シリコンバレー駐在員が語るRSAカンファレンス2024 ～セキュリティトレンドの最前線～

2024/5/30

セミナープログラム

16:00～	**東京エレクトロン デバイスと日立ソリューションズ ～各社の米国ビジネスについて～** 各社の米国ビジネスの概要についてご説明いたします。 Hitachi Solutions America, Ltd. Business Designer, Business Development and Alliances **Koson Aoki**
16:10～	**RSAカンファレンス2024 ～セキュリティトレンド最前線を探る～** 会場、EXPOの雰囲気、Innovation Sandboxの結果を交えてレポートします。 東京エレクトロン デバイスと日立ソリューションズのシリコンバレー駐在員が参加し、 彼らの目線で見えるセキュリティトレンドを解説いたします。 TOKYO ELECTRON DEVICE AMERICA, INC Senior Technical Marketing Specialist **Tommy Miyoshi** Hitachi Solutions America, Ltd. Manager, Business Development and Alliances **Aya Goke**
17:00	**終了予定**

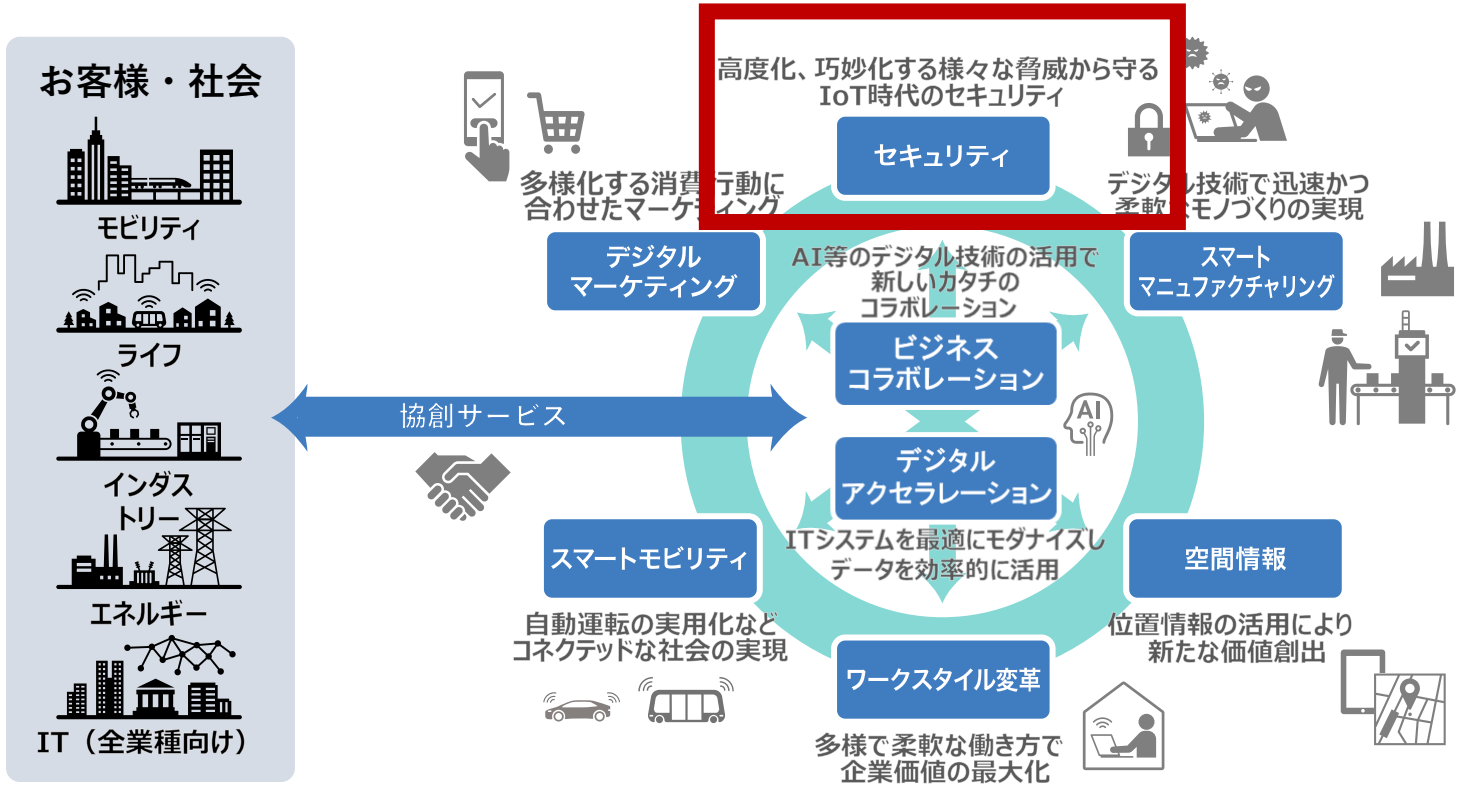
東京エレクトロン デバイスと日立ソリューションズ
～各社の米国ビジネスについて～

株式会社日立ソリューションズ

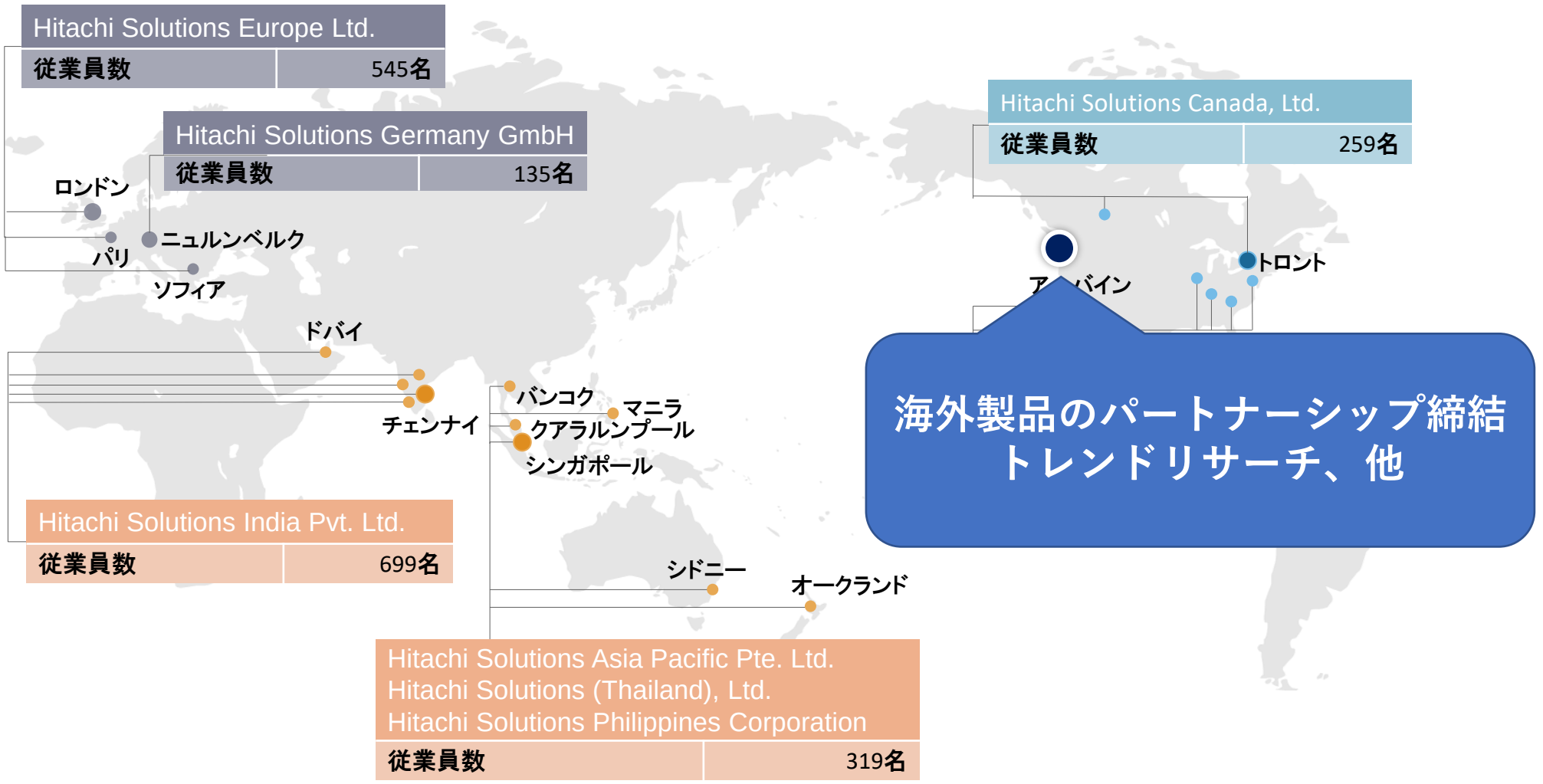
設立年月日	1970年(昭和45年)9月21日
代表者等	取締役社長 山本 二雄
資本金	200億円
従業員数	4,914名(単独) 13,861名(連結) 2022年9月30日現在
主な事業内容	**ソフトウェア・サービス事業** **情報処理機器販売事業**

本社所在地：東京都品川区東品川四丁目１２番７号
最寄駅：JRりんかい線　品川シーサイド駅

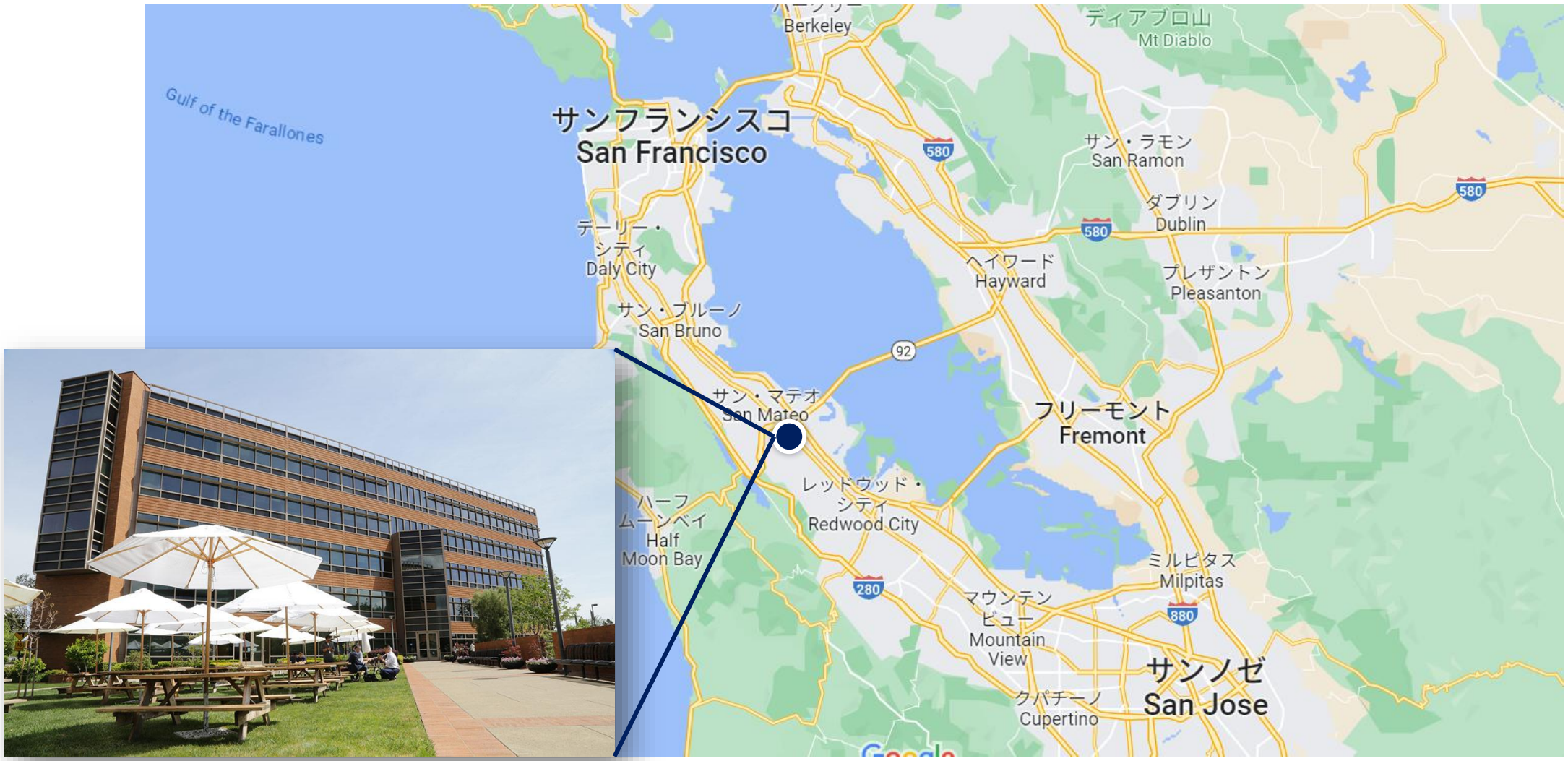
豊富な知識、最新の技術で、さまざまな製品やサービスを柔軟に組み合わせ、お客様や社会の課題に対して最適なソリューションをグローバルに提供



株式会社日立ソリューションズ　海外ビジネス



株式会社日立ソリューションズ　シリコンバレー拠点



HITACHI Inspire the Next　株式会社 日立ソリューションズ

東京エレクトロン デバイス

東京エレクトロン デバイス株式会社

設立年月日	1986年3月3日
代表者等	代表取締役社長 徳重 敦之
資本金	24億9千5百万円
従業員数	1,318名(連結) 2023年3月31日現在
主な事業内容	**半導体及び電子デバイス（EC）事業** **コンピュータシステム関連（CN）事業**

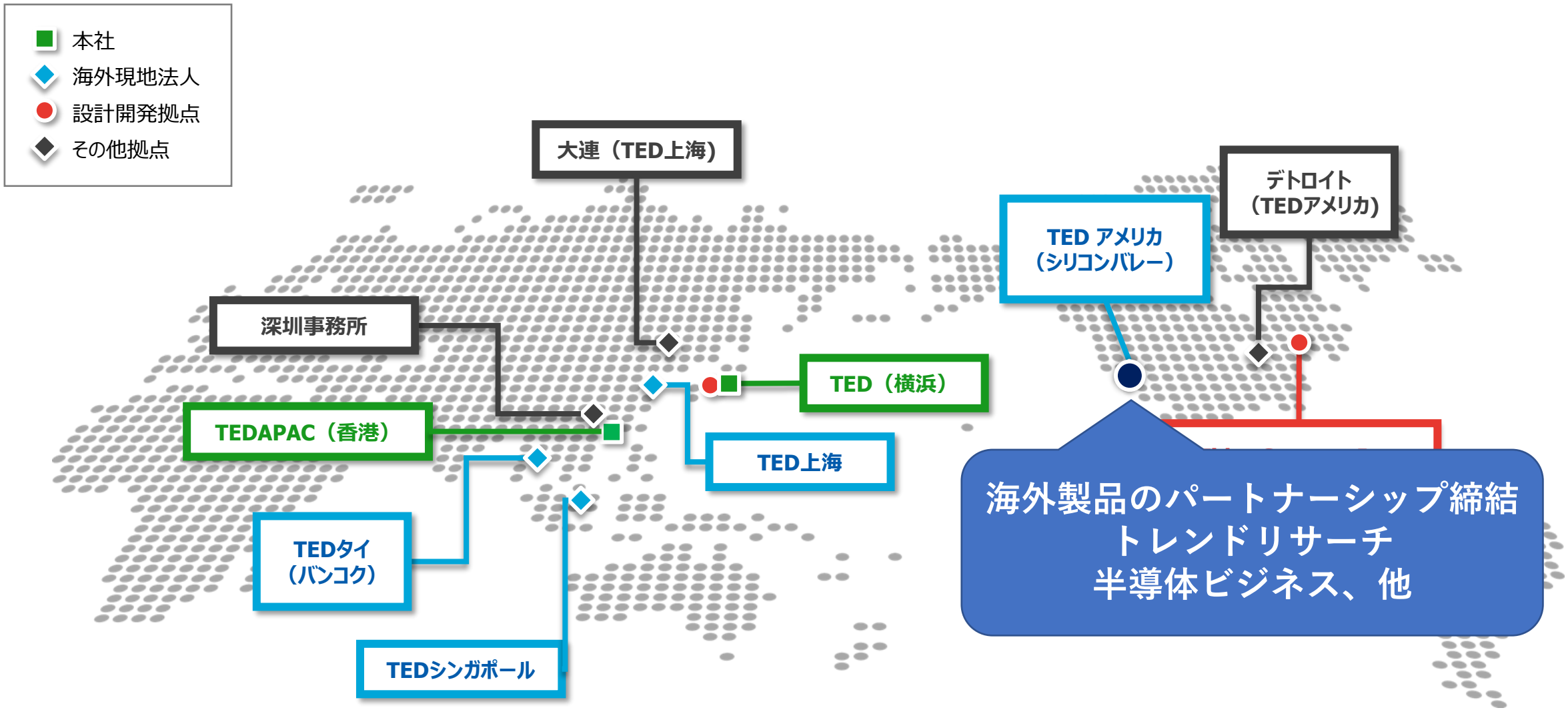
本社所在地：神奈川県横浜市神奈川区金港町１番地４
横浜イーストスクエア
最寄駅：JR線　横浜駅

最先端の半導体やネットワークシステムなどを、高度な技術サポートと、徹底した検証による品質保証とともに提供する技術商社

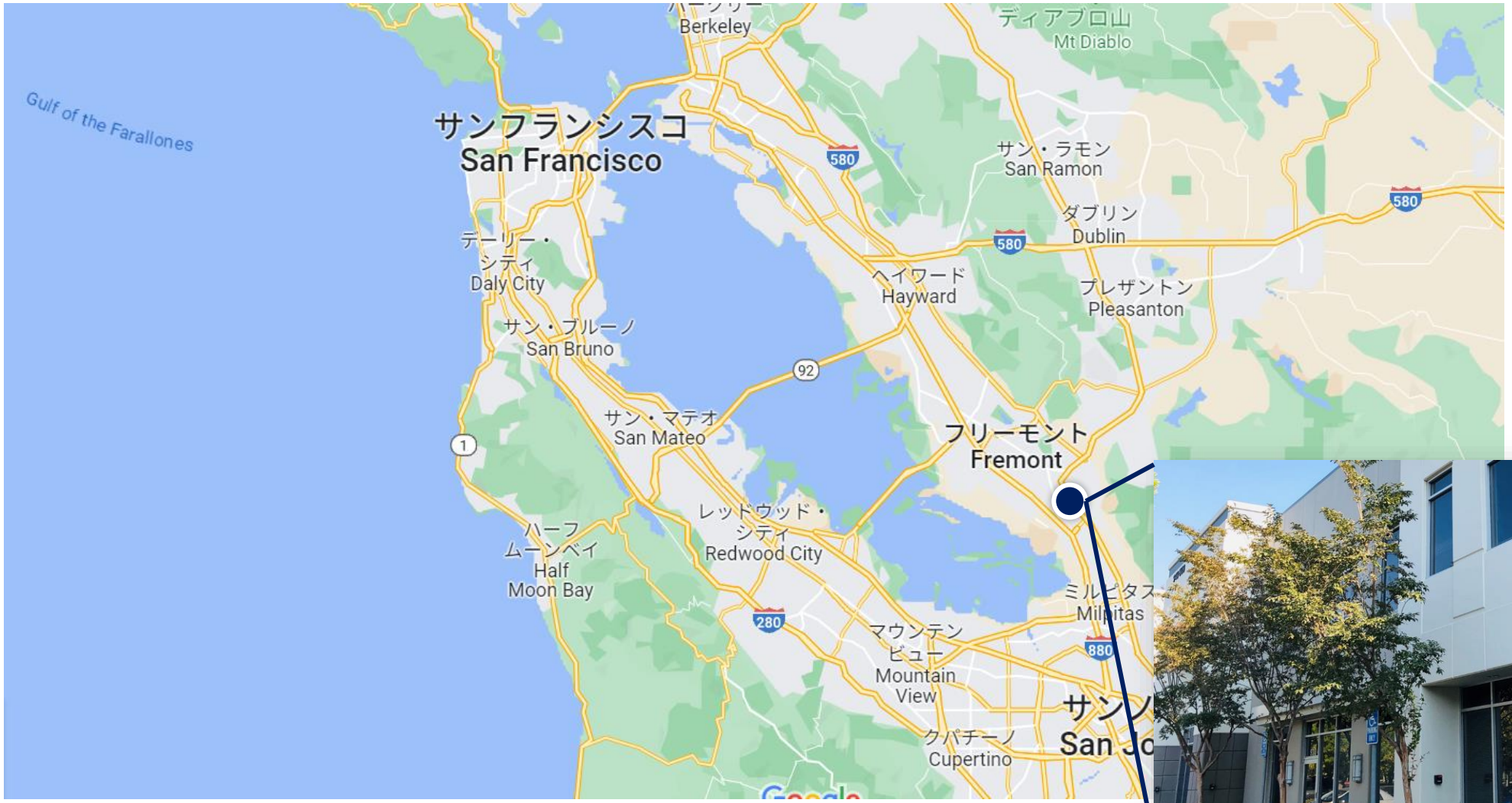
HITACHI Inspire the Next　株式会社 日立ソリューションズ

東京エレクトロン デバイス

東京エレクトロン デバイス株式会社　海外ビジネス



東京エレクトロン デバイス株式会社 シリコンバレー拠点



HITACHI
Inspire the Next
株式会社 日立ソリューションズ

東京エレクトロン デバイス

RSAカンファレンス2024
～セキュリティトレンド最前線を探る～

Agenda

- RSA Conference Viewing
- Sessions
- Innovation Sandbox
- Expo
- Networking
- Sum-up

Agenda

- **RSA Conference Viewing**
- Sessions
- Innovation Sandbox
- Expo
- Networking
- Sum-up

What is the RSA Conference?

RSAカンファレンスとは・・・

1991年からつづく

世界最大級のセキュリティカンファレンス

The 2024 theme - “The Art of Possible”

Passes & Rates

Show Details	Full Conference	Expo Plus	Expo	On Demand
EARLY BIRD | (OCT 24 - JAN 12)				+
DISCOUNT | (JAN 13 - APR 5)				+
STANDARD | (APR 6 - MAY 3)				×
REGULAR	$2,695	$495	$99	$695
LOYALTYPLUS	$2,395	$495	$99	$695
GOVERNMENT	$2,395	$495	$99	$695
1DAY	$1,535	$495	$99	$695
STUDENT/FACULTY	$875	$495	$99	$695

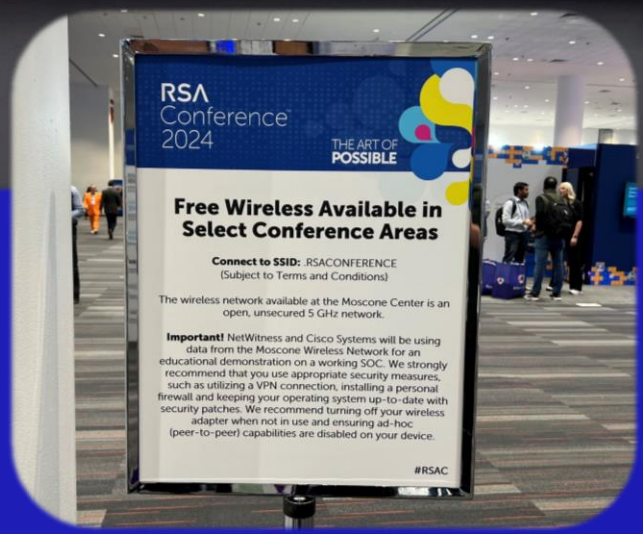

RSAConference2024
THE ART OF POSSIBLE
RSAConference2024
San Francisco | May 6 – 9 | Moscone Center
RSAC Perks Pack
Look inside for chances to participate in RSAC sponsor giveaways, drawings, and more. Simply bring your booklet to corresponding sponsor booths to redeem for prizes and other Conference perks.
THE ART OF POSSIBLE
#RSAC
Google Cloud Security
Trellix
Akamai
BlackBerry
CHECK POINT
CROWDSTRIKE
FORTINET
IBM
splunk>
VARONIS

The scenery of this year

THE ART OF POSSIBLE

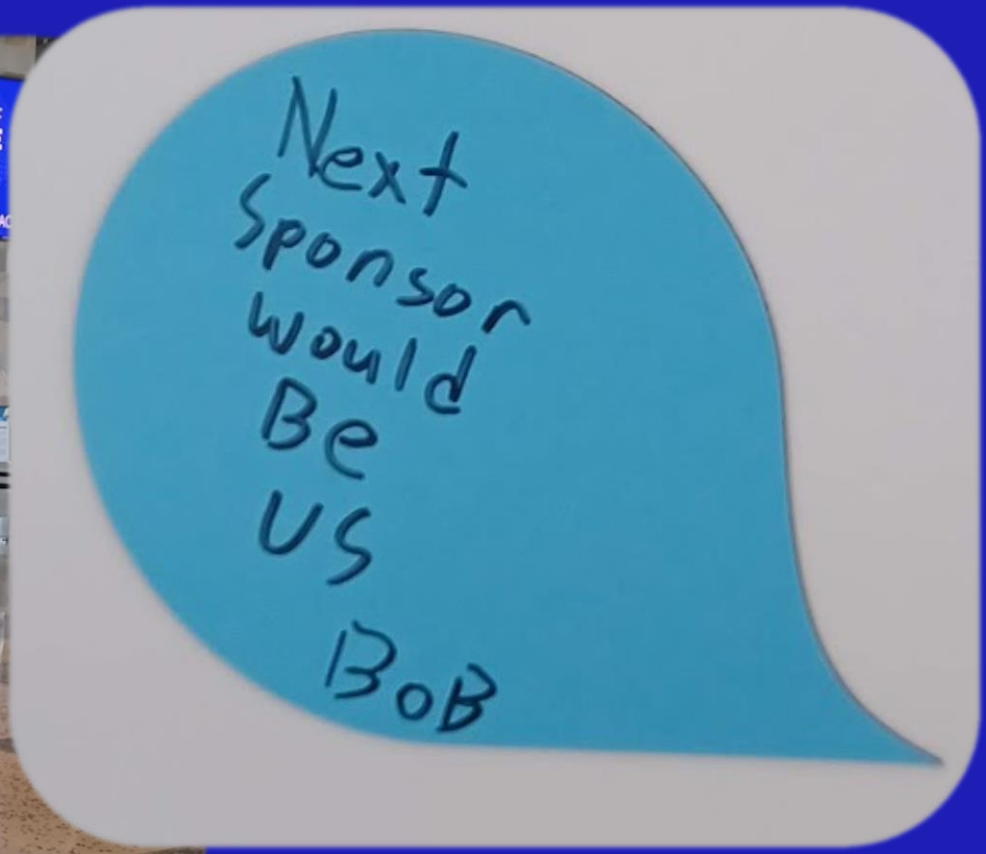
The scenery of this year

The scenery of this year



THE ART OF POSSIBLE

The scenery of this year



THE ART OF POSSIBLE

The scenery of this year

The scenery of this year

THE ART OF POSSIBLE

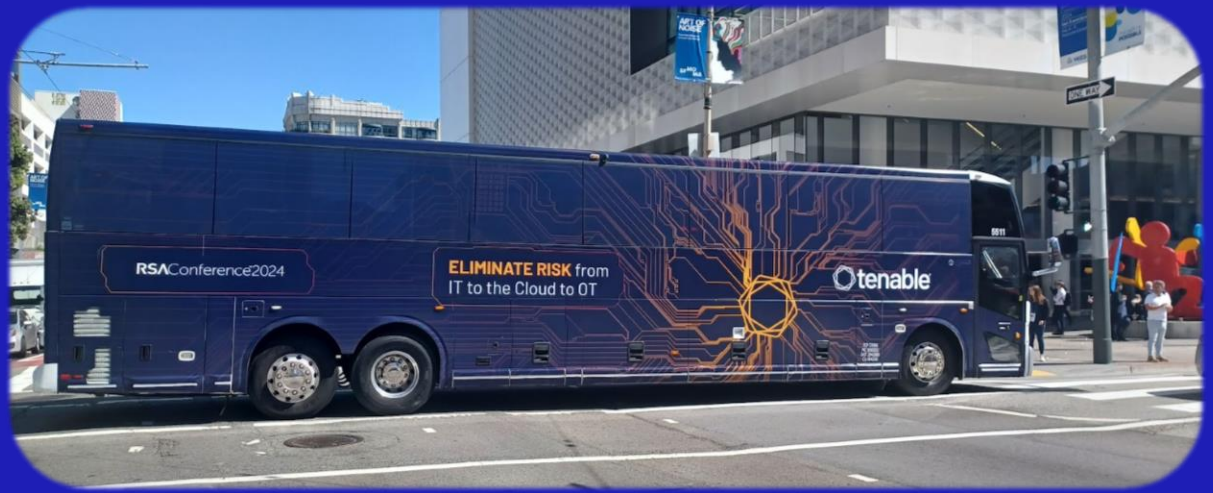
The scenery of this year

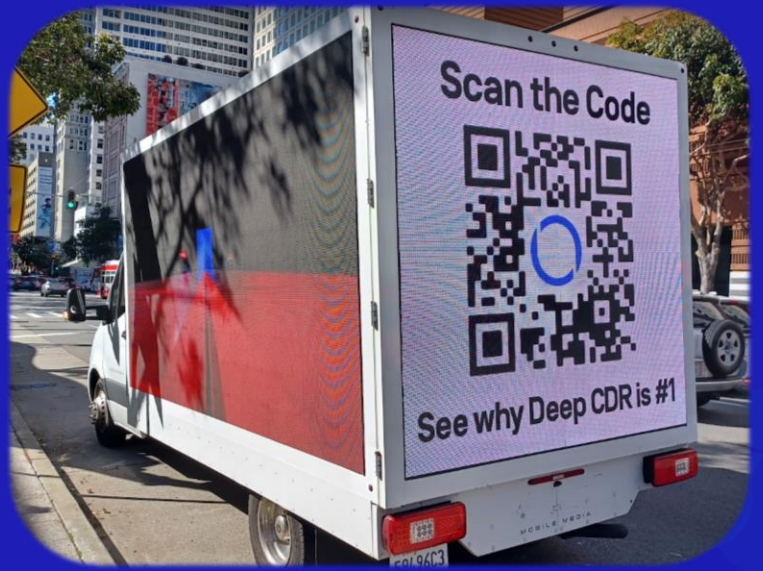

rubrik
rubrik
COMPLETE
CYBER RESILIENCE
DELIVERED


Joyride PIZZA
Bar One
Bar One
A SentinelOne Experience


FOGO DE CHÃO
Synack

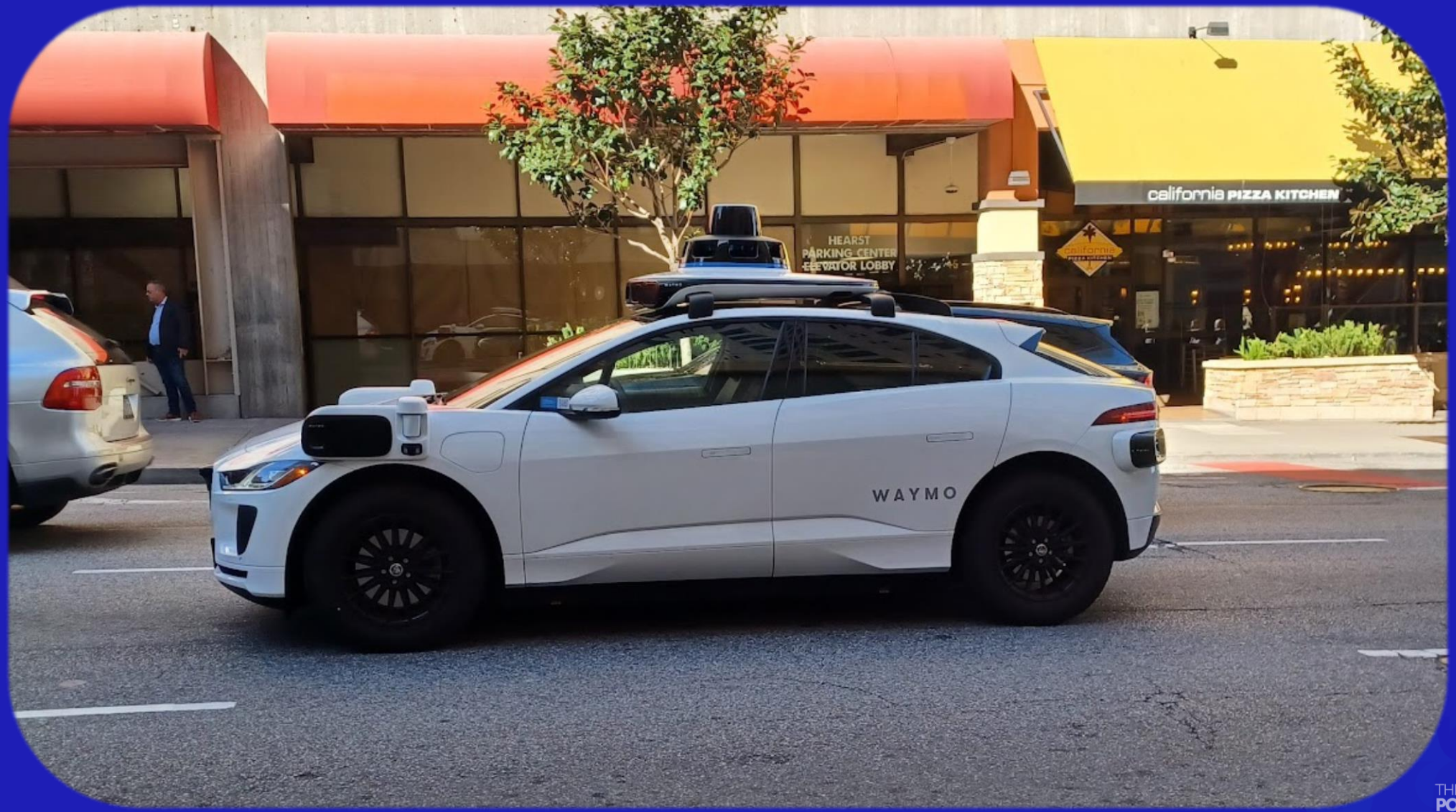
The scenery of this year





THE ART OF POSSIBLE

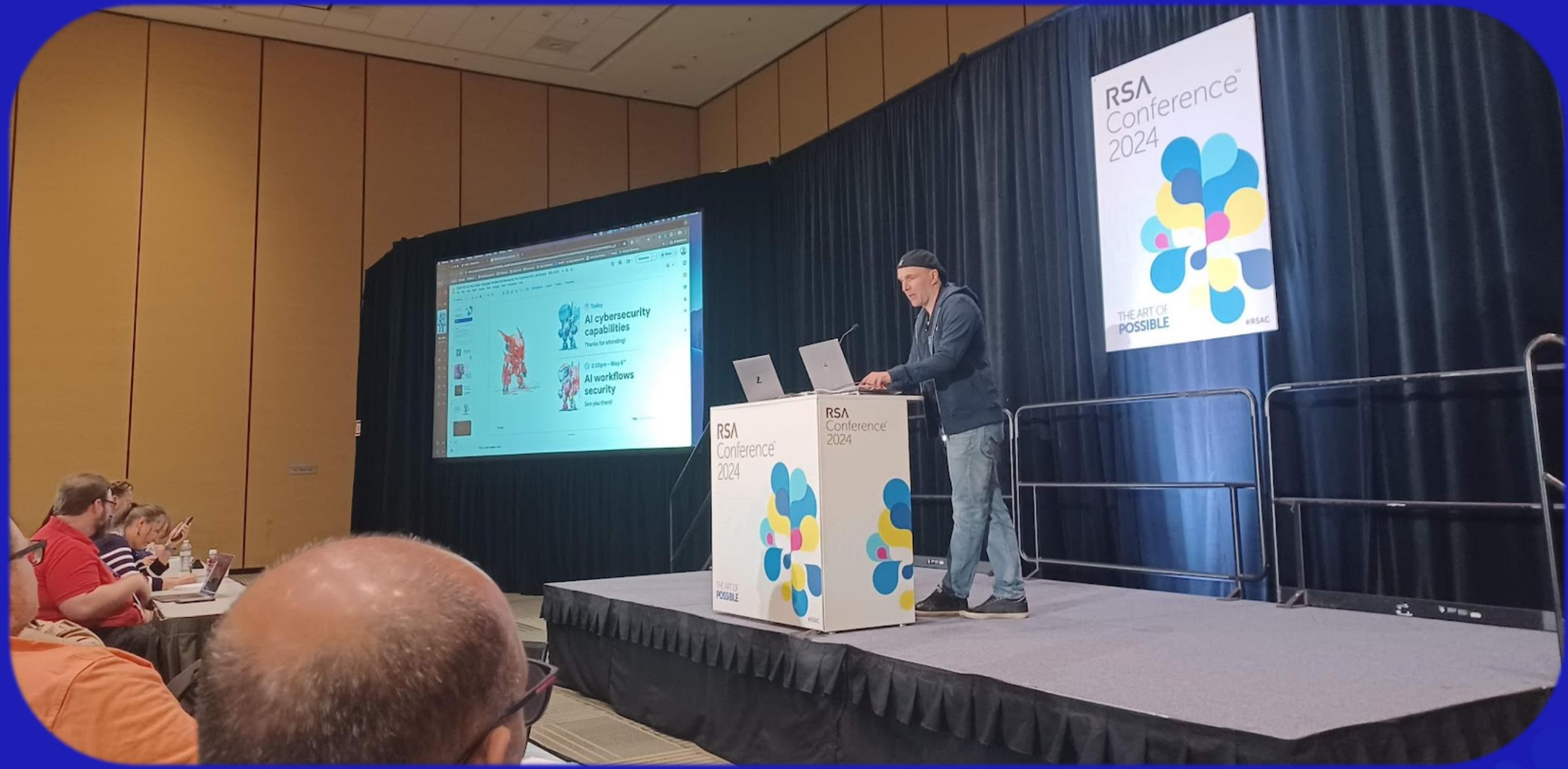
The scenery of this year



Agenda

- RSA Conference Viewing
- Sessions
- Innovation Sandbox
- Expo
- Networking
- Sum-up


ThirdParty&VendorRiskManagement
Privacy&DataProtection
CSuiteView
HumanElement
Analytics&Intelligence
CloudSecurity
Policy&Government
IntersectionofAI&Security
Law
Identity
DevSecOps&ApplicationSecurity
Hackers&Threats
Innovation&Startups
Cryptography
GovernanceRisk&Compliance
SecurityStrategy&Architecture
ProfessionalDevelopment&PersonnelManagement
Consumer&IndustrialTechnologies



Elie Bursztein
Google &
DeepMind
AI Cybersecurity
Technical
And
Research Lead,
Google
DeepMind

How Large Language Models Are Reshaping the Cybersecurity Landscape

THE ART OF POSSIBLE

How Large Language Models Are Reshaping the Cybersecurity Landscape

Current AI weaponization risks assessment

Phishing

Risk: ●●●●●

LLM might write more convincing personalized BEC phishing emails using OSINT info

Malware

Risk: ●●

GenAI can be abused to create malicious documents that escape traditional AVs, no real world evidence yet

Misinformation

Risk: ●●●●●

GenAI can be used to create more believable disinformation campaigns

Proliferation?

Risk: ●

Unproven concerns that GenAI can be used to build nuclear, chemical, biological weapons

How Large Language Models Are Reshaping the Cybersecurity Landscape

The LLM blackmarket is already in full swing

Name	Price	Functionality			w/wo Voucher Copy	Infrastructure
		Malware	Phishing Email	Scam Site		
CodeGPT	10 βytes*	●	○	○	No	Jailbreak prompts
MakerGPT	10 βytes*	●	○	◐	No	Jailbreak prompts
FraudGPT	$90/month	●	●	●	No	-
WorkGPT	€100/month	●	●	○	No	-
XXXGPT	$90/month	●	○	○	Yes	Jailbreak prompts
WolfGPT	$150	●	●	●	No	Uncensored LLM
Evil-GPT	$10	●	●	●	No	Uncensored LLM
DarkBERT	$90/month	●	●	○	No	-
DarkBARD	$80/month	◐	◐	○	No	-
BadGPT	$120/month	◐	◐	◐	No	Censored LLM
BLACKHATGPT	$199/month	●	○	○	No	-
EscapeGPT	$64.98/month	●	◐	◐	No	Uncensored LLM
FreedomGPT	$10/100 messages	●	○	○	Yes	Uncensored LLM
DarkGPT	$0.78/50 messages	●	○	○	Yes	Uncensored LLM

*βytes is the forum token of hackforums.net: ◐ indicates implicit mention.

https://arxiv.org/pdf/2401.03315v1.pdf

THE ART OF POSSIBLE

How Large Language Models Are Reshaping the Cybersecurity Landscape

LM capabilities explored today

Scaling content review

Detecting Multi-modal malware

Securing codebases

Speeding up incident response

How Large Language Models Are Reshaping the Cybersecurity Landscape

PayPal

Thank You for Your Order!

Dear Luca Invernizzi, we appreciate your business and are excited to have you as a customer. Your bitcoin purchase has been successfully completed.

Order Confirmation

Order Confirmation Number	15985578144
Date of Purchase	22 March 2024
Order Amount	$299.99
Product	BTC (Bitcoin)

If you have any questions or need assistance, please call Customer Support at +1 (866) 278-4075.

Customer Details

Name	Luca Invernizzi
Email	invernizzi.l@gmail.com

Please call us on **+1 (866) 278-4075** within 24 hours of receiving this email if you need to cancel your order.

Thanks and Regards,
Kiarra Paul Schneider
PayPal Support Team
PAYPZMK7OXDTM4

This document is likely a phishing attempt impersonating Paypal and should not be trusted. Here are some reasons why:

- Suspicious phone number: The phone number "+1 (866) 278-4075" does not match the official PayPal customer support phone numbers.
- Urgency or pressure tactics: The document urges you to call within 24 hours to cancel the order, creating a sense of urgency and pressuring you to act quickly.
- Call back requested: The document asks you to call a specific phone number, which could be used to steal your personal information.

Perfectly understood the image complex content

Identified key discrepancy from real invoice

Retrieval data will be key here to get correct number

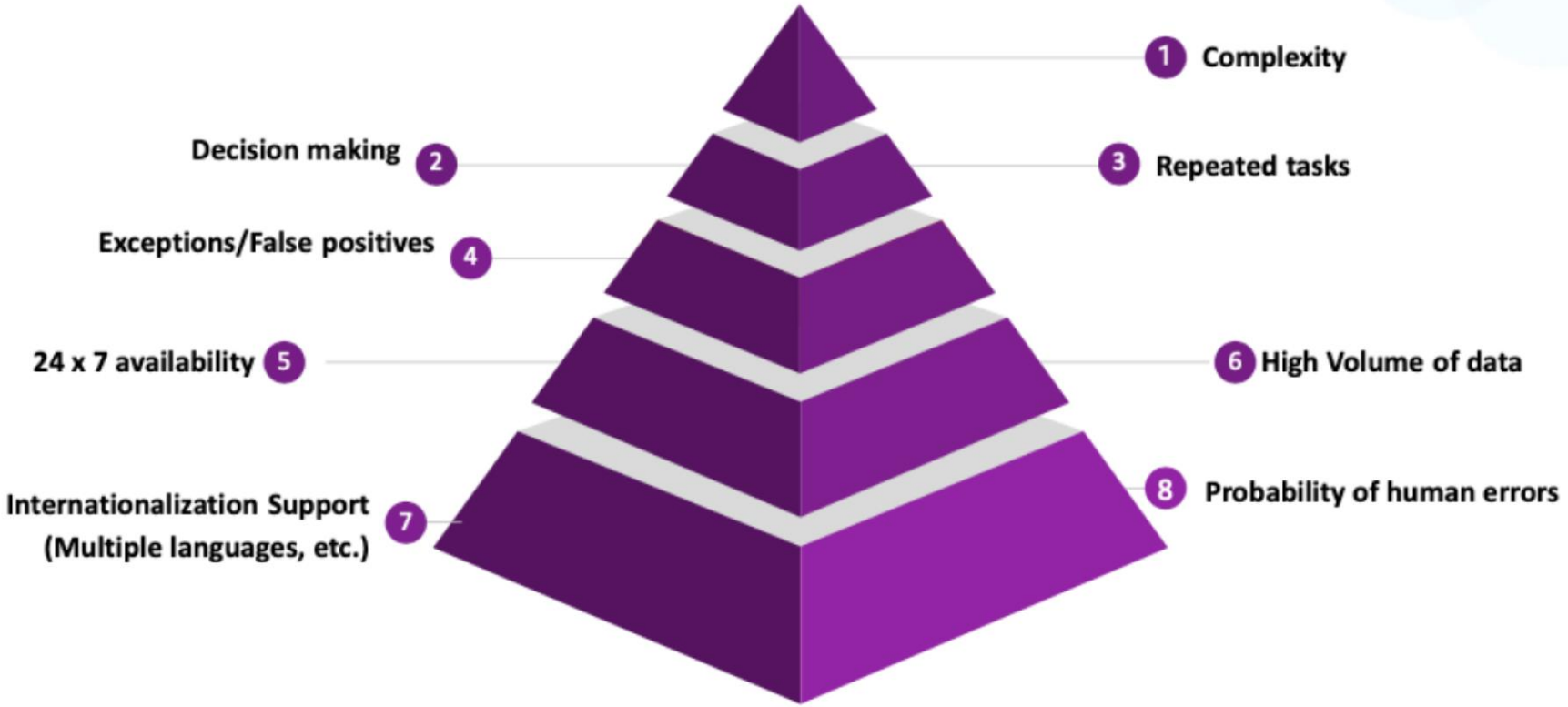
Correctly assessed risk and consequence

RSAConference2024

THE ART OF POSSIBLE

How Large Language Models Are Reshaping the Cybersecurity Landscape

Metrics To Measure AI Impact On Cybersecurity Products



Teza Mukkavilli
CISO, ChargePoint

Gopi Ramamoorthy
Head of Security & GRC Engineering, Symmetry Systems

THE ART OF POSSIBLE

Top 10 Security Products That Would Be Elevated or Eliminated by GenAI

Let's Ask AI: Perplexity's Response

Which cybersecurity product will be eliminated by AI?

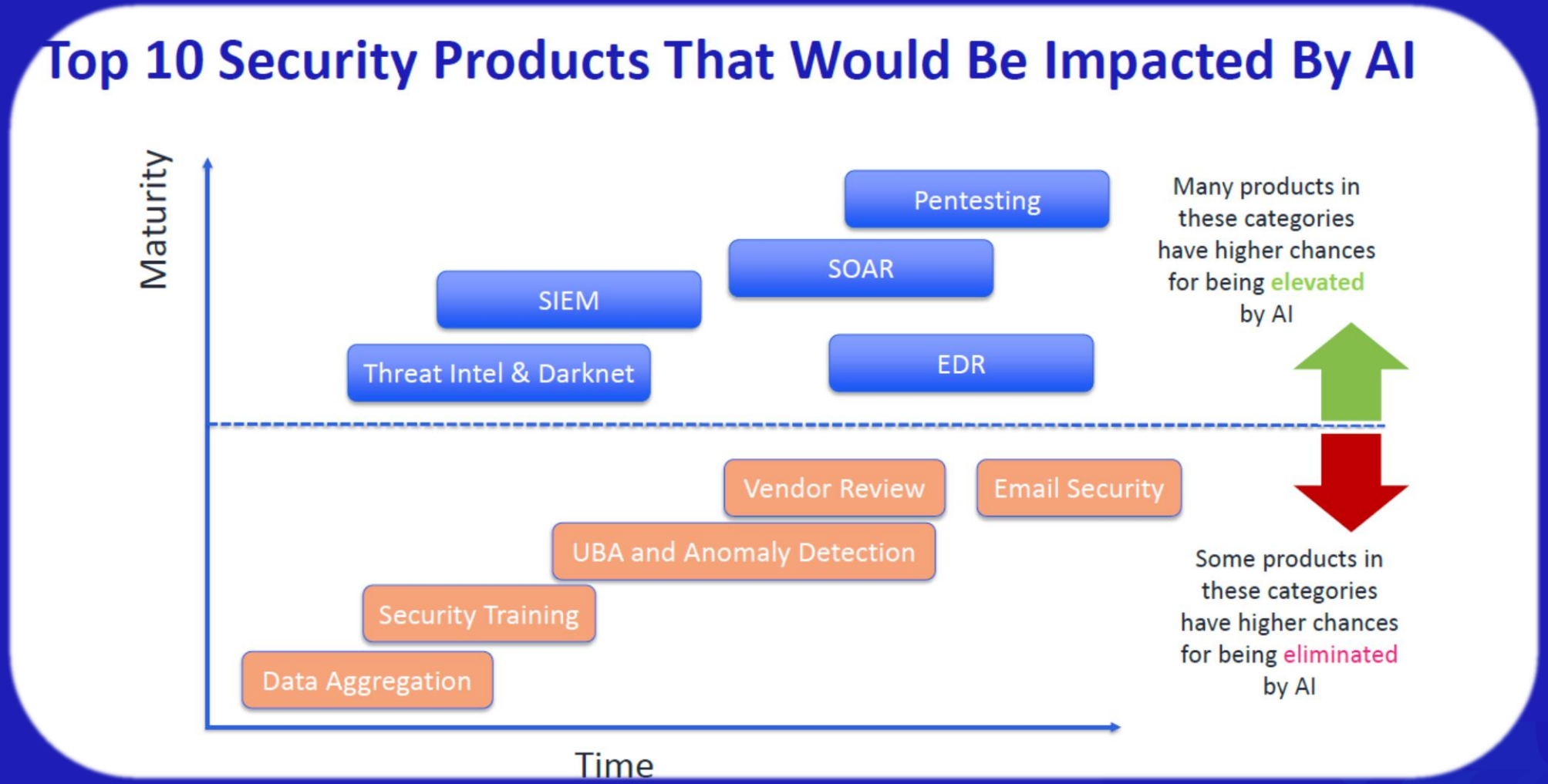
... One significant aspect is the elimination of project management tasks in cybersecurity, with estimates suggesting that 80% of these tasks could be eliminated

「サイバーセキュリティのプロジェクト管理業務が、2030年までに80%がAIによって廃止される可能性がある。」

perplexity

18-Mar-2024

Top 10 Security Products That Would Be Elevated or Eliminated by GenAI



Top 10 Security Products That Would Be Elevated or Eliminated by GenAI

Which Cybersecurity Products Will Be Eliminated By AI?

Top 10 Security Products That Would Be Elevated or Eliminated by GenAI

Nicholas Kakolowski
Senior Research Director,
IANS Research

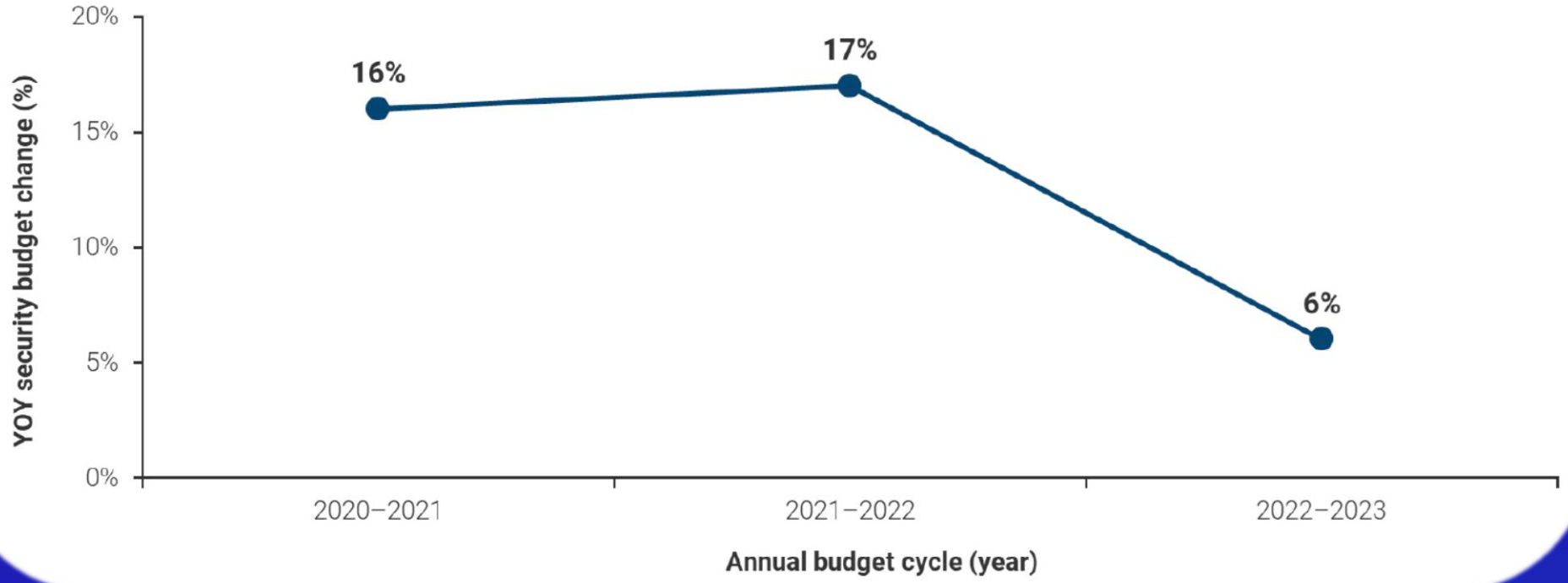
Steve Martano
Partner, Cybersecurity
Practice, Artico Search

State of the CISO 2024: Doing More With Less

Budgets are Tightening

Budget Growth Drops to a Third of Last Year's Overall Budget Change

Year-over-year change in the security budget

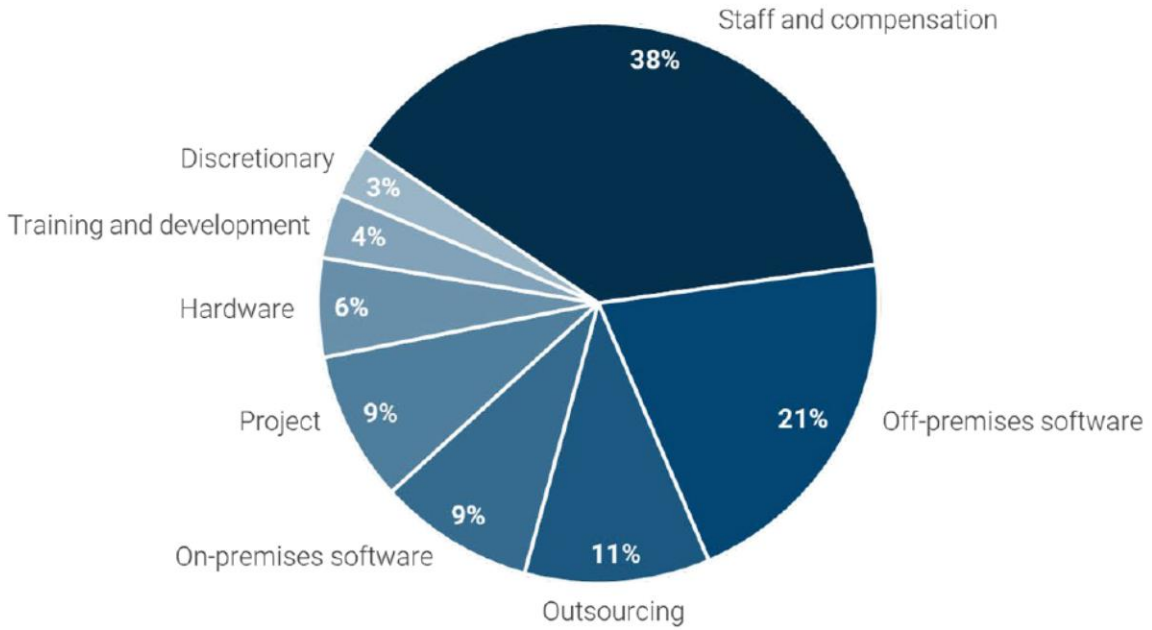


State of the CISO 2024: Doing More With Less

Infosec Spend Priorities

Staff and Compensation Claims the Largest Budget Share

Breakdown of the annual security budget

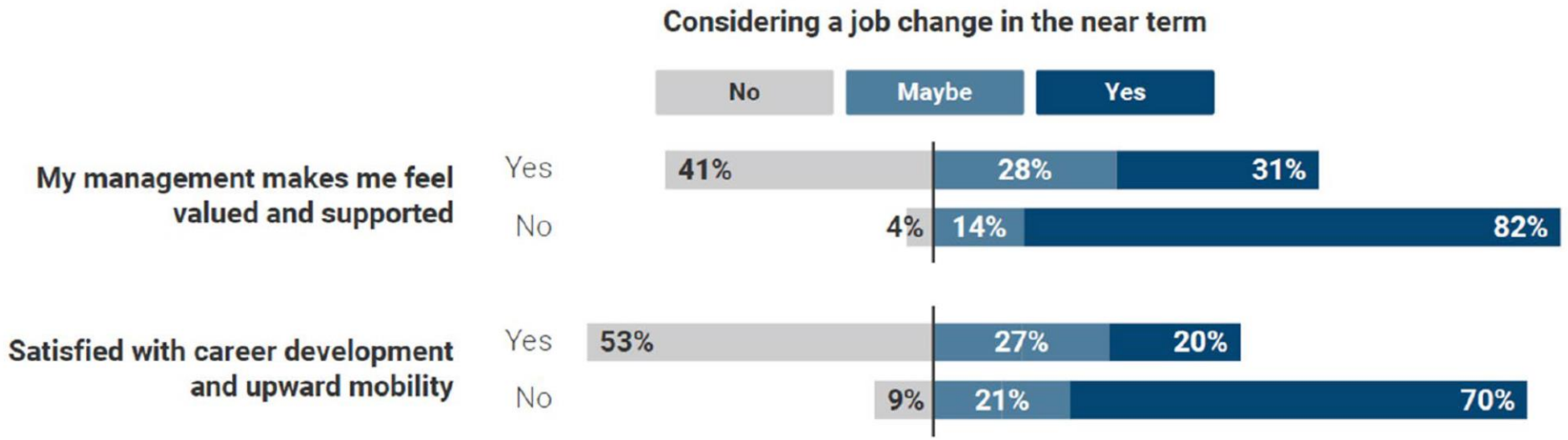


State of the CISO 2024: Doing More With Less

Creating a Sense of Progression Is Critical

Feeling Valued and Supported Coincides With Higher Staff Retention

Staff satisfaction levels vs. job-change considerations (%)



State of the CISO 2024: Doing More With Less

Ed Skoudis
President, SANS Technology Institute College

Heather Mahalik
DFIR Curriculum Lead, SANS Institute & Cellebrite

Terrence Williams
SANS Certified Instructor/Security Engineer II, SANS Institute and AWS

Stephen Sims
Offensive Operations Curriculum Lead and Fellow, SANS Institute

Johannes Ullrich
Dean of Research, SANS Technology Institute College

THE ART OF POSSIBLE

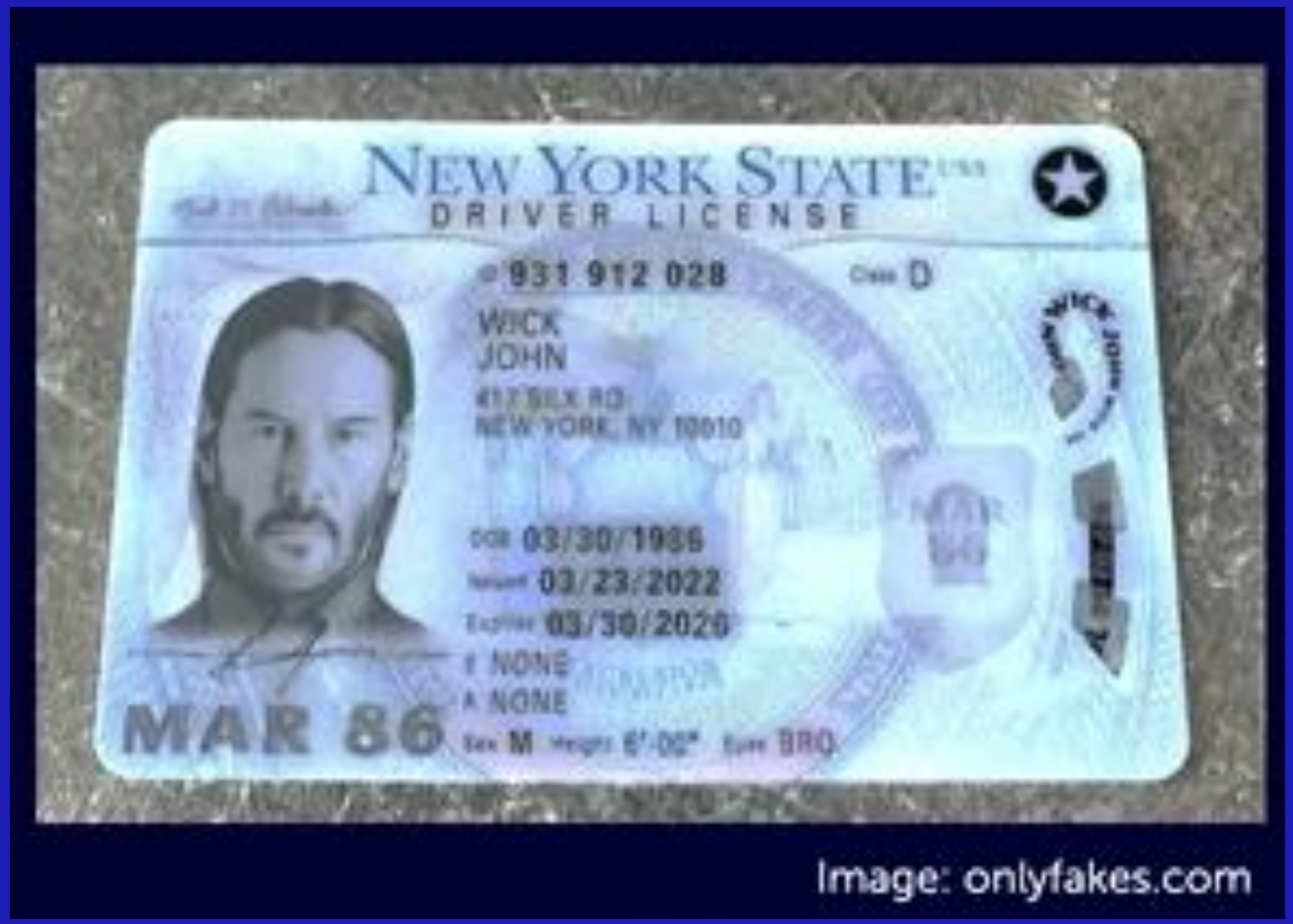
The Five Most Dangerous New Attack Techniques You Need to Know About

1. 技術的負債のセキュリティへの影響
2. AI時代の合成アイデンティティ
3. Sextortion
4. GenAI選挙の脅威
5. 脅威の乗数としての攻撃型AI

1．技術的負債のセキュリティへの影響

	Device 1	Device 2
Operating System	CentOS 6.4	FreeBSD 11.4
File Dates	December 2022	April 2024
Earliest Copyright	2002	1998
Perl	yes	Yes 5.30.2
Python	2.6 (3.6. installed by not used)	3.9.16
Java	OpenJDK 1.8.0	
PHP	-	8.0.16
Postgres	-	15.4

2．AI時代の合成アイデンティティ



引用：https://medium.com/@brilliantsocial/on-the-internet-nobody-knows-you-re-a-dog-d08981020cbb

3． Sextortion

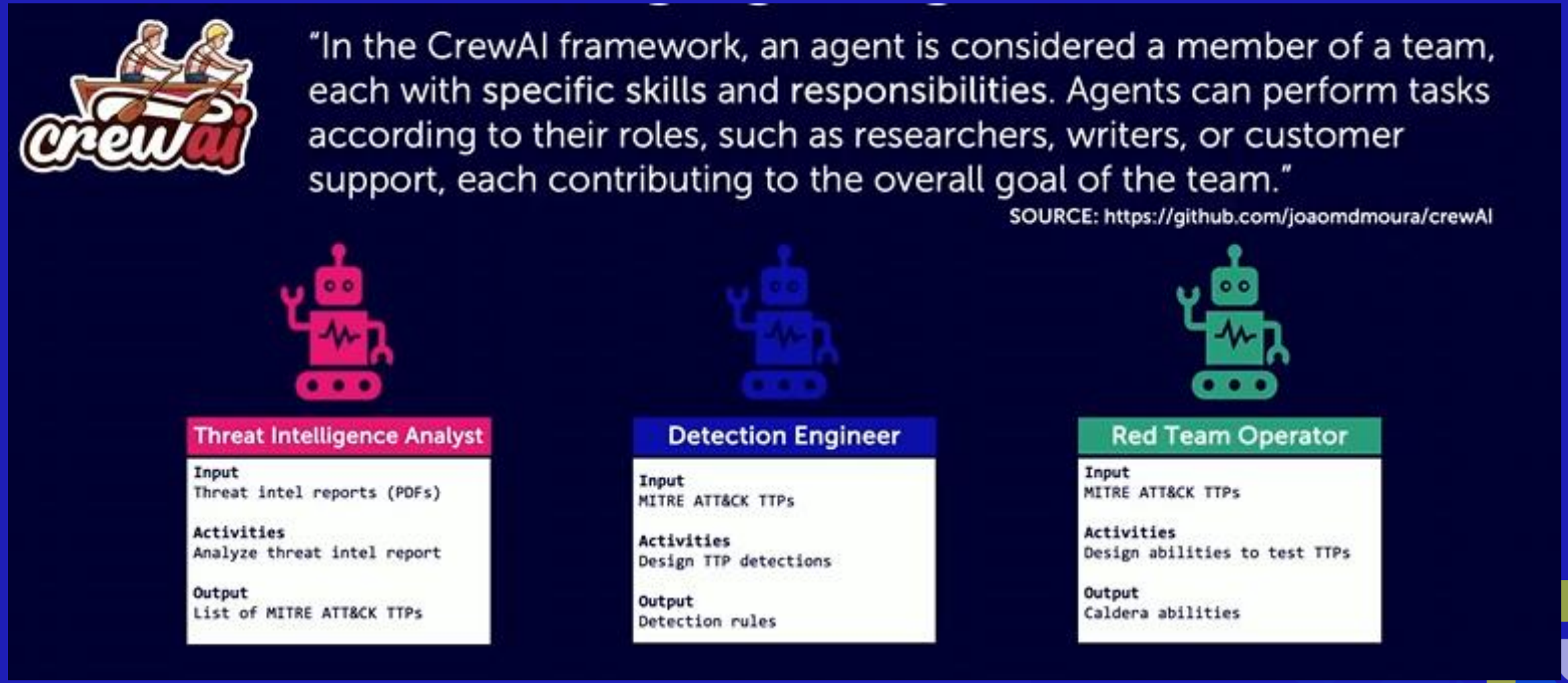
4．選挙におけるGenAIの脅威

The Power of Collaboration and Collective Action

Tech Accord	20+ leading tech companies committed to combating deceptive AI use in 2024 elections
OMB Memorandum M-24-10	Promoting AI collaboration and resource sharing across government
State-Level AI Bills	Transparency, accountability, and fairness
Collaboration	Governments, tech companies, and civil society

Image by DALL-E

5．脅威の乗数としての攻撃的AI



Agenda

- RSA Conference Viewing
- Sessions
- **Innovation Sandbox**
- Expo
- Networking
- Sum-up

Pi

新進気鋭のサイバーセキュリティ企業が画期的な技術を披露し、
「最も革新的な新興企業」のタイトルを競う名誉あるプラットフォーム。
過去のファイナリストはこれまで80件以上の買収を果たし、
135億ドルの投資を得た。
ファイナリストは、業界の審査員とライブ聴衆を前に、
3分間のピッチとそれに続く質疑応答セッションで自社の技術を披露する。

審査基準

- 解決する課題
- アイデアの独自性
- 技術・製品のインパクト
- チームメンバー
- 市場開拓状況

THE ART OF POSSIBLE

HIDDENLAYER
PROTECT YOUR ADVANTAGE

View of the Innovation Sandbox venue

View of the Innovation Sandbox venue

THE ART OF POSSIBLE

aembit
ワークロードID&
アクセスマネジメント

ANTIMATTER
機密データ制御

BEDROCK SECURITY
GenAI&Cloud
データセキュリティ

Dropzone AI
AI SOC アナリスト

harmonic
AI Posture Mgt

MITIGA
Cloud&SaaS
Detection&Response

POSECURITY
ACCESS IS OUR PRIORITY ZERO
人とマシンのクラウドIAM管理

RAD SECURITY
クラウドネイティブの
脅威検知と対応

Reality Defender
ディープフェイク検出/保護

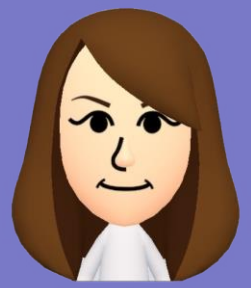
VulnCheck
次世代脆弱性管理

THE ART OF POSSIBLE

Predictions

Winner! ANTIMATTER

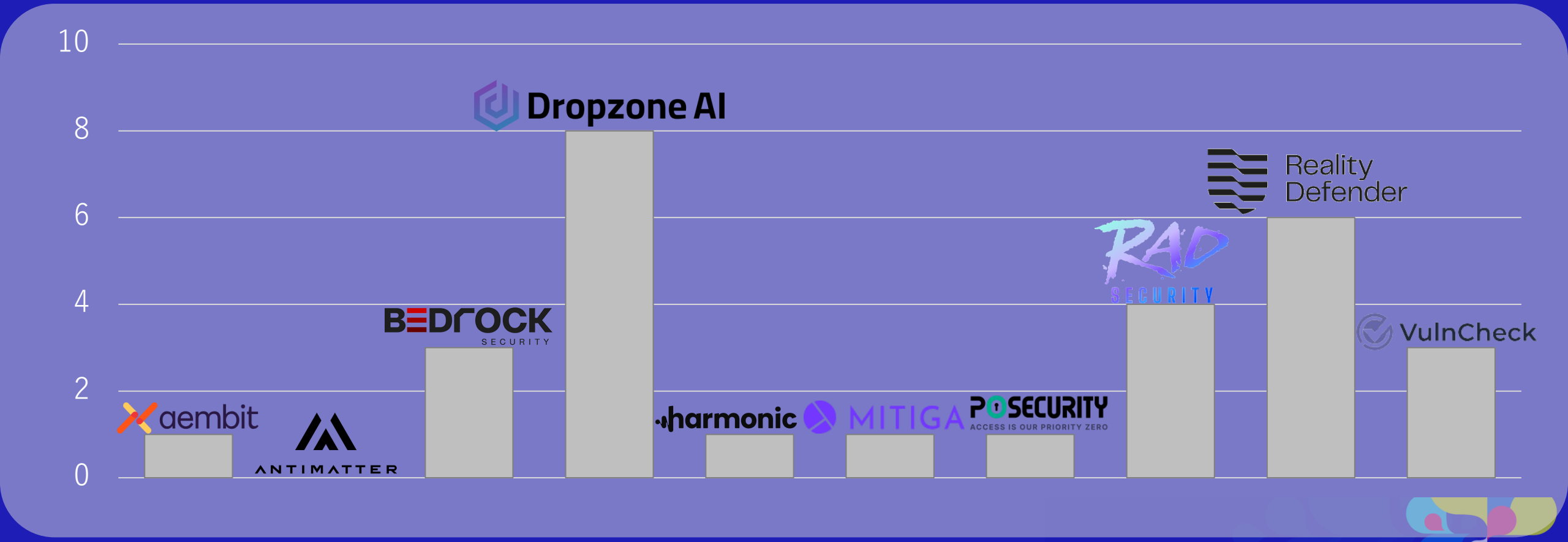
Runner up! aembit



Dropzone AI *Winner!*

VulnCheck *Runner up!*

Predictions by Webinar Participants
(Pre-announcement statistics)



Don’t know : 34

THE ART OF POSSIBLE

Prediction by Generative AI

Pi 「私が注目したファイナリストは、aembitだ。」

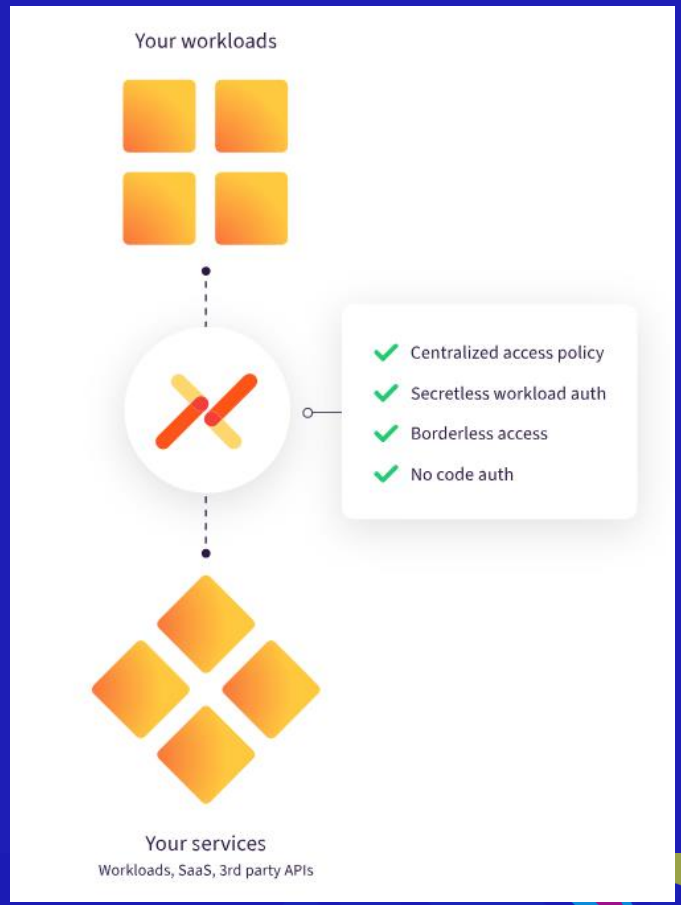
The winner is ・・・

THE ART OF POSSIBLE

The Award results

“It's one of the most consequential problems we face, especially in an election year. ...and it's a problem that we need to solve.”

THE ART OF POSSIBLE

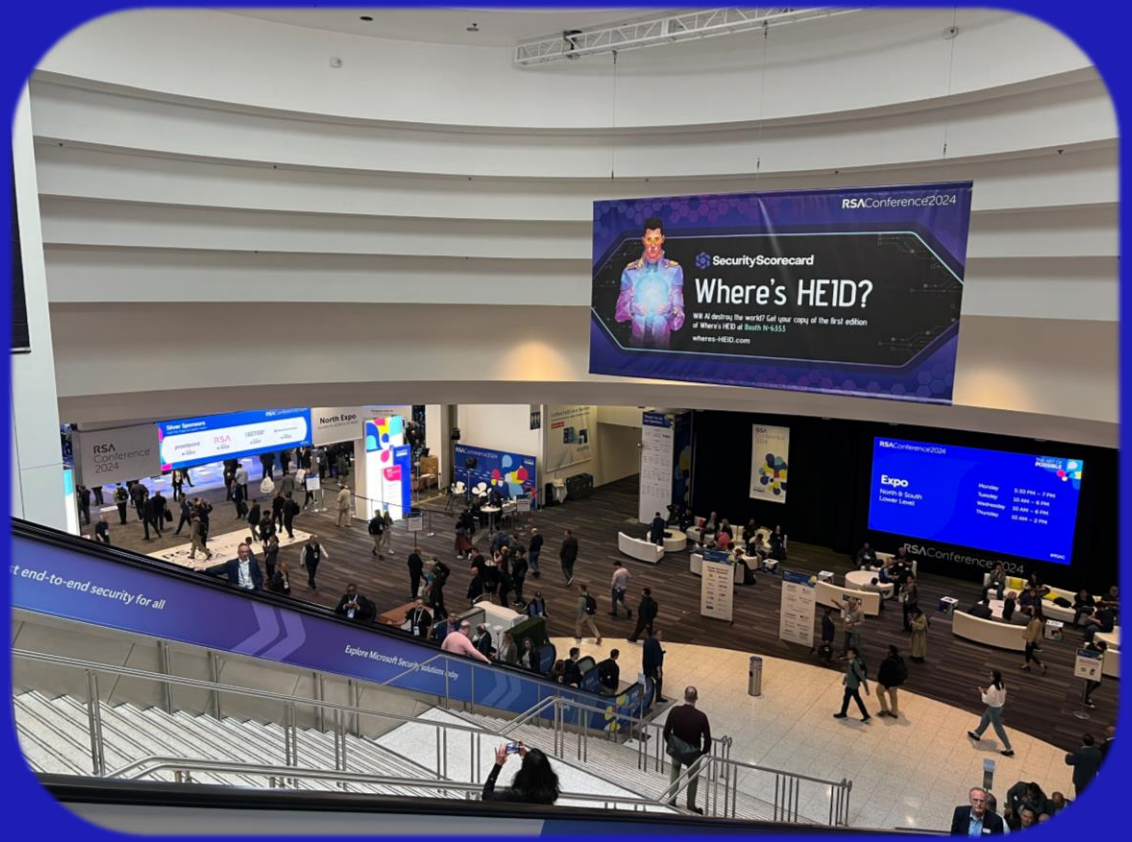


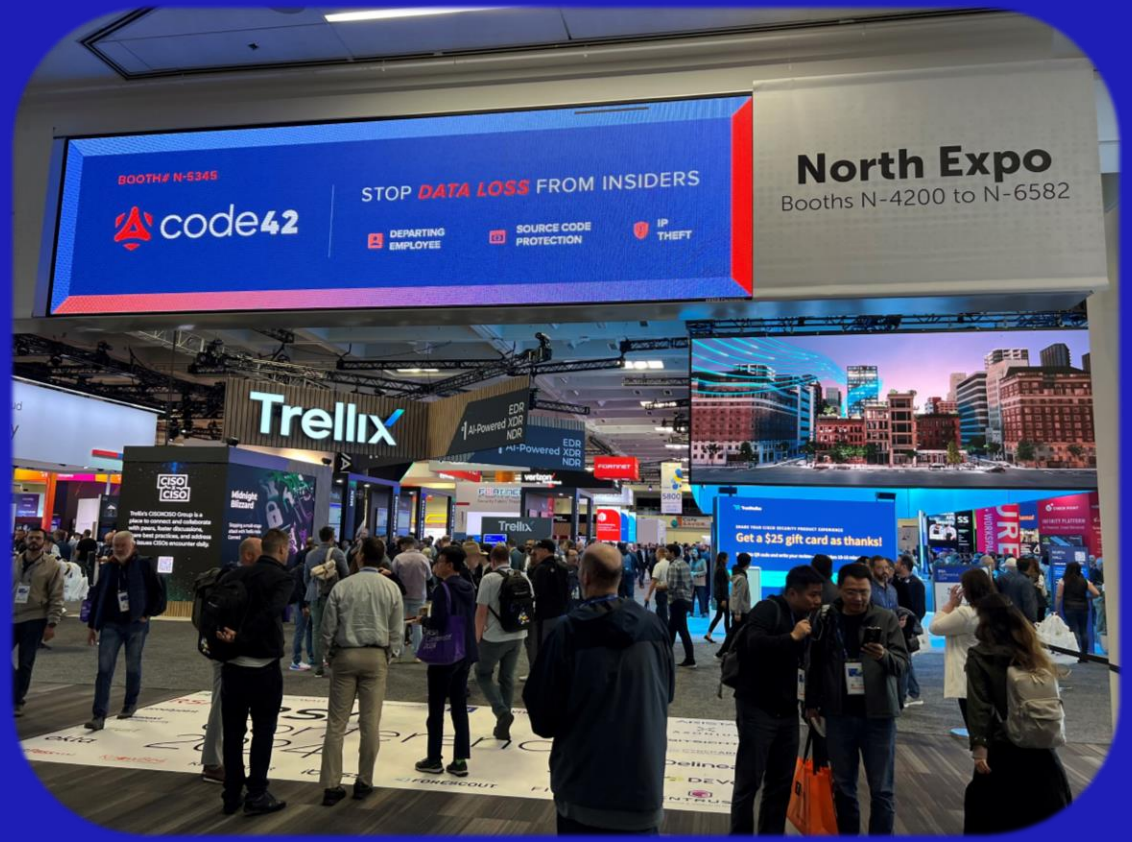
THE ART OF POSSIBLE

Agenda

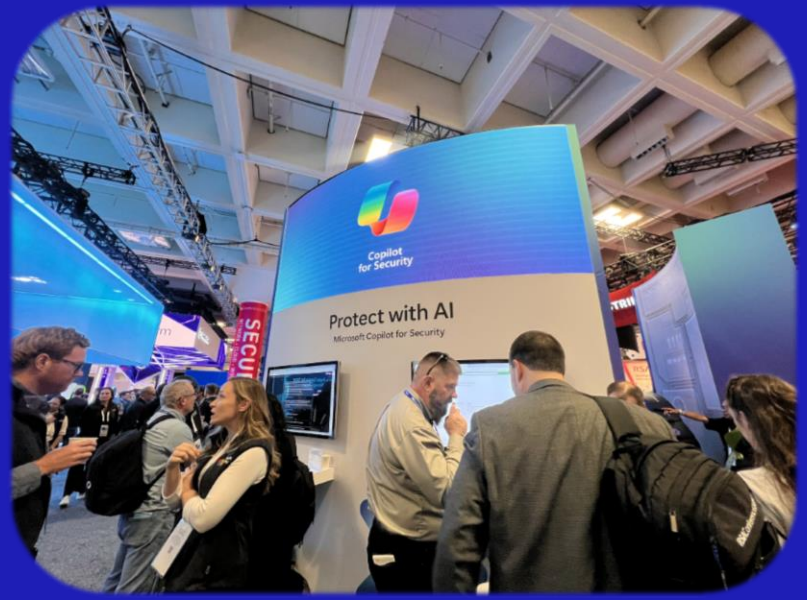
- RSA Conference Viewing
- Sessions
- Innovation Sandbox
- Expo
- Networking
- Sum-up


IdentityandAccessManagement
CloudSecurity
ApplicationSecurity
DataSecurity
ManagedSecurityServices
RiskManagementandCompliance
NetworkInfrastructureSecurity
SecurityOperationsandIncidentResponse
SecurityServices
ThreatIntelligence
DeviceSecurity
EndpointSecurity
FraudPreventionTransactionSecurity

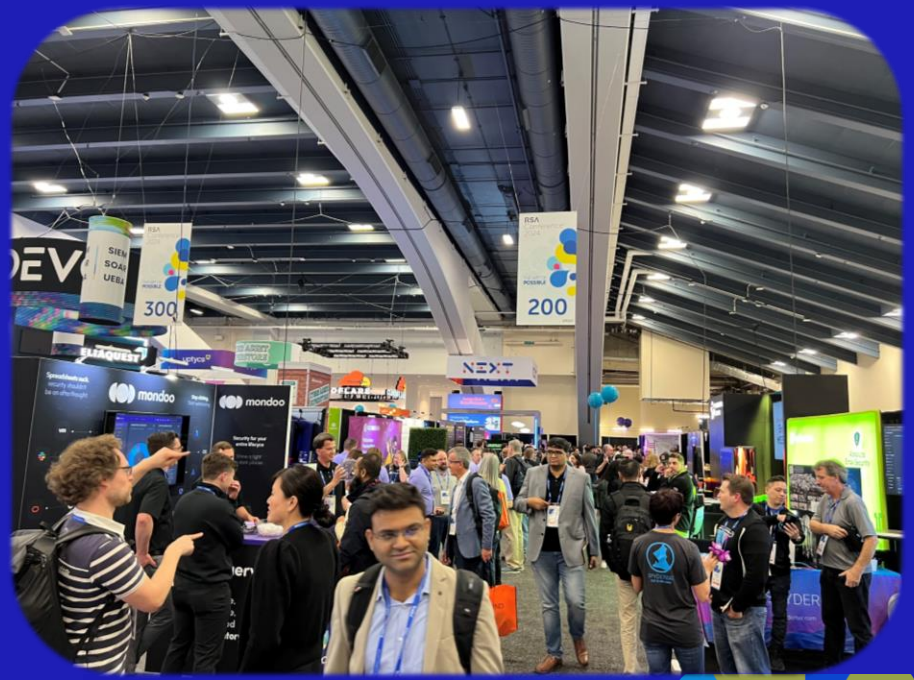




THE ART OF POSSIBLE



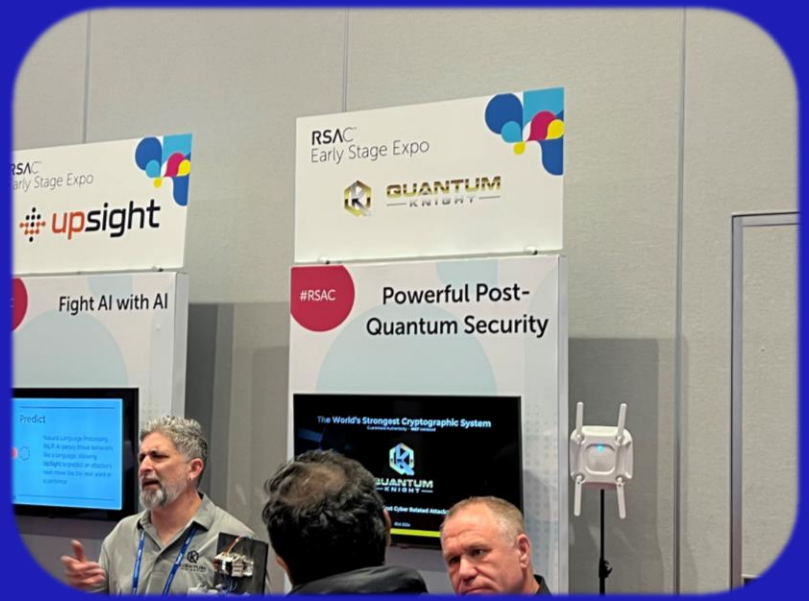
THE ART OF POSSIBLE



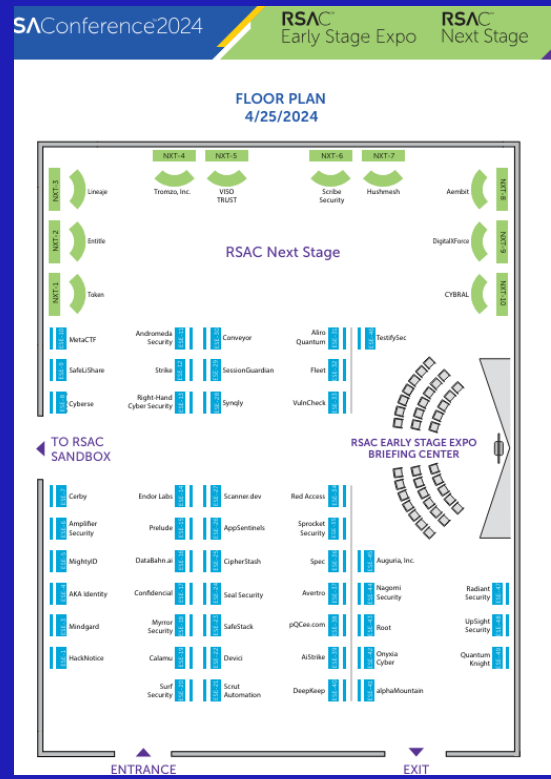
THE ART OF POSSIBLE

THE ART OF POSSIBLE

THE ART OF POSSIBLE

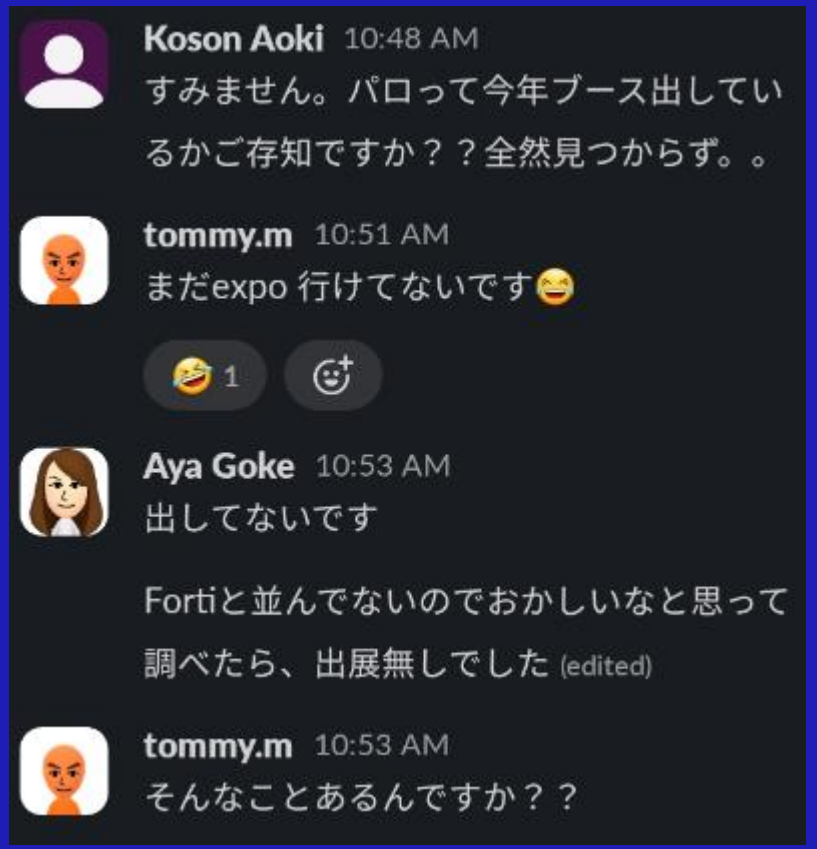


THE ART OF POSSIBLE

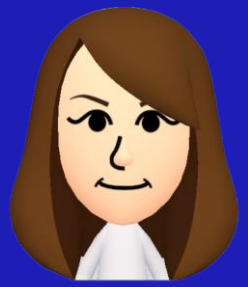


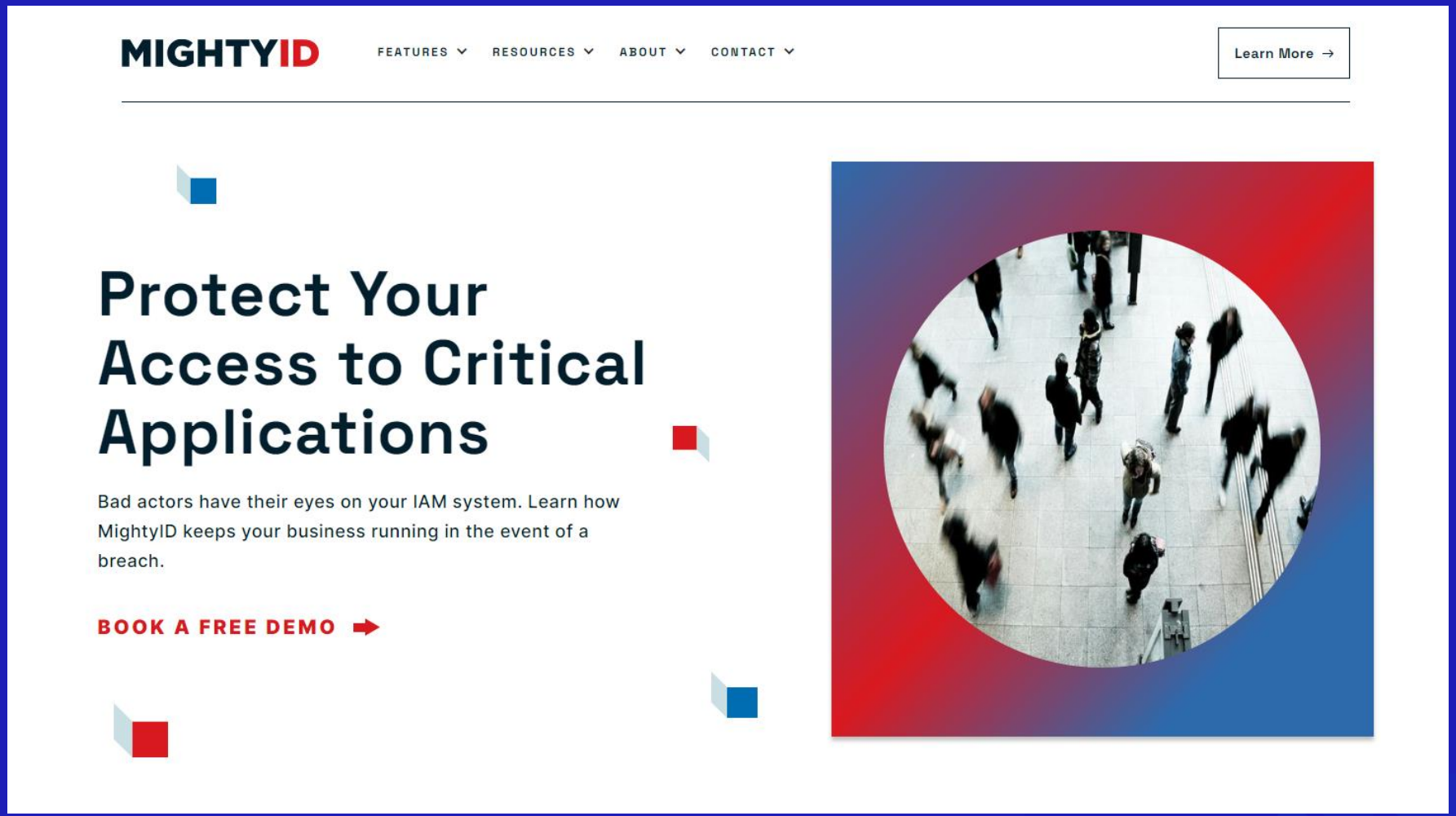
THE ART OF POSSIBLE

Where is Palo Alto Networks??

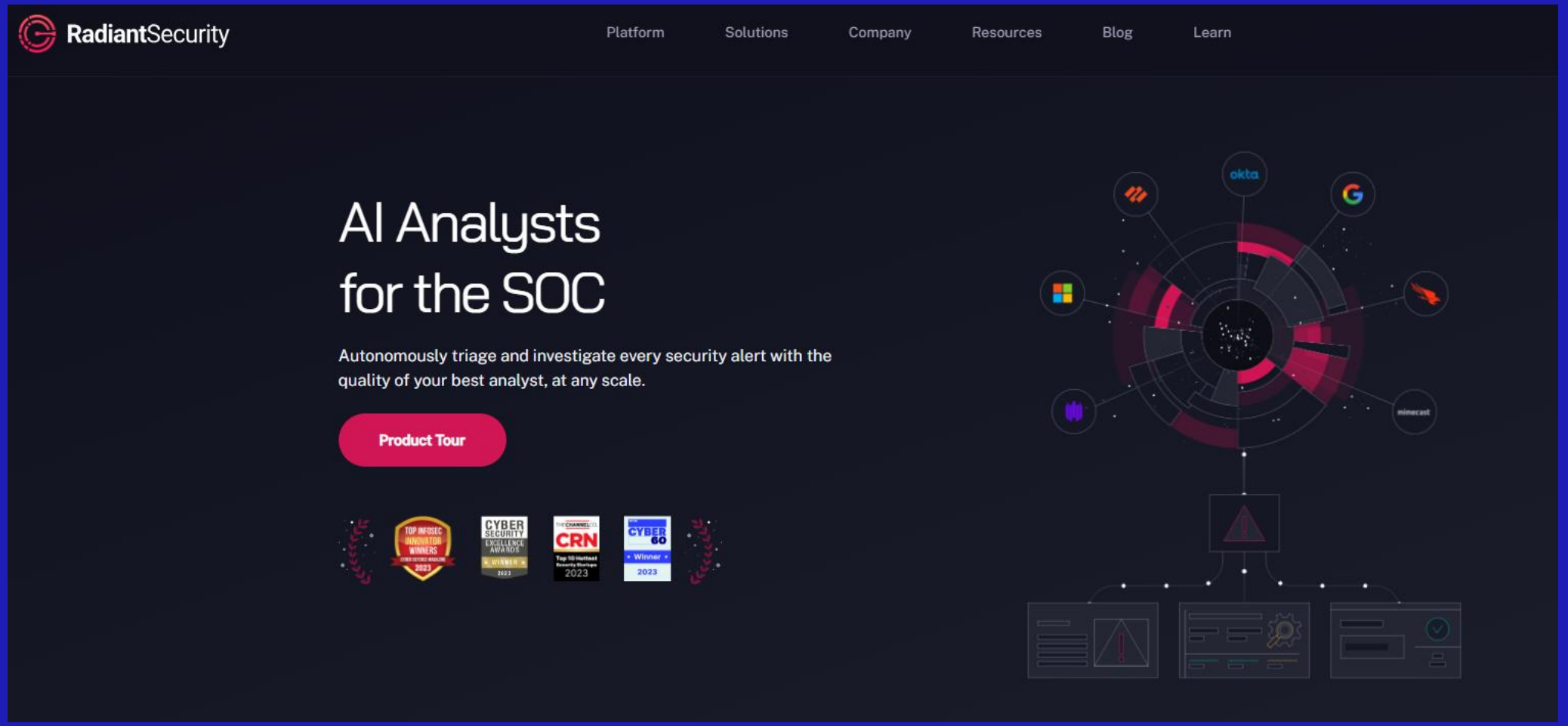


THE ART OF POSSIBLE




MIGHTYID
FEATURES
RESOURCES
ABOUT
CONTACT
Learn More →
Protect Your Access to Critical Applications
Bad actors have their eyes on your IAM system. Learn how MightyID keeps your business running in the event of a breach.
BOOK A FREE DEMO

Tommy's featured vendor



Agenda

- RSA Conference Viewing
- Sessions
- Innovation Sandbox
- Expo
- **Networking**
- Sum-up

Networking

THE ART OF POSSIBLE

DNX & Hitachi Solutions Security Event

THE ART OF POSSIBLE

Agenda

- RSA Conference Viewing
- Sessions
- Innovation Sandbox
- Expo
- Networking
- Sum-up

THE ART OF POSSIBLE

See you next year!

THE ART OF POSSIBLE

Survey Benefits

RSA Conference 2024

世界最大規模のセキュリティカンファレンス
1991年にたった1つのパネルディスカッションから始まる

2024年	
参加者	：41,000人以上
セッション数	：425セッション
出展企業数	：600社

THE ART OF POSSIBLE

The State of Venture Capital in Cybersecurity

Speaker:Dave DeWalt(NightDragon), Mark Hatfield(Ten Eleven Ventures), Yoav Leitersdorf(YL Ventures), Chenxi Wang(Rain Capital), Nadav Zafrir(Team 8)

概要:投資家による2023年振り返りと今後の展望

・2023年はセキュリティ分野への投資は大きく落ち込んだが、寧ろ2021、2022年がやや過大評価気味であり、プレゼンすれば誰でも出資を受けることが出来た。現在は妥当な評価に落ち着いていると見ている

・2023年はシード案件が多かった

・ベイエリアでは昨年から毎週木曜日にAIのミートアップが開催され活況である

・2023年から2024年に掛けてサイバーを専業とするファンド設立が増加している

・当たり前の話だが、投資家であっても良い投資先を探し当てるのは本当に困難

・AIを攻撃・防御双方から見た場合、2～3年は防御側に不均衡な状態が続くが、それ以降平準化されるだろう

・2023年上場企業にとって最大のニュースは米国証券取引委員会(SEC)の新たなサイバーセキュリティの開示規則

・投資家がスタートアップに投資をする際のポイント：投資家同士のコミュニティが最近は重要、オープンマインドで物事に取り組めるか、チームとして動けるか、ここぞという時にリスクテイクが出来るかetc.

・今後のブルーオーシャン：セキュリティガバナンス、アイデンティ、AI&3rdPatyRisk、
AIによるセキュリティオペレーション、保険、DLP、SIEM

Gartner's Top Predictions for Cybersecurity 2023-2024

Speaker:Leigh McMullen Distinguished VP, Analyst & Gartner Fellow, Gartner

概要:Gartnerのアナリストによる、今後3年間、2027年までの8つのセキュリティ動向予測

1. Privacy(2024) - 最新のプライバシー規制は顧客データの大半をカバーするが、プライバシーを競争上の優位性として武器化出来る組織は10%以下に留まる
2. Talent(2025) -サイバーセキュリティ・リーダーの半数近くが転職、内25%は全く別の職務に就く
3. Risk(2025) -サイバーセキュリティ・リーダーの50%は、企業の意思決定を促進するためにサイバーリスクの定量化を試みるが失敗する
4. Zero Trust(2026) -最も重要な資産のリスク軽減を優先して、ゼロトラストを実施する
5. Threat Landscape(2026) -脅威検知・調査・対応(TDIR)機能の60%以上が、検知された脅威の検証と優先順位付けのためにエクスポージャー管理データを活用
6. Board Governance(2026) -取締役会の70%にサイバーセキュリティの専門知識を持つメンバーが1人含まれる
7. Third Party(2027) -従業員の75%がIT部門以外の場所でスキル向上を目指す
8. Human Factor(2027) -大企業CISOの50%が、サイバーセキュリティに起因する摩擦を最小化し、人間中心のセキュリティ慣行を採用

How Large Language Models Are Reshaping the Cybersecurity Landscape

Speaker:Elie Bursztein Google & DeepMind AI Cybersecurity Technical And Research Lead, Google DeepMind

概要:Googleのエンジニアによる、AI-大規模言語モデル(LLM)の攻撃側・防御側でのユースケース

AIは攻撃側にも防御側双方にそれぞれメリットをもたらしている

攻撃側：フィッシングメールやフェイク動画を始めとした誤情報等、人間の心理の隙間を突いてくるソーシャルエンジニアリング分野に効果を発揮

ブラックマーケットでは、攻撃専用大規模言語モデルによるマルウェア生成、フィッシングメール作成、フィッシングサイト作成といったサービスが既に展開

防御側：主に4つ

詐欺等の誤った情報のコンテンツを教師なし学習で検知

文字と画像とを組み合わせたPDFマルウェアの検知

コードに内在する脆弱性の確認と自動パッチ適用

インシデント発生時のサマリーレポート作成、といったジャンルで効果を発揮

State of the CISO 2024: Doing More With Less

Speaker:Nicholas Kakolowski Senior Research Director, IANS Research / Steve Martano Partner, Cybersecurity Practice, Artico Search

概要:CISOの2024年時点における最新情報

・CISOに対する期待が技術的なリーダーシップの役割から、よりエグゼクティブの役割へと変化しているが、実際の肩書のCレベルに相当するのは20%程で、それ以外はVicePresidentやExecutiveに留まる

・取締役会に4半期事に報告作業をしているCISO程、取締役会の対応やセキュリティ予算要求に満足

・セキュリティ予算は一昨年度までは2桁の成長率で昨年度は景気後退の影響を受け1桁に留まる

・セキュリティの全体予算の内、人権費とクラウドセキュリティへの割当が半分以上。オンプレよりもクラウドの方がセキュリティ予算は増加傾向。人件費を抑える為の自動化ツールはそれを使いこなせるアナリストが不在

・人材の流動性が激しいアメリカでは、4年目で転職を考え始めるが7年在職すると長期在職傾向有り。「マネージャーが自分のことを価値があるとみなして協力的」、「上昇志向とかキャリア開発が満足している状態」であれば転職率が下がる為、CISOはコミュニケーションスキルが必須

Top 10 Security Products That Would Be Elevated or Eliminated by GenAI

Speaker:Teza Mukkavilli CISO, ChargePoint / Gopi Ramamoorthy Head of Security & GRC Engineering, Symmetry Systems

概要:AIの登場によりどのセキュリティ製品が無くなるのか、より効果を発揮するのかを考察

・AIがセキュリティ製品に与えるインパクト指標として、複雑性、意思決定、繰り返しのタスク、誤検知、24/365運用、大量のデータ処理、多言語を含む国際的サポート、ヒューマンエラーが挙げられる

・生成AI Perplexityによる予想→「サイバーセキュリティのプロジェクト管理業務が、2030年までに80%がAIによって廃止される可能性がある。」

・Speaker予想→データアグリゲーション、セキュリティトレーニング、ユーザーの振る舞い検知、アノマリー検知、ベンダー評価、Emailセキュリティ等が無くなり、脅威情報やSIEM、Pentesting、SOAR、EDRはAIによってより高機能化

・CISOコミュニティ予想→ベンダー評価、SOAR/Workflow、ユーザーの振る舞い検知、アノマリー検知、セキュリティトレーニングが無くなる

The Five Most Dangerous New Attack Techniques You Need to Know About

Speaker:Ed Skoudis President/ Heather Mahalik DFIR Curriculum Lead/ Terrence Williams/ Stephen Sims Offensive Operations Curriculum Lead/ Johannes Ullrich Dean of Research, SANS

概要:SANSのパネリストによって、現在と今後、意識すべき攻撃を5つピックアップしたパネルディスカッション

1) 技術的負債のセキュリティへの影響: 技術的負債は、時間が経ってから影響が現れる。Perlのように、利用や技術が減少、サプライチェーン複雑化により技術的負債の脅威ベクトルが増大→負債の精算をすべきとき。
2) AI時代の合成アイデンティティ: 品質ではなく”コスト”がAIのゲームチェンジャー。過去数万ドルかかっていたものが数ドルで作成できるようになり、攻撃への利用が容易に。偽造を見抜くため、本人確認の精度を上げると、intrusiveness（押しつけがましさ）が上がってしまう問題もある。→コスト、intrusiveness、セキュリティのバランスをとることが課題。
3) Sextortion: AIの画像生成技術向上により、写真や動画が本物でなくとも恐喝に使われうる。Facebookなどに掲載している写真をもとに、誰もが被害者となる可能性を持つ。FBIが注意を呼びかけている。
4) 選挙におけるGenAIの脅威と対策：GenAIによる選挙の脅威は、主要なプラットフォームすべてに存在する。選挙プロセスに対する信頼の低下や民主主義の基盤を脅かす。
5) 脅威の乗数としての攻撃的AI：自動化とAIにより、攻撃力/攻撃者が増加。これまでの攻撃者がより迅速に攻撃できるだけでなく、非技術的な攻撃者も、補助ツールによって脆弱性を迅速に見つけ、悪意のあるキャンペーンを素早く立ち上げ、実行できる。→今後はAIエージェントを活用し、人の関与がなくとも成立する自動的な対策の仕組みと環境を作っていく必要がある。

CSA AI Summit at RSAC - Building Trust in AI: Proactive Safeguards for Responsible GenAI Adoption

Speaker:Jim Reavis CEO, Cloud Security Alliance and Illena Armstrong, President of CSA

概要:Innovationと経済の関係からAIの重要性とAI利用促進のための5ステップを紹介

- McKinseyの予想 “GenAIが産業に与える年間インパクトは最大4兆4000億ドル”は妥当か？→妥当
  最大4兆4000億ドル＝日本円で660億円という高い予想。これに対して会場に「高すぎるか？」と挙手を募ったところ、あまり手は上がらず。会場全体で妥当と感じている雰囲気。
- なぜ妥当との意見になるのだろうか？→過去、テクノロジーによってGDPは大きな影響を受けたから。
  GDP曲線において、電気やモーター、電子機器、コンピューターなどのInnovation後、GDPが大きく増加した。AIも大きな影響を与えると考えられている。
- AI利用促進のための5ステップ
  Step1：シャドウAIの発見ー環境全体（パブリック/プライベートクラウド、SaaSアプリ等）からAIモデル/エージェントを検出し、カタログ化する。
  Step2：アセスメントー発見したAIモデル/エージェントを評価する方法を用意し、リスクや利用状況、規制対応を数値化。
  Step3：データ＆AIのマッピングーAIが主に利用する非構造化データのセキュリティ、権利、サニタイズ、リネージが重要。
  Step4：データ＆AIのコントロール：理解したデータ内容に基づき、許可されていないユーザーへの提供をブロックするとる。
  Step5：データ＆AIのマッピング：データとAIモデル、データ利用における大きな影響を理解する。

The Time is Now: Redefining Security in the Age of AI

Speaker:Jeetu Patel Executive Vice President and General Manager, Security and Collaboration, Cisco, Tom Gillis Senior Vice President and General Manager, Security , Cisco

概要:サイバーセキュリティにおける劇的な変化とセキュリティ業界に必要な変化

- AIは、人/ITに変化もたらす。AIは人の能力増強に有効。AIを用いたデジタルワーカーが20人の開発者を100人に拡張したり、40人のカスタマーサービスを250人に拡張したり、社員が8～10人のアシスタントをもつ働き方への変化していく。
- AI利用の拡大は、膨大なデータや処理を生む。
- 膨大なデータ処理は、データセンター/アプリケーション/インフラの在り方を変える。
- 3つの新しい技術は、セキュリティ課題にも変化をもたらす。
  技術①AI：攻撃者はAIを武器として利用。防御者もAIをネイティブに利用するようになる。
  技術②カーネルレベルの可視化：エンドポイントが侵害され、エンドツーエンドで暗号化された場合、 侵害を検知できる。
  技術③ハードウェアアクセラレーション：セキュリティスループットや入出力、暗号化をGPUやDPUで高速化できる。
- セキュリティ業界の変化→AIによる変化を受けて、セキュリティ業界もAIを用いて変わる必要性に迫られている
- 人の介在不要で学習するツール：セグメンテーションの難しさは、アプリケーション動作のベースライン理解の難しさから生じる。ベースライン理解には、90日は必要だが、その後も大きなイベント発生により変化する可能性がある。AIとカーネル可視化により、人の介在なしに、詳細な理解と継続的な学習をツールが提供可能となる。
- 自動化されたセグメンテーション/アップグレード：ファイアウォールは常に大量の処理を行っているため、アップグレードの機会は少ない。この機会を逃すと、未更新の状態が長く続くことになるが、この作業をAIで自動更新できるようになるのではないか。

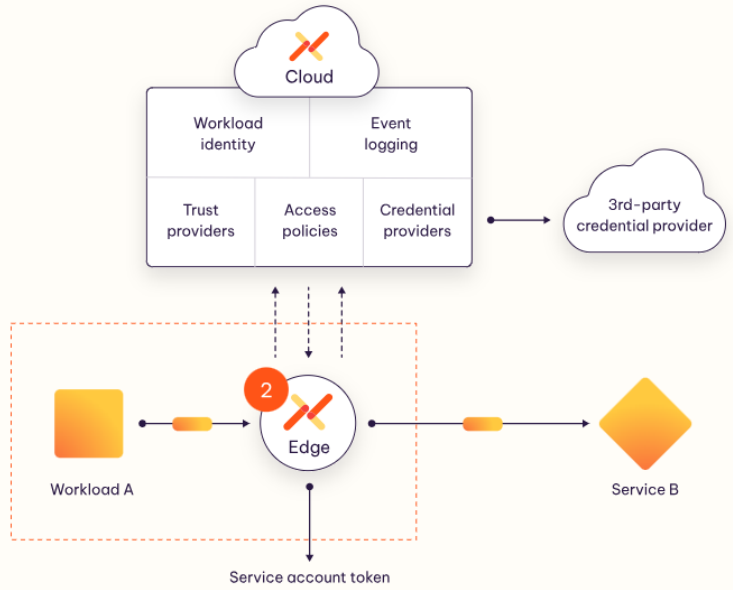
aembit

ワークロード・アイデンティティ・アクセス管理プラットフォーム

- クラウド、SaaS、データセンターにわたるワークロード （ソフトウェアアプリケーションやサービス） 間のアクセスに関するポリシーを作成し、ポリシーに基づいてワークロードのアクセスを管理。
- ワークロードのアクセスをセキュアにするとともに、管理口数を削減する。
- 100以上のテクノロジーと統合。

拠点	Silver Spring, MD
設立	2021
調達額	$ 18.04M
評価額	$ 40.39M /Seed
CEO	David Goldschlag
VC	Ballistic Ventures (California), CrowdStrike, Okta Ventures, Ten Eleven Ventures

1. Client workload makes request to service
2. Aembit Edge intercepts client request
3. Aembit Edge retrieves service account token
4. Aembit Edge requests access credential on behalf of client
5. Aembit Cloud authenticates client using attestation
6. Aembit Cloud checks authorization policy & conditional access requirements
7. Aembit Cloud requests access credential from provider
8. Client workload makes request to service
9. Aembit Edge injects credential into client request and forwards it
10. Aembit Edge send access event log to Aembit Cloud



Works Seamlessly with Your Tech Stack

Aembit integrates with 100+ of your favorite technologies.

snowflake apigee Confluence GitGuardian ATLASSIAN Google Cloud

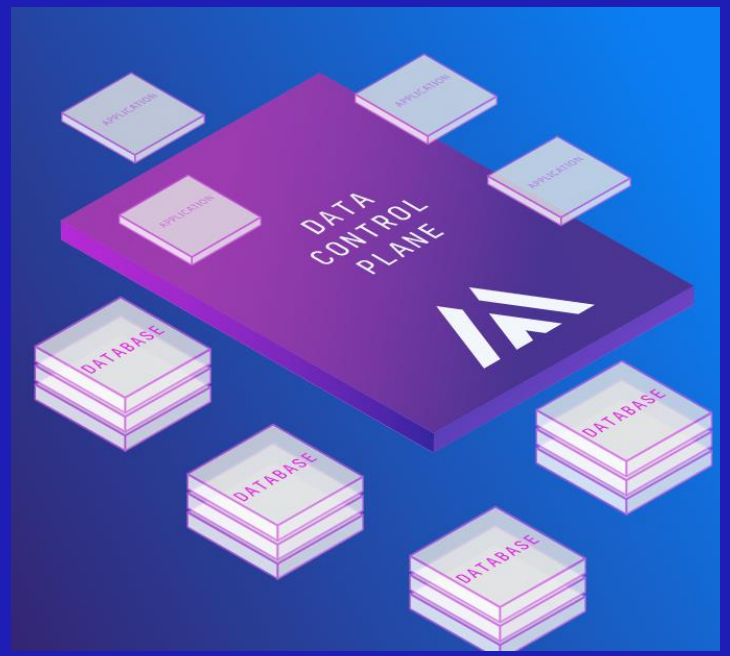
GitLab stripe slack OpenID MySQL

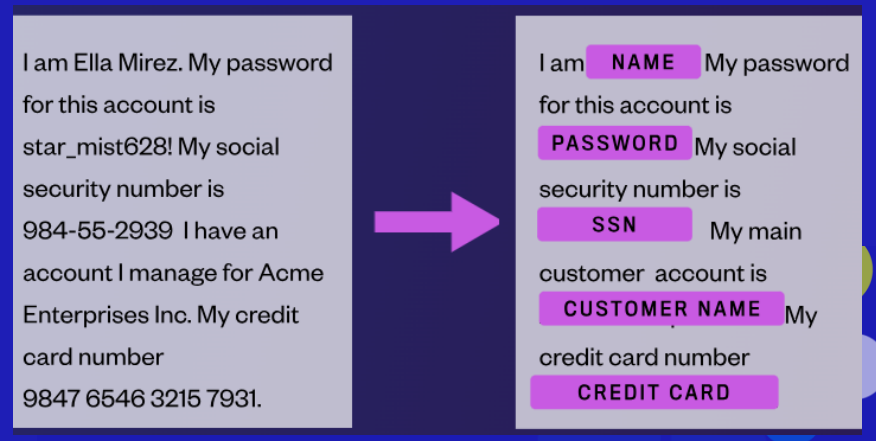
ANTIMATTER

機密データプラットフォーム

- あらゆるデータストアGとenAIを含むアプリケーションにおいて、データの匿名化、ログ記録、暗号化、アクセス制御を行う。
- 提供する機能
  ①AIやMLで使用するデータをユーザー情報に基づいて制御。
  ②クラウド上のデータ分類とアクセス制御。
  ③SaaSで利用するデータの暗号化。

拠点	Oakland, CA
設立	2020
調達額	$ 11.99M
評価額	$ 56.99M /Series A
CEO	Andrew Krioukov
VC	General Catalyst, New Enterprise Associates, UNION Labs VC



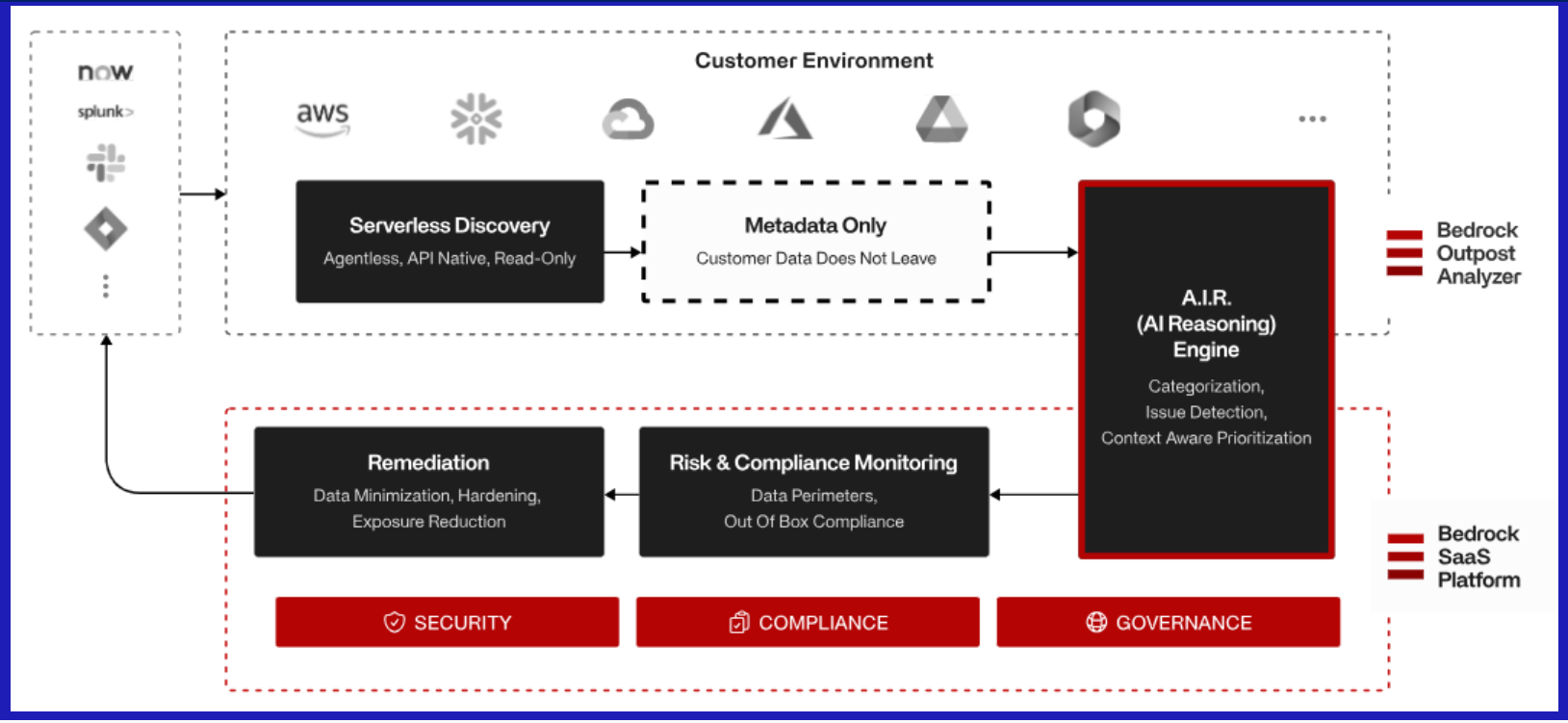


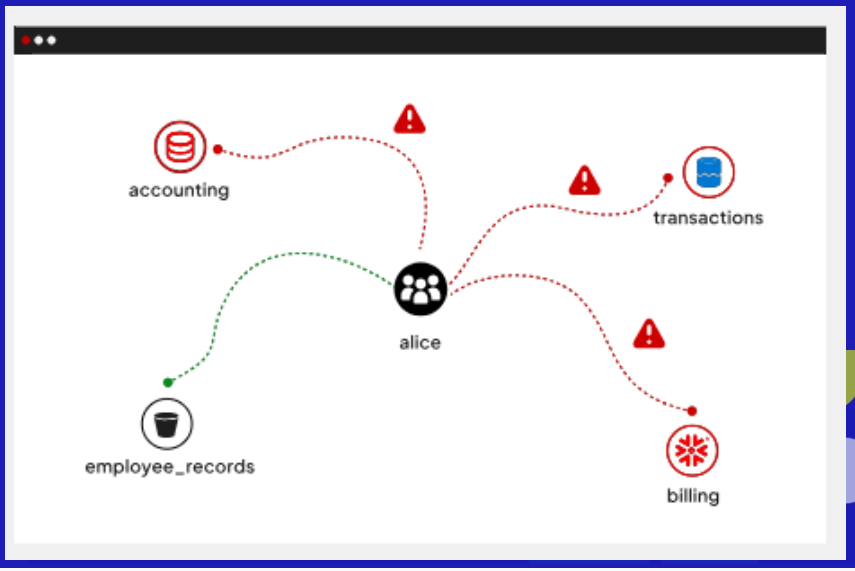
BEDROCK SECURITY

データセキュリティプラットフォーム

- AI Reasoning Engineで、顧客環境のメタデータからデータを発見/分類し、ルールに依存しないリスク評価＆コンプライアンス・モニタリングを実施。
- サーバーレスで、顧客環境の既存APIを使用して、構造化/非構造化データセットを検出。
- 正確なリスク評価とワンクリックでの修復を提供する。

拠点	Menlo Park, CA
設立	2021
調達額	$ 20.00M
評価額	$ 25.00M /Early Stage
CEO	Pranava Adduri
VC	Greylock



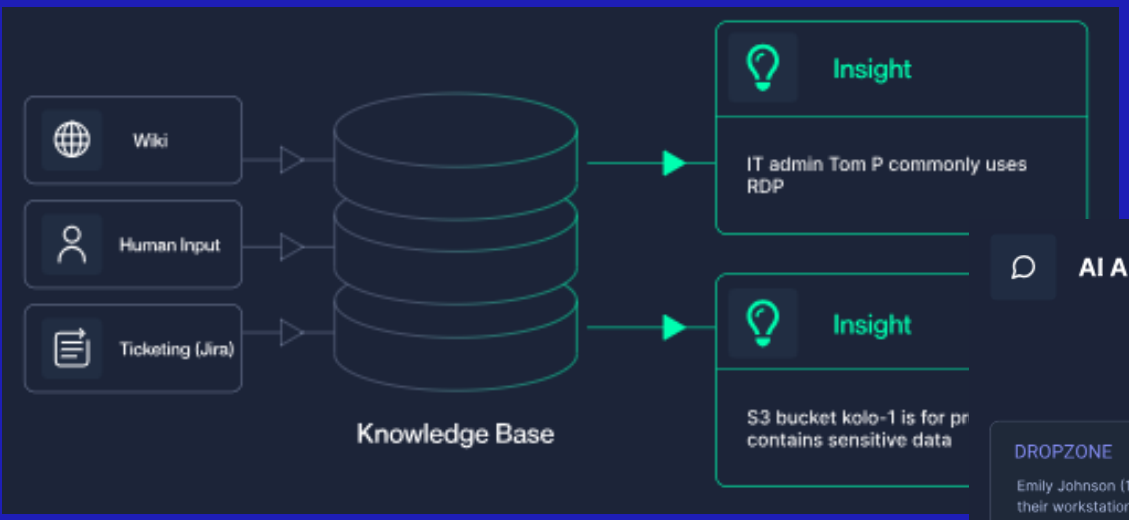


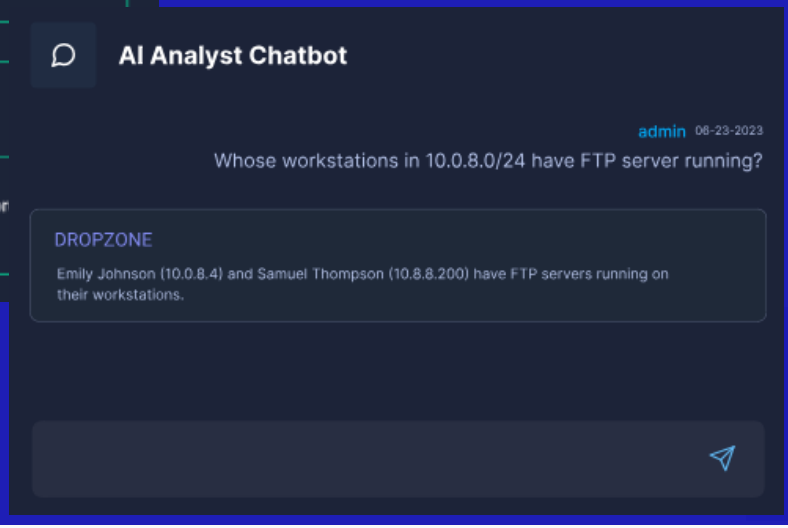
Dropzone AI

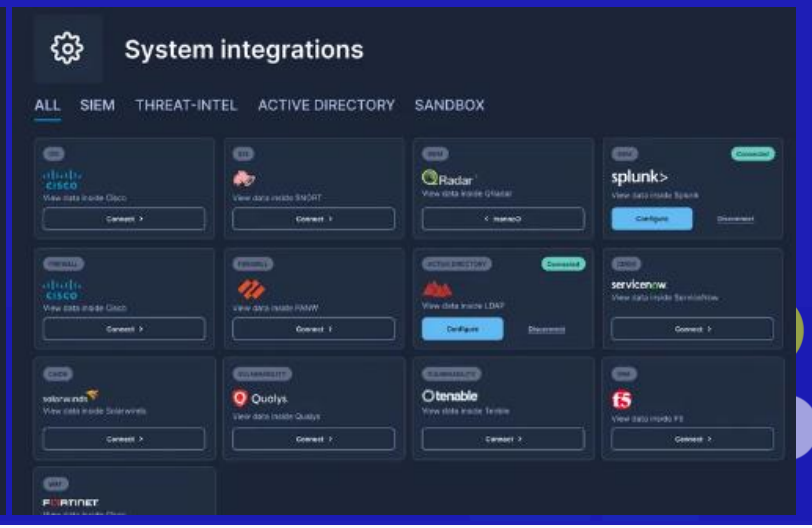
AI SOC アナリスト

- 既存のセキュリティツール（SIEM、EDR、ファイアウォール、CSPなど）と統合し、セキュリティアラートを 24時間365日 自律的に調査。
- システムから組織のコンテキストを自動抽出し、意思決定のためのレポートを生成。
- 特定のアラートや質問を調査するためのチャットボットを提供。
- アラート調査を100％カバーし、迅速かつ正確なセキュリティ対応に貢献する。

拠点	Seattle, WA
設立	2023
調達額	$ 3.39M
評価額	$ 13.59M /Seed
CEO	Edward Wu
VC	Decibel Partners, In-Q-Tel, Jesse Rothstein, Jon Oberheide, Oliver Friedrichs, PSL Ventures





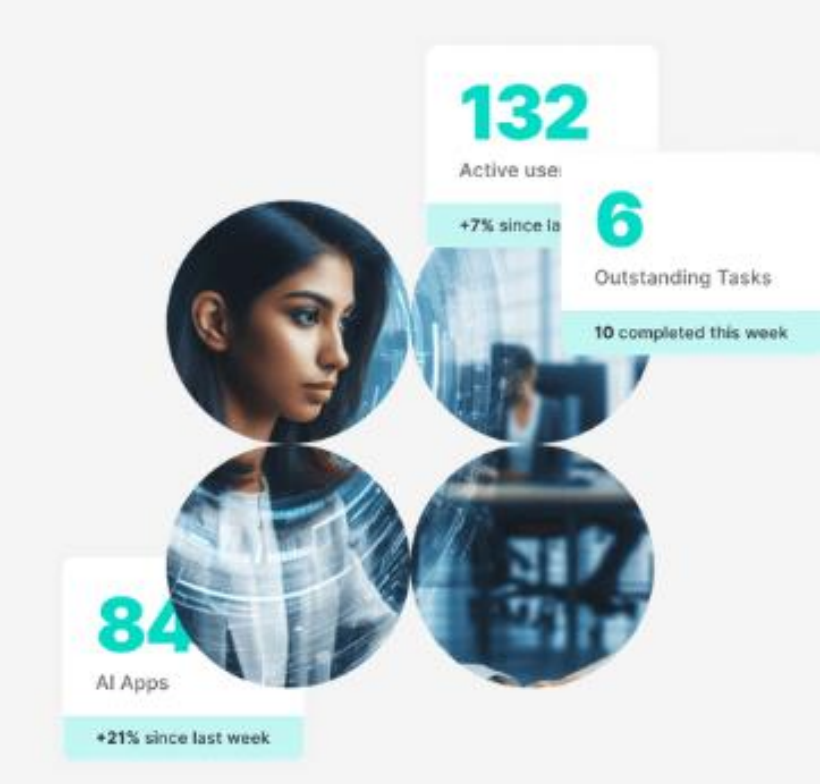


harmonic

Generative AIセキュリティプラットフォーム

- 企業内のGenAI採用状況を可視化し、シャドーAIの発見、AIアプリケーションのリスクアセスメント/コンプライアンス/セキュリティを提供。
- 独自のデータ保護LLMは、センシティブなデータの理解と検出に強みをもち、データセキュリティやプライバシーに貢献する。

拠点	San Francisco, CA
設立	2023
調達額	$ 8.46M
評価額	$ NA /Seed
CEO	Alastair Paterson
VC	Daniel Bernard, Eileen Burbidge, Jerry Perullo, Nicholas Warner, Sequoia Capital, Storm Ventures, Ten Eleven Ventures



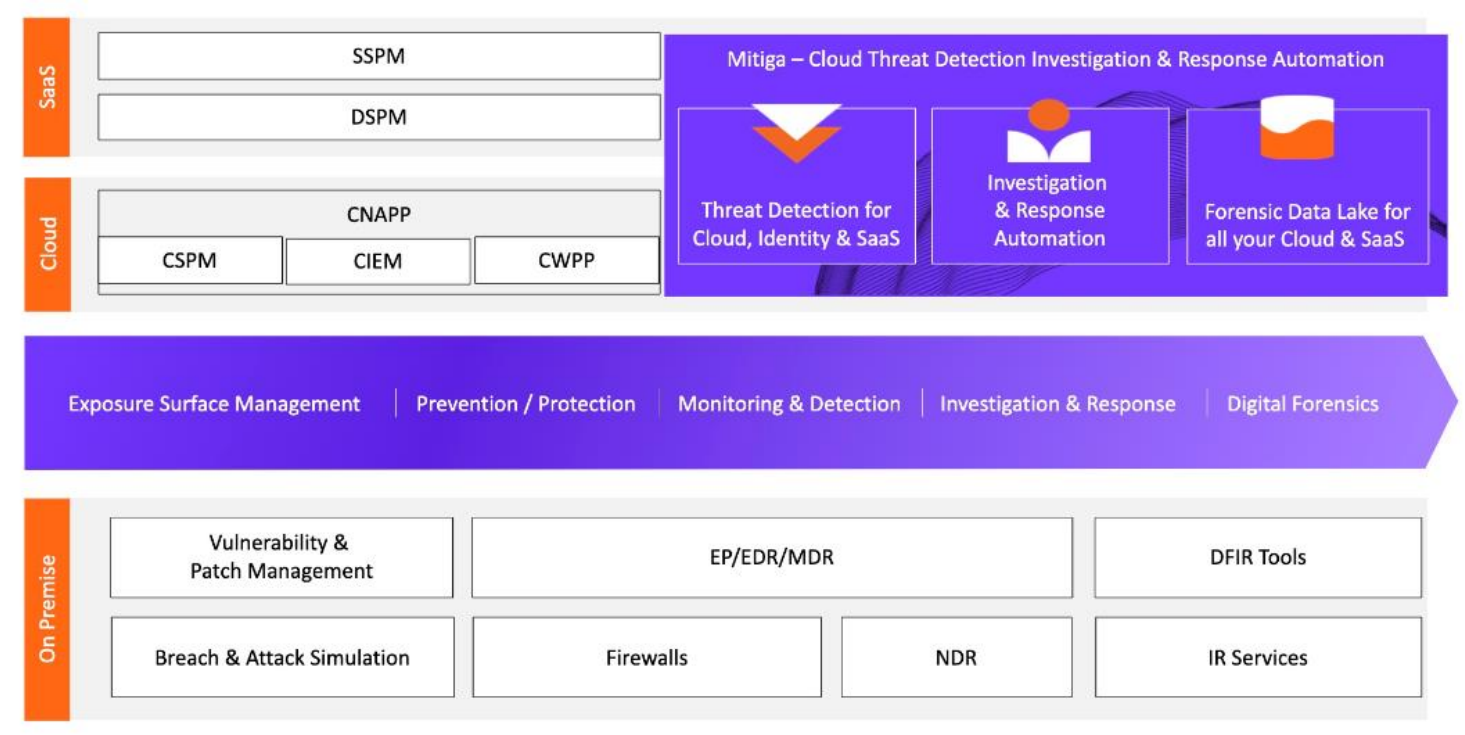
THE ART OF POSSIBLE

MITIGA

SOC強化プラットフォーム

- SaaSおよびクラウド脅威の検出、調査、および対応を実施。
- 最大1,000日分のフォレンジックデータをエンリッチおよび相関させる
  クラウドセキュリティデータレイクをプロアクティブに作成し、
  そのデータを使用して顧客環境の脅威を検出。
- クラウド侵害に備えるためのツール不足を補う。

拠点	Tel Aviv, Israel
設立	2019
調達額	$ 52.2M
評価額	$ 145.00M /Early Stage
CEO	Ariel Parnes
VC	Ari Buchler, Atlantic Bridge Capital, Blackstone, Cisco Investments, ClearSky, DNX Ventures, Direct Round, Ferocity Capital, Flint Capital, Glilot Capital Partners, Julian Levy, Key Capital (Switzerland), Rain Capital, Samsung NEXT Ventures



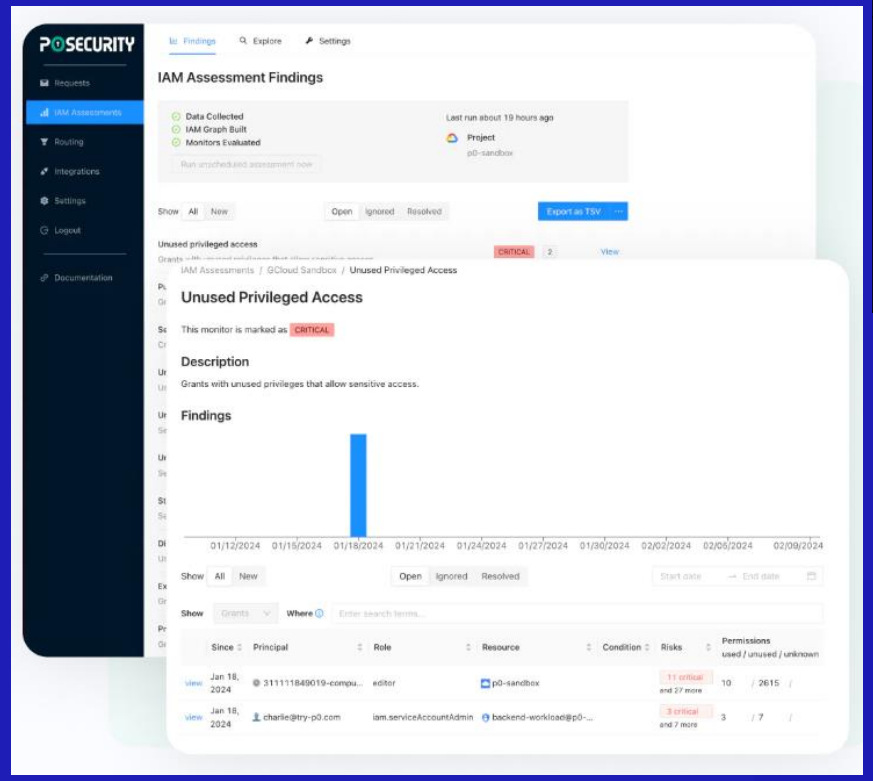
THE ART OF POSSIBLE

P0SECURITY
ACCESS IS OUR PRIORITY ZERO

クラウド・アクセス・ガバナンス・プラットフォーム

- 人やマシンなどのID インベントリを作成し、リスク態勢を評価。
- アクセスライフサイクルを管理し、アクセスエスカレーションを自動化。
- ユーザーがリソースにアクセスするのにかかる時間を短縮し、IAM攻撃対象領域を削減する。

拠点	Doral, FL
設立	2018
調達額	$ 17.50M
評価額	$ 22.80M /Early Stage
CEO	Ricardo Villadiego
VC	Bossanova Investimentos, Forgepoint Capital, KnowBe4 Ventures, SoftBank Investment Advisers, Alibaba Capital Partners

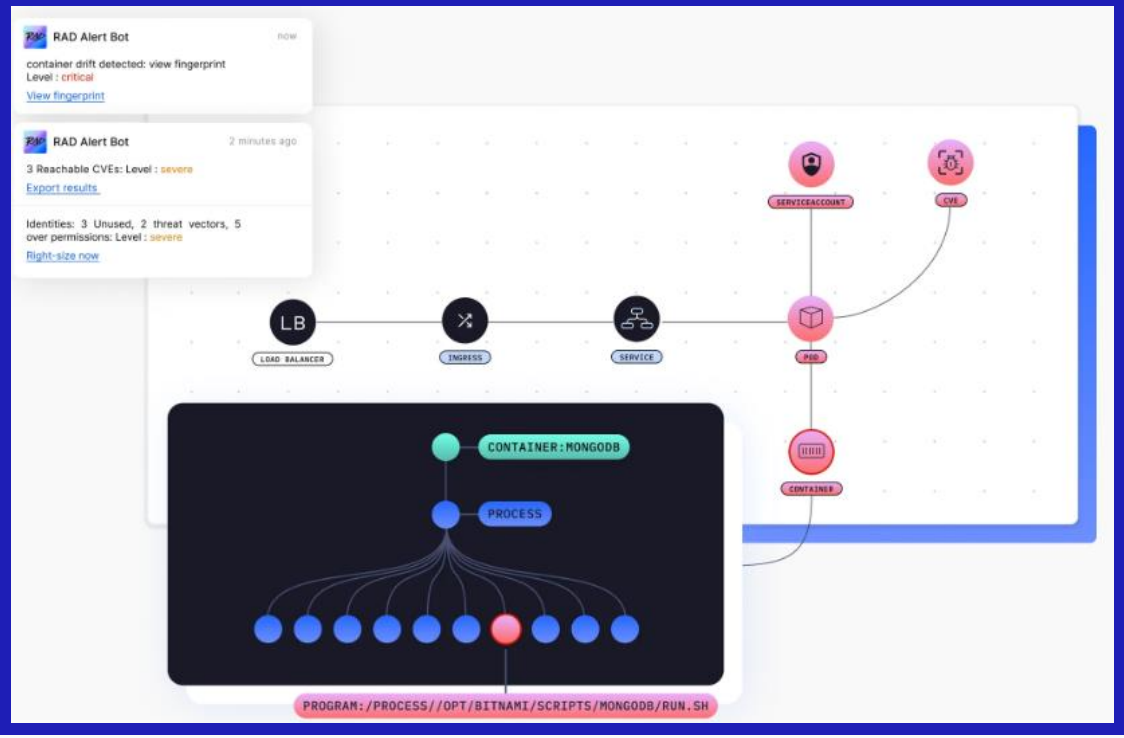


THE ART OF POSSIBLE

クラウドネイティブの脅威検知と対応プラットフォーム

- ソフトウェアサプライチェーン、クラウドネイティブインフラ、ワークロード、アイデンティティ全体にわたるユーザー固有の適切な行動の行動のフィンガープリントを作成。
- フィンガープリントをもとにゼロデイ攻撃を検出し、シフトレフトと態勢管理を強化する。

拠点	San Francisco, CA
設立	2021
調達額	$ 5.06M
評価額	$ NA /Seed
CEO	Brooke Motta
VC	.406 Ventures, Aviso Ventures, Forgepoint Capital, Gula Tech Adventures, Vertex Ventures US

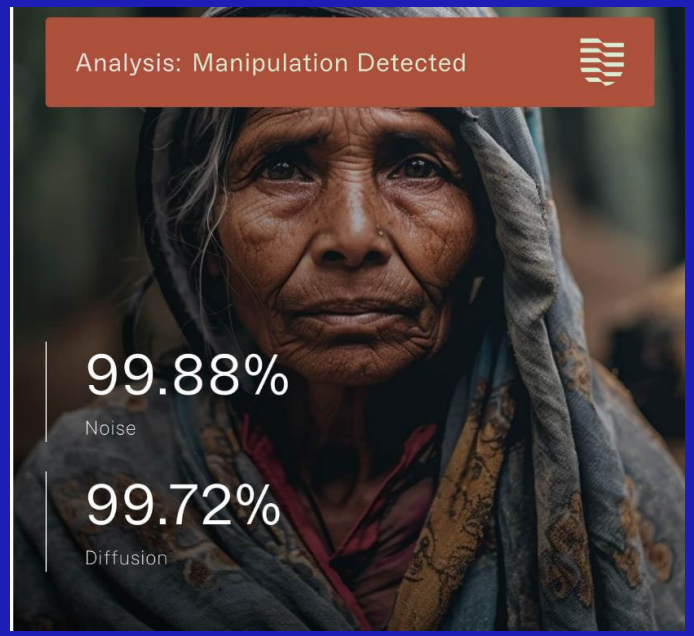


Reality Defender

ディープフェイク検出/保護

- 画像/動画/音声などの幅広いコンテンツに対し、ディープフェイクをリアルタイムで判別。
- 判別は決定論的ではなく確率論であるため、真正性をテストするための透かしや事前の認証は不要。
- マルチモデルアプローチにより、あらゆる角度からあらゆるファイルを調査し、拡散防止を支援する。

拠点	New York, NY
設立	2018
調達額	$ 22.42M
評価額	$ NA /NA
CEO	Benjamin Colman
VC	Amino Capital, Comcast, Contour Venture Partners, DCVC, ex/ante, Nat Friedman, Partnership Fund for New York City, Threadneedle Ventures, Y Combinator



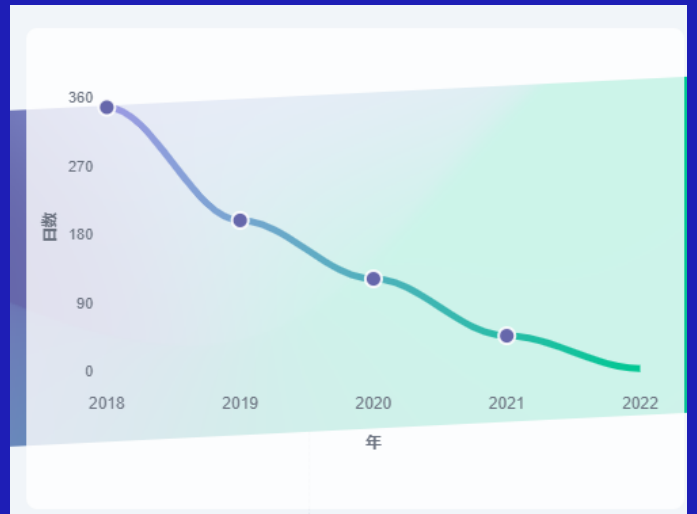
THE ART OF POSSIBLE

VulnCheck

次世代のサイバー脅威インテリジェンス・プラットフォーム

- 脆弱性データに加えて、セキュリティ チームが修復作業の優先順位を付けるのに必要なコンテキストを提供。
- エクスプロイトの情報で脆弱性データを充実させ、攻撃が発生する前の対策を支援する。

拠点	Lexington, MA
設立	2021
調達額	$ 3.2M
評価額	$ NA /Seed
CEO	Anthony Bettini
VC	Aviso Ventures, In-Q-Tel, Lux Capital, Oliver Friedrichs, Sorenson Capital



サイバー脅威の状況は変わった。

2018年には、武器化されたエクスプロイトを持つ**2.5%の**CVEについて、エクスプロイトの武器化には1年弱を要した。

2023年まで早送りすると、搾取兵器化は***8日間***に短縮されている。

Exploit Intelligence for Vulnerability Prioritization

Vulnerability Intelligence

Early access to new vulnerability information not found in the NVD along with dozens of unique fields.

Exploit Intelligence

Real-time monitoring of **exploit PoCs**; exploitation timelines; ransomware, botnet, and APT / threat actor activity.

Initial Access Intelligence

In-house developed exploit PoCs, packet captures, and Suricata signatures to defend against **initial access** vulnerabilities.

Assessment Intelligence

Integrate **vulnerability assessment** into existing asset inventory systems, anywhere Package URLs or CPE strings are present

Thank you☺