manual effort
- Granular labelling
- Human AI assistant

Fortify Audit Assistant first & ground breaking since 2019

© 2023 Open Text

Learning from AI to build better suited solutions

2020 Key SOC challenges

- Talent shortage
- Long exposure time
- Evolving threats
- Information overload
- Manual repetitive task

Robotic Driven SOC 1/4

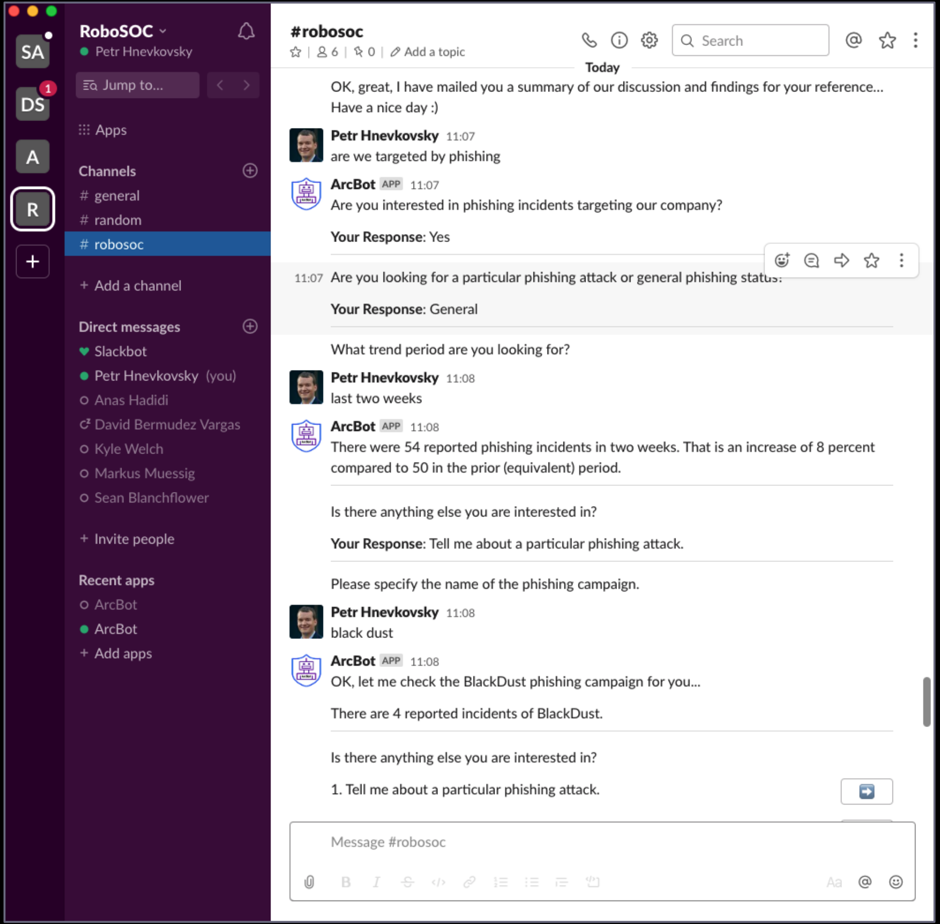
AI and RPA Improving SecOps

RoboSOC Security Guide

Innovation Lab

© 2023 Open Text

Gain immediate insight without technical burden



OK, great, I have mailed you a summary of our discussion and findings for your reference... Have a nice day :)

Petr Hnevkovsky 11:07
are we targeted by phishing

ArcBot APP 11:07
Are you interested in phishing incidents targeting our company?

Your Response: Yes

11:07 Are you looking for a particular phishing attack or general phishing status?

Your Response: General

What trend period are you looking for?

Petr Hnevkovsky 11:08
last two weeks

ArcBot APP 11:08
There were 54 reported phishing incidents in two weeks. That is an increase of 8 percent compared to 50 in the prior (equivalent) period.

Is there anything else you are interested in?

Your Response: Tell me about a particular phishing attack.

Please specify the name of the phishing campaign.

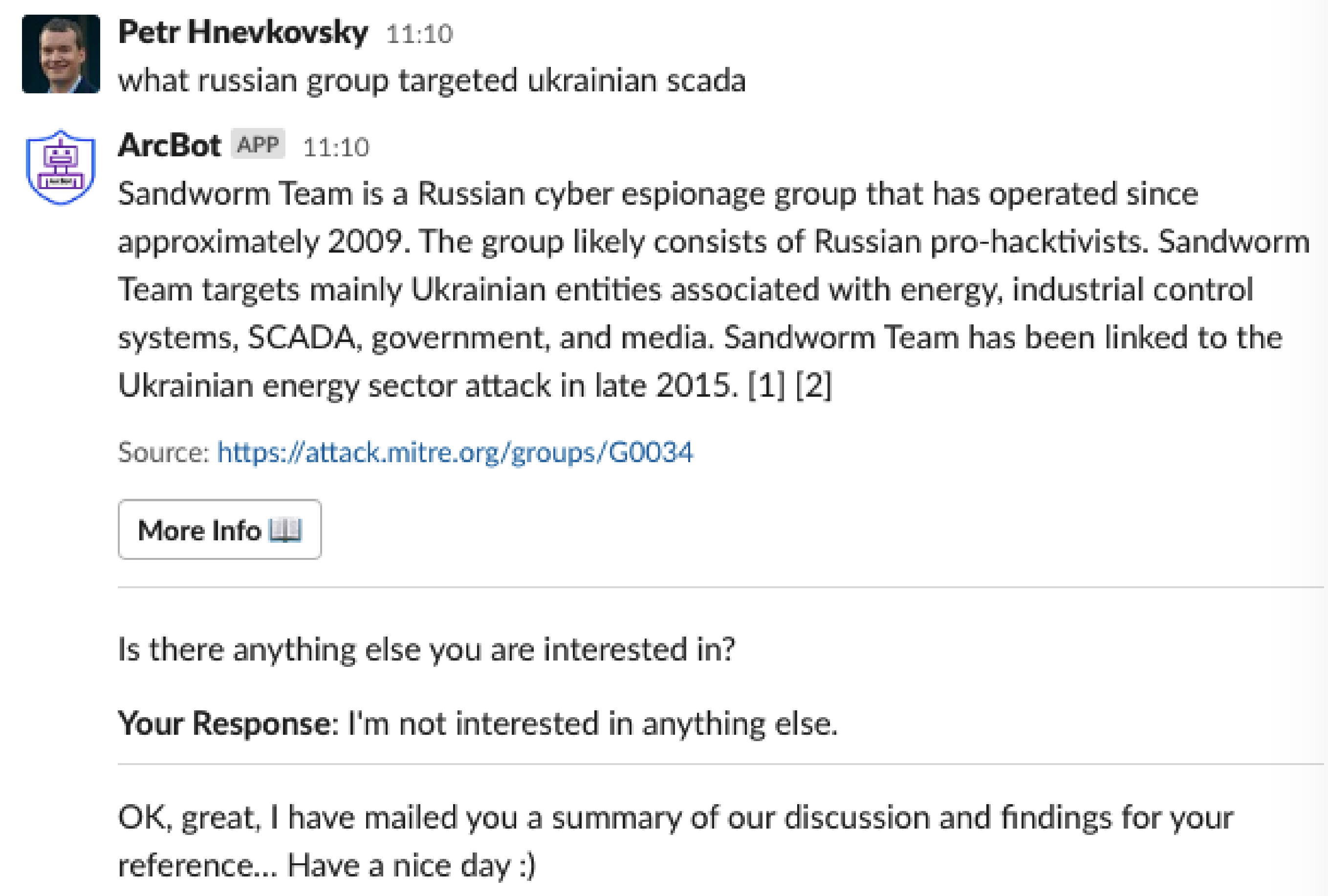
Petr Hnevkovsky 11:08
black dust

ArcBot APP 11:08
OK, let me check the BlackDust phishing campaign for you...

There are 4 reported incidents of BlackDust.

Is there anything else you are interested in?

1. Tell me about a particular phishing attack.



Petr Hnevkovsky 11:10
what russian group targeted ukrainian scada

ArcBot APP 11:10
Sandworm Team is a Russian cyber espionage group that has operated since approximately 2009. The group likely consists of Russian pro-hacktivists. Sandworm Team targets mainly Ukrainian entities associated with energy, industrial control systems, SCADA, government, and media. Sandworm Team has been linked to the Ukrainian energy sector attack in late 2015. [1] [2]

Source: https://attack.mitre.org/groups/G0034

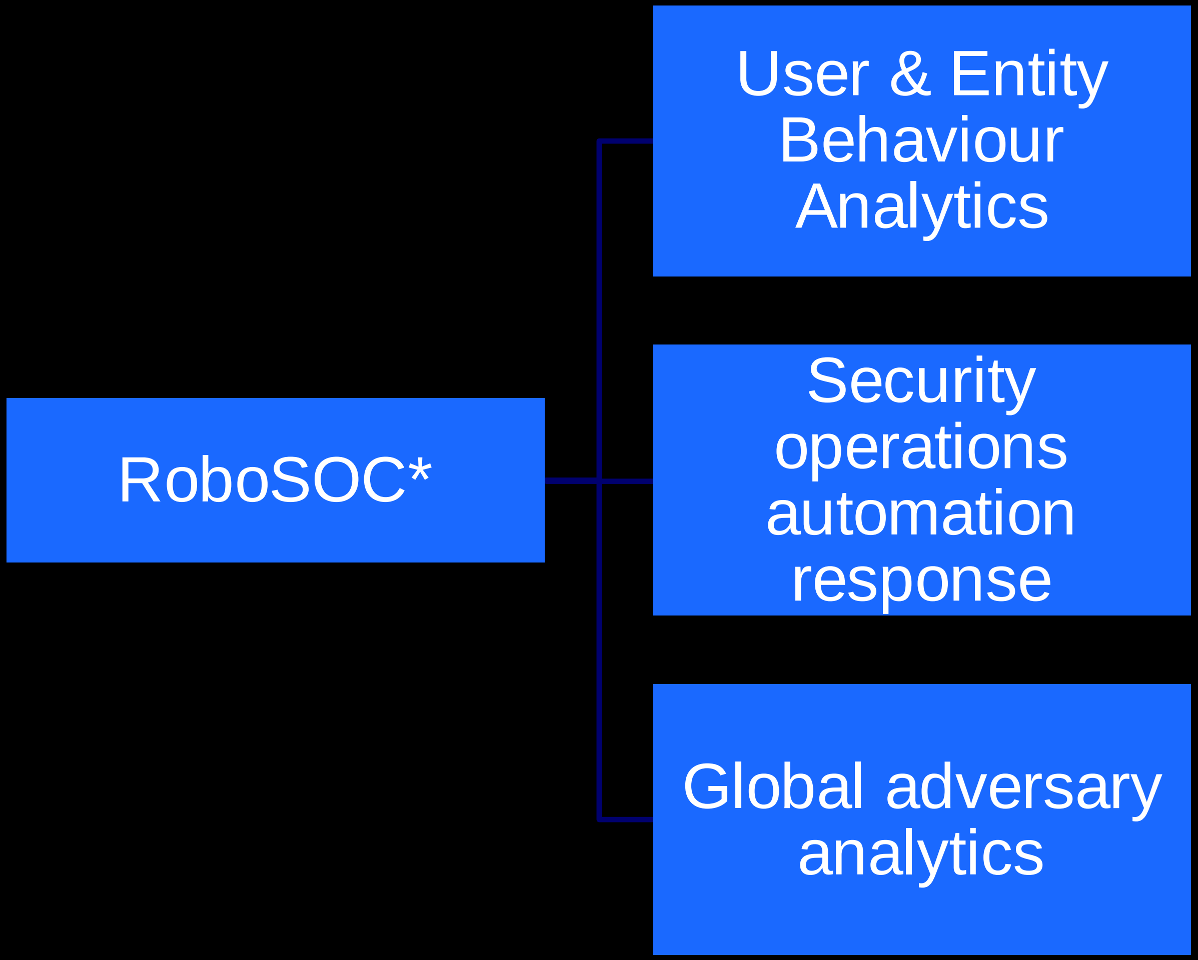
Is there anything else you are interested in?

Your Response: I'm not interested in anything else.

OK, great, I have mailed you a summary of our discussion and findings for your reference... Have a nice day :)

© 2023 Open Text

Derived new accurate & reliable AI and RPA capabilities

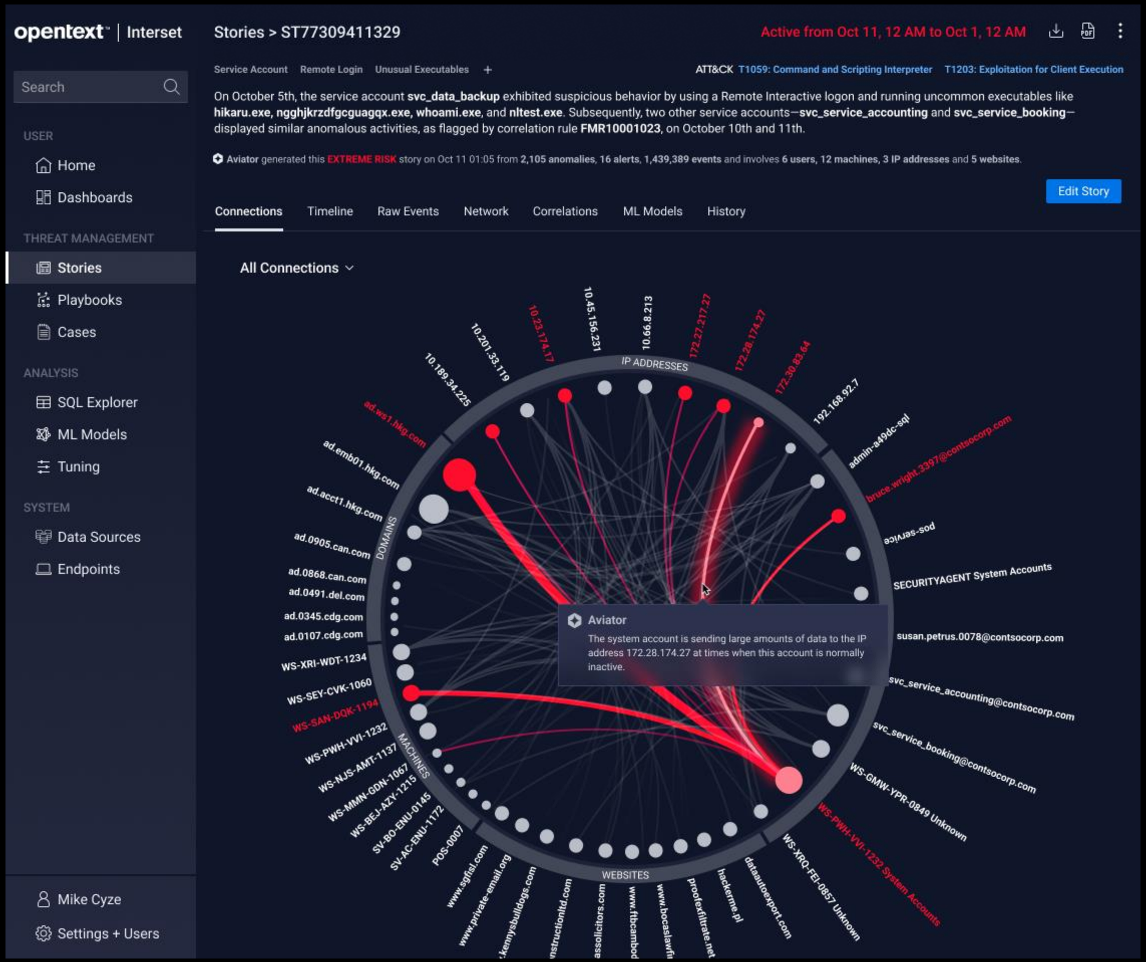


RoboSOC*

User & Entity Behaviour Analytics

Security operations automation response

Global adversary analytics



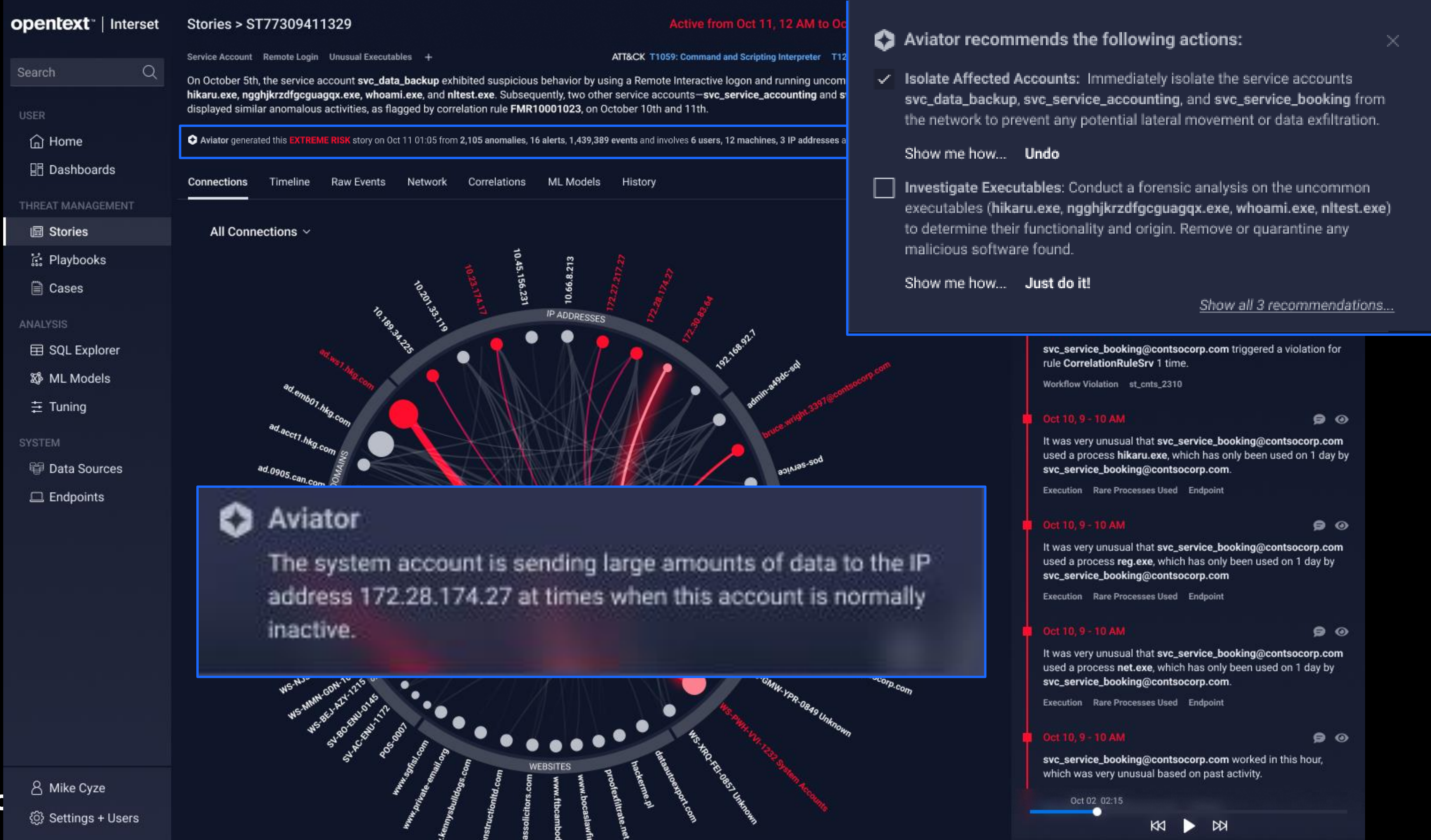
On October 5th, the service account **svc_data_backup** exhibited suspicious behavior by using a Remote Interactive logon and running uncommon executables like **hikaru.exe, ngghjkrzdfgcguagqx.exe, whoami.exe**, and **nltest.exe**. Subsequently, two other service accounts—**svc_service_accounting** and **svc_service_booking**—displayed similar anomalous activities, as flagged by correlation rule **FMR10001023**, on October 10th and 11th.

Aviator generated this EXTREME RISK story on Oct 11 01:05 from **2,105 anomalies, 16 alerts, 1,439,389 events** and involves **6 users, 12 machines, 3 IP addresses** and **5 websites**.

Aviator

The system account is sending large amounts of data to the IP address 172.28.174.27 at times when this account is normally inactive.

ArcSight Security Analytics



Stories > ST77309411329

Active from Oct 11, 12 AM to Oc

On October 5th, the service account **svc_data_backup** exhibited suspicious behavior by using a Remote Interactive logon and running uncom **hikaru.exe, ngghjkrzdfgcguagqx.exe, whoami.exe**, and **nltest.exe**. Subsequently, two other service accounts—**svc_service_accounting** and s displayed similar anomalous activities, as flagged by correlation rule **FMR10001023**, on October 10th and 11th.

Aviator generated this **EXTREME RISK** story on Oct 11 01:05 from **2,105 anomalies, 16 alerts, 1,439,389 events** and involves **6 users, 12 machines, 3 IP addresses** a

Aviator recommends the following actions:

☑ **Isolate Affected Accounts:** Immediately isolate the service accounts **svc_data_backup**, **svc_service_accounting**, and **svc_service_booking** from the network to prevent any potential lateral movement or data exfiltration.

☐ **Investigate Executables**: Conduct a forensic analysis on the uncommon executables (**hikaru.exe, ngghjkrzdfgcguagqx.exe, whoami.exe, nltest.exe**) to determine their functionality and origin. Remove or quarantine any malicious software found.

Aviator

The system account is sending large amounts of data to the IP address 172.28.174.27 at times when this account is normally inactive.

svc_service_booking@contsocorp.com triggered a violation for rule **CorrelationRuleSrv** 1 time.

Workflow Violation st_cnts_2310

Oct 10, 9 - 10 AM

It was very unusual that **svc_service_booking@contsocorp.com** used a process **hikaru.exe**, which has only been used on 1 day by **svc_service_booking@contsocorp.com**.

Execution Rare Processes Used Endpoint

Oct 10, 9 - 10 AM

It was very unusual that **svc_service_booking@contsocorp.com** used a process **reg.exe**, which has only been used on 1 day by **svc_service_booking@contsocorp.com**

Execution Rare Processes Used Endpoint

Oct 10, 9 - 10 AM

It was very unusual that **svc_service_booking@contsocorp.com** used a process **net.exe**, which has only been used on 1 day by **svc_service_booking@contsocorp.com**.

Execution Rare Processes Used Endpoint

Oct 10, 9 - 10 AM

svc_service_booking@contsocorp.com worked in this hour, which was very unusual based on past activity.

Detect Insider Threat accurately & with one rich source

Easy to understand high-quality insight to

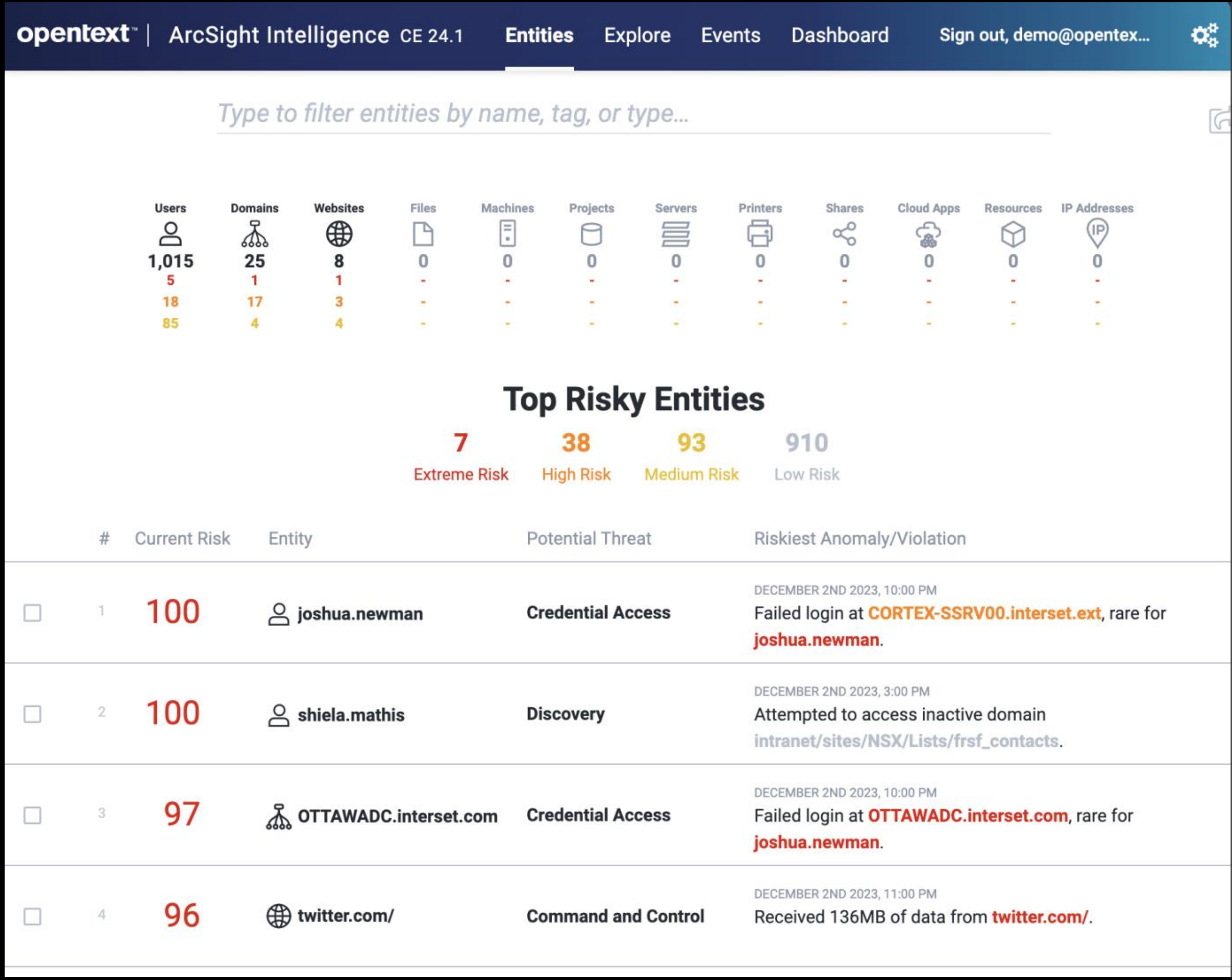
- Data Exfiltration
- Corporate Espionage
- Password Brute Forcing
- Bad IT Hygiene

CROWDSTRIKE

MS Defender

SentinelOne

Azure AD


opentext™ | ArcSight Intelligence CE 24.1
Entities
Explore
Events
Dashboard
Sign out, demo@opentex...
Type to filter entities by name, tag, or type...

Users	Domains	Websites	Files	Machines	Projects	Servers	Printers	Shares	Cloud Apps	Resources	IP Addresses
1,015	25	8	0	0	0	0	0	0	0	0	0
5	1	1	-	-	-	-	-	-	-	-	-
18	17	3	-	-	-	-	-	-	-	-	-
85	4	4	-	-	-	-	-	-	-	-	-

Top Risky Entities

7	38	93	910
Extreme Risk	High Risk	Medium Risk	Low Risk

	#	Current Risk	Entity	Potential Threat	Riskiest Anomaly/Violation
☐	1	100	joshua.newman	Credential Access	DECEMBER 2ND 2023, 10:00 PM Failed login at CORTEX-SSRV00.interset.ext, rare for joshua.newman.
☐	2	100	shiela.mathis	Discovery	DECEMBER 2ND 2023, 3:00 PM Attempted to access inactive domain intranet/sites/NSX/Lists/frsf_contacts.
☐	3	97	OTTAWADC.interset.com	Credential Access	DECEMBER 2ND 2023, 10:00 PM Failed login at OTTAWADC.interset.com, rare for joshua.newman.
☐	4	96	twitter.com/	Command and Control	DECEMBER 2ND 2023, 11:00 PM Received 136MB of data from twitter.com/.

© 2023 Open Text

Cognitive / Responsive Cyber Defense (XDR +)

Warning Signals

Threat detection and hunting earlier to minimize dwell time

Far-space Adversary Signals

Early warning signals and adversary analytics that indicate an imminent or impending attack.

Behavioral Signals

User behavior analytics to identify insider threats often associated with compromised accounts/credentials.

Correlation

Real-time correlation that provides instant visibility into known threats as well as suspicious patterns.

Network Detection

Network telemetry to detect lateral movement, and anomalous traffic and provide forensic playback.

Identity and Endpoint Controls

Identity account and endpoint blocking, containment, re-imaging, and forensics

ATT&CK* Enterprise Matrix

WoA
WoC

Warnings of Attack
Warnings of Compromise

IoA

Indicators of Attack

IoC

Indicators of Compromise

© 2023 Open Text

Cyber resilience

- Protect apps, data and identities
- Detect & respond

Human capital

- Provide virtual assistants
- Human & AI partnership
  1 + 1 = 3

Digital transformation

- Aviator boosts your growth
- Enable your AI with your data

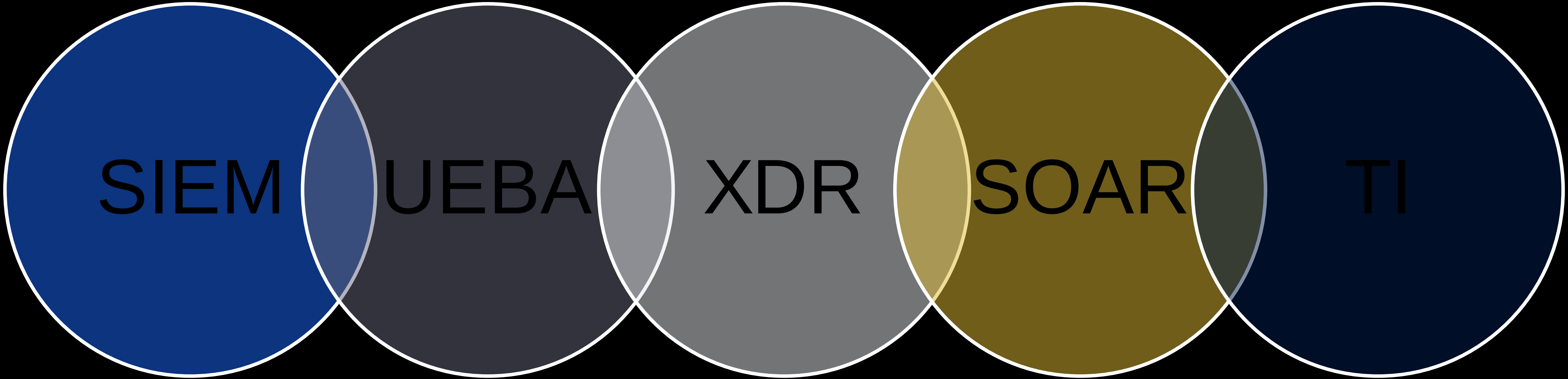
© 2023 Open Text

How can AI Aviator secure your business?

opentext.ai | phnevkovsky@opentext.com

© 2023 Open Text

Security analytics convergence



SIEM

UEBA

XDR

SOAR

TI

© 2023 Open Text

ArcSight Intelligence unique values

Minutes instead of days or never

Accurate Detection

Self-learning Intelligence

Friction-less Integration

Reduce TCO

© 2023 Open Text

Enable your AI models and sensitive data analytics

AI data challenges now and forever

- Data sprawl
- Compliance mandate
- Sensitive data leak
- Public environments
- Biases & pollution

Discover	• Structured & unstructured
Classify	• Understand risk
Act	• Sanitize & protect

Voltage Fusion Data Privacy and Protection

© 2023 Open Text