ZenithLive24 | zscaler

サイバーセキュリティの最前線：脅威から守る革新ソリューション

ゼットスケーラー株式会社
セールスエンジニアリング本部 セールスエンジニア部
樋口 皓太朗

セーフハーバー

将来の見通しに関する記述

本プレゼンテーションは、情報提供のみを目的としてZscaler, Inc.本プレゼンテーションに含まれる内容は、発表者、Zscaler、または Zscalerの役員、取締役、従業員、代理人、アドバイザーによる推奨、約束、表明ではありません。本プレゼンテーションは、すべてを網羅するものでも、あなたが望むすべての情報を含むものでもありません。

本プレゼンテーションには、将来の見通しに関する記述が含まれています。計画中の製品およびアップグレード、事業戦略、Zscalerの将来の事業に関する経営陣の計画および目標に関する記述を含め、歴史的事実に関する記述を除くすべての記述は、将来の見通しに関する記述です。これらの記述には、既知および多数の未知のリスク、不確実性、仮定、およびその他の要因が含まれており、将来予想に関する記述によって明示または暗示される業績または成果を含め、本メッセージに記載された記述と大きく異なる結果が生じる可能性があります。さらに、当社は非常に競争が激しく変化の激しい環境で事業を展開しており、新たなリスクが随時出現する可能性があります。当社がすべてのリスクを予測することは不可能であり、当社の事業に対するすべての要因の影響や、いかなる要因または要因の組み合わせが、当社が行う将来見通しに関する記述に含まれるものと実際の結果または業績が大きく異なる可能性の程度を評価することもできません。当社の財務および経営成績に影響を及ぼす可能性のあるその他のリスクおよび不確実性は、証券取引委員会に提出した最新の報告書に記載されています。 これらの報告書は、当社ウェブサイト（http://ir.zscaler.com）またはSECウェブサイト（www.sec.gov）でご覧いただけます。

場合によっては、「予想する」、「信じる」、「継続する」、「熟考する」、「可能性がある」、「推定する」、「期待する」、「探求する」、「意図する」、「可能性が高い」、「かもしれない」、「計画する」、「可能性がある」、「予測する」、「プロジェクトする」、「はずである」、「ターゲットする」、「する予定である」、「だろう」などの用語、またはこれらの用語の否定語、またはその他の類似語によって、将来の見通しに関する記述を識別することができます。Zscalerは、これらの将来の見通しに関する記述の大部分を、事業に影響を及ぼすと思われる将来の出来事に関する現在の予想および予測に基づいています。実際の成果や結果は、これらの将来予想に関する記述で意図されたものとは大きく異なる可能性があります。本メッセージに記載されている将来の見通しに関する記述はすべて、本書の日付現在において入手可能な情報に基づくものであり、作成日以降に発生する事象や状況を反映するために、提供された将来の見通しに関する記述を更新する義務を負うものではありません。

歴史上 最初のサイバーセキュリティ対策といわれている仕組みは？

A: IBM Mainframe OS with Chipset

B: Apple II Elk Cloner向け ウイルススキャナー

C: AT&T Bell Labs ネットワークファイアウォール

D: ARPANET 特定プログラム削除ソフトウェア

歴史上 最初のサイバーセキュリティ対策といわれている仕組みは？

A: IBM Mainframe OS with Chipset

B: Apple II Elk Cloner向け ウイルススキャナー

C: AT&T Bell Labs ネットワークファイアウォール

D: ARPANET 特定プログラム削除ソフトウェア

*所説あります。

いたちごっこは続く

アンチウィルスソフト

ヒューリスティック検査

サンドボックス

CSPM・SSPM

FW

URLフィルタ

EDR

SDP・ZTNA

プロキシ

モバイル型AVや
プロキシ

ZTA・
おとり技術

AI駆動型
攻撃

サイバー攻撃からの対策の整理

Cyber Kill Chain
(Lockheed Martin)

MITRE ATT&AK

偵察 | リソース開発 | 初期アクセス | 実行 | 永続化 | 権限昇格 | セキュリティ回避 | 資格情報入手 | 探索 | ラテラルムーブメント | データ収集 | C2C | データ | 影響

対策すべきことを整理すると

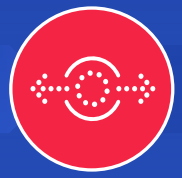
- 攻撃対象領域の最小化
- 不正侵入の防止
- ラテラルムーブメント (水平移動) の排除
- 不正侵入の防止
- データ流出の阻止

Zscalerの包括的なサイバー脅威対策

攻撃者が発見する
偵察

侵入する
足場を確立、マルウェアを配信

水平に移動する
ネットワーク内を移動する



データを盗む
情報漏洩/暗号化

zscaler

攻撃対象領域の最小化

- 攻撃対象領域の管理
- ゼロトラストのアプリ アクセス
- 攻撃対象領域の排除

不正侵入の防止

- 高度な脅威対策
- ファイアウォール/IPS
- サンドボックス
- AppProtection™
- ブラウザ分離
- DNSセキュリティ
- クラウドリソース
- URLフィルタリング

ラテラル ムーブメントの排除

- AIアプリ セグメンテーション
- 特権アクセス
- デセプション
- マイクロセグメンテーション

データ流出の阻止

- AIを活用した データの検出と分類
- 転送中データの保護
- 保存データの保護

リスクの評価と侵害の検出

Risk360

統合型の脆弱性管理

デセプション

ITDR

脅威ハンティング

侵害分析

Zscalerの包括的なサイバー脅威対策

攻撃者が発見する
偵察

zscaler

攻撃対象領域の最小化

攻撃対象領域の管理

ゼロトラストのアプリ アクセス

攻撃対象領域の排除

侵入する
足場を確立、マルウェアを配信

不正侵入の防止

高度な脅威対策

サンドボックス

ブラウザ分離

クラウドリソース

ファイアウォール/IPS

AppProtection™

DNSセキュリティ

URLフィルタリング

水平に移動する
ネットワーク内を移動する

ラテラル ムーブメントの排除

AIアプリ セグメンテーション

特権アクセス

デセプション

マイクロセグメンテーション

データを盗む
情報漏洩/暗号化

データ流出の阻止

AIを活用した
データの検出と分類

転送中データの保護

保存データの保護

リスクの評価と侵害の検出

Risk360

統合型の
脆弱性管理

デセプション

ITDR

脅威ハンティング

侵害分析

攻撃対象領域の最小化 | 不正侵入の防止 | ラテラル ムーブメントの防止 | 情報漏洩の防止

1. リモート ユーザー向けの
インバウンドVPNを廃止
2. すべてをZero Trust Exchangeの
背後に隠し、攻撃対象領域を排除
3. 攻撃対象領域を把握

近日
リリース
予定

外部攻撃対象領域管理
(EASM)

EASMによるデータ統合

既存の領域

ドメイン

ASN

ホスト

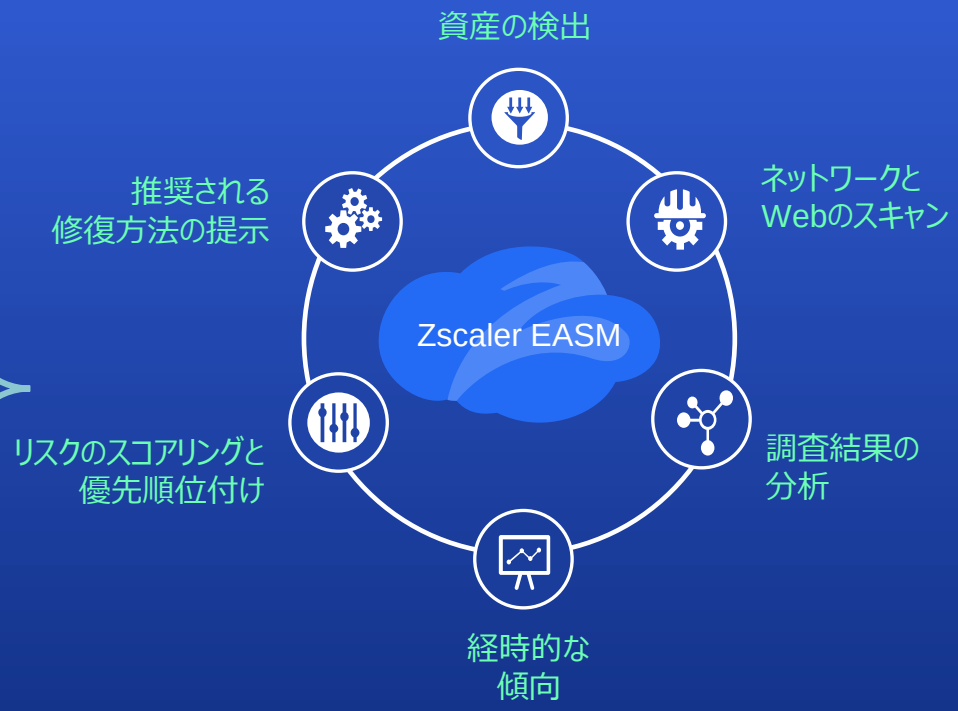
IPアドレス

Webページ

TLS証明書

Zscaler ThreatlabZ

Zscaler Risk360



ロードマップ

パブリック ストレージ バケット

パブリック コード リポジトリー

Zscaler Avalor Data Fabric

Zscaler Deception

Zscaler Private Access

Zscaler DSPM

Zscaler Breach Predictor

EASM

Search

- Dashboard
  - Insights Overview
  - Assets Overview
- Insights
- Assets
- Alerts
- Administration
- Notifications
- Tools
- Account
- Log Out

Insights Overview

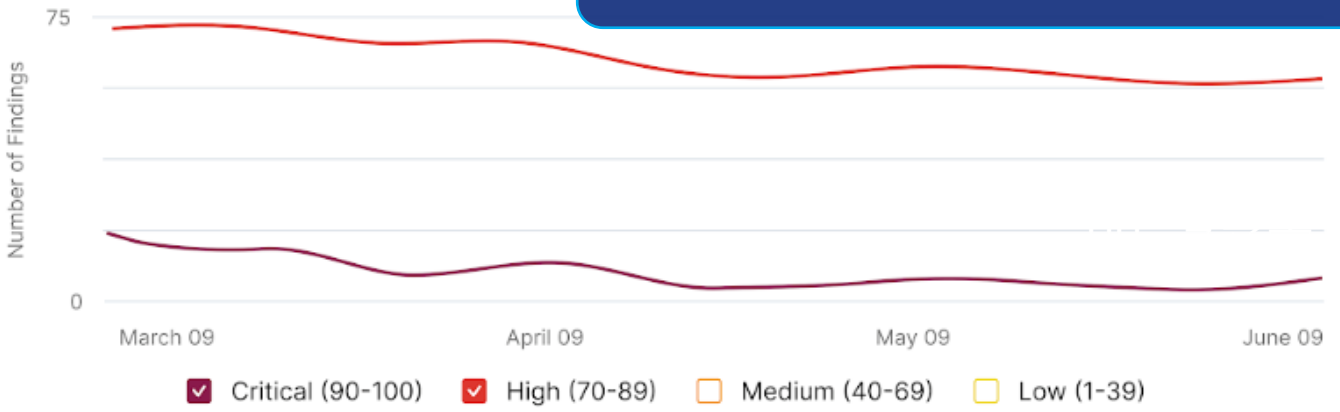
Last updated on June 09, 2024 | Organization: AcmeHealthcare

攻撃対象領域の管理

Distribution of Findings by Risk Level

Critical	High	Medium	Low
5 findings	56 findings	1,878 findings	4,155 findings

Findings over time by Risk Level



Findings Percentage by Category

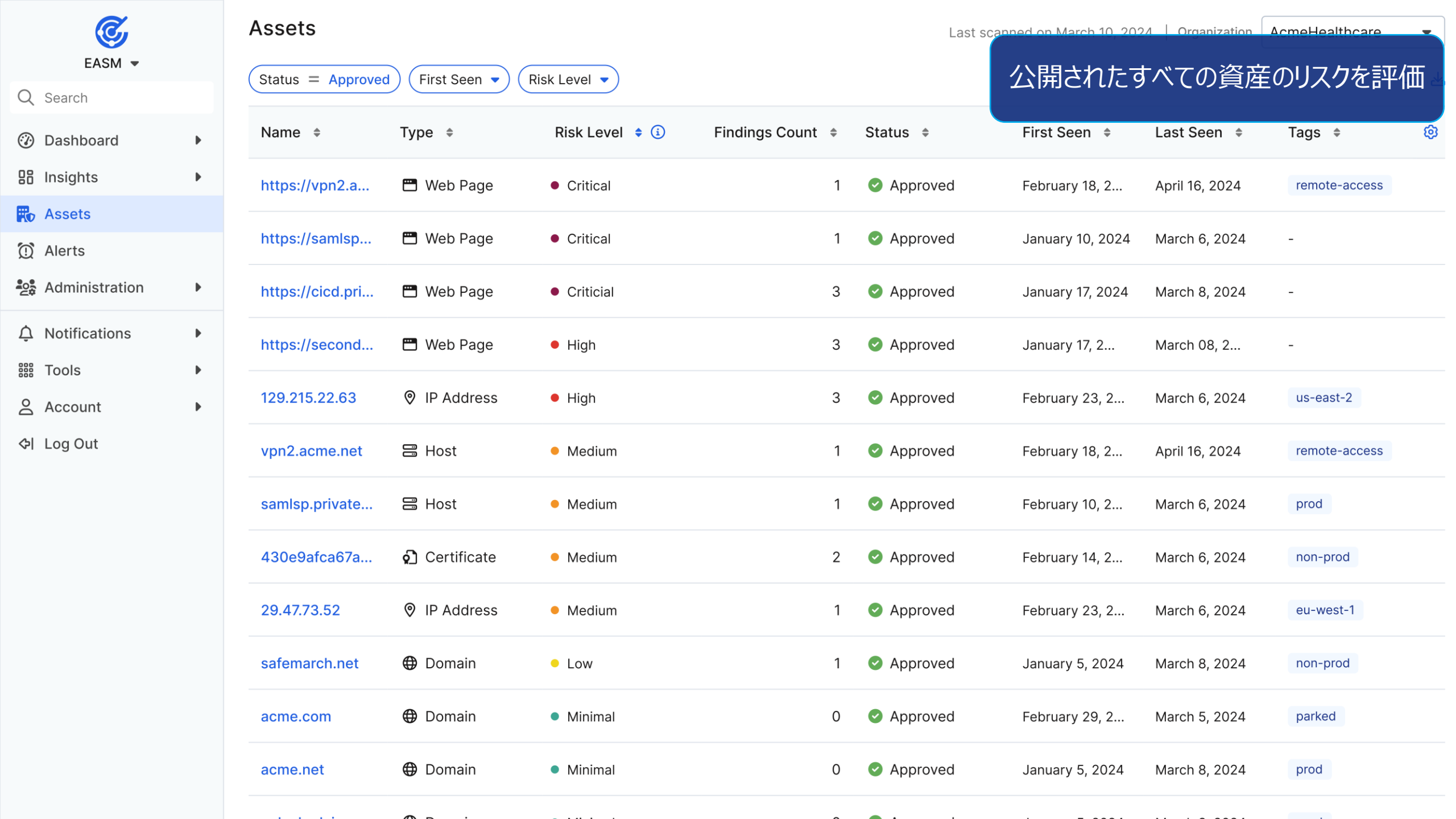
Top 5 Lookalike Domains by Exposure

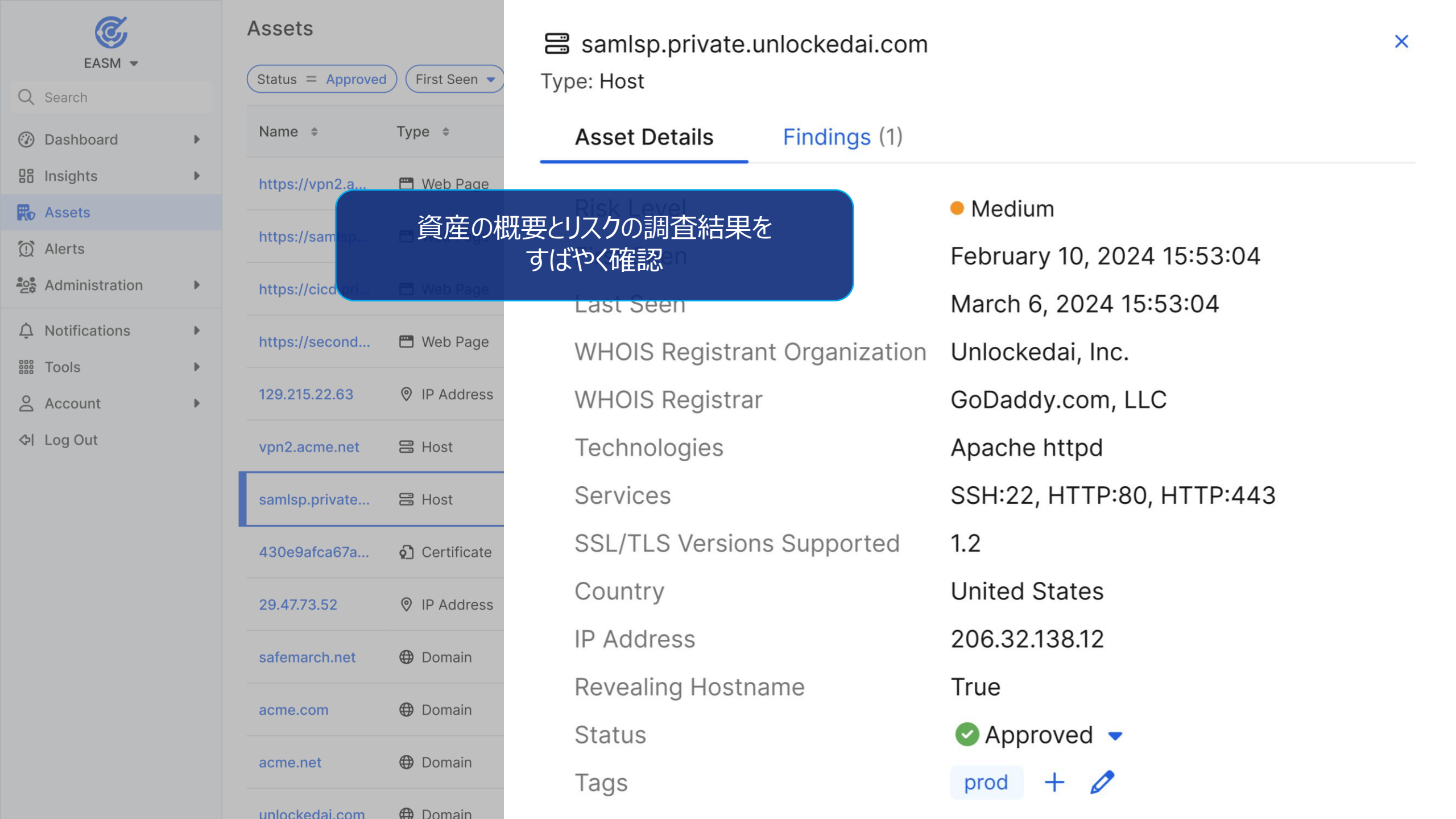
View All Lookalike Domains >

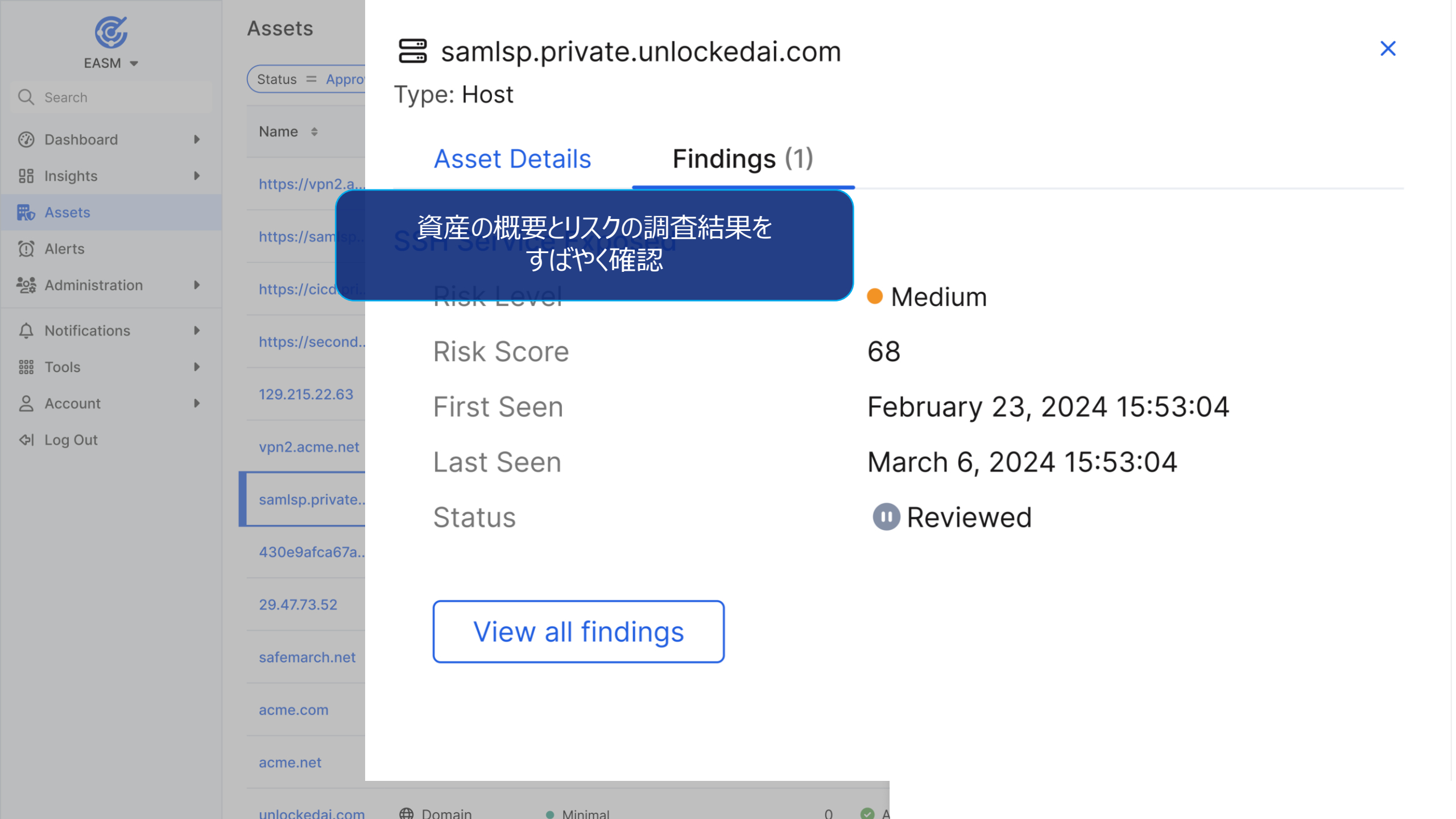
Original Domain	Lookalike Domain	Risk Category	Exposure Score
unlockedai.com	unlockedai.com	Registered Lookalike	90
unlockedai.com	unlokedai.com	Registered Lookalike	90
unlockedai.com	unlocked-ai.com	Registered Lookalike	85
unlocked.ai	unlockedlogin.ai	Registered Lookalike	81
unlockedai.com	unlockedai.net	Preventative Lookalike	73

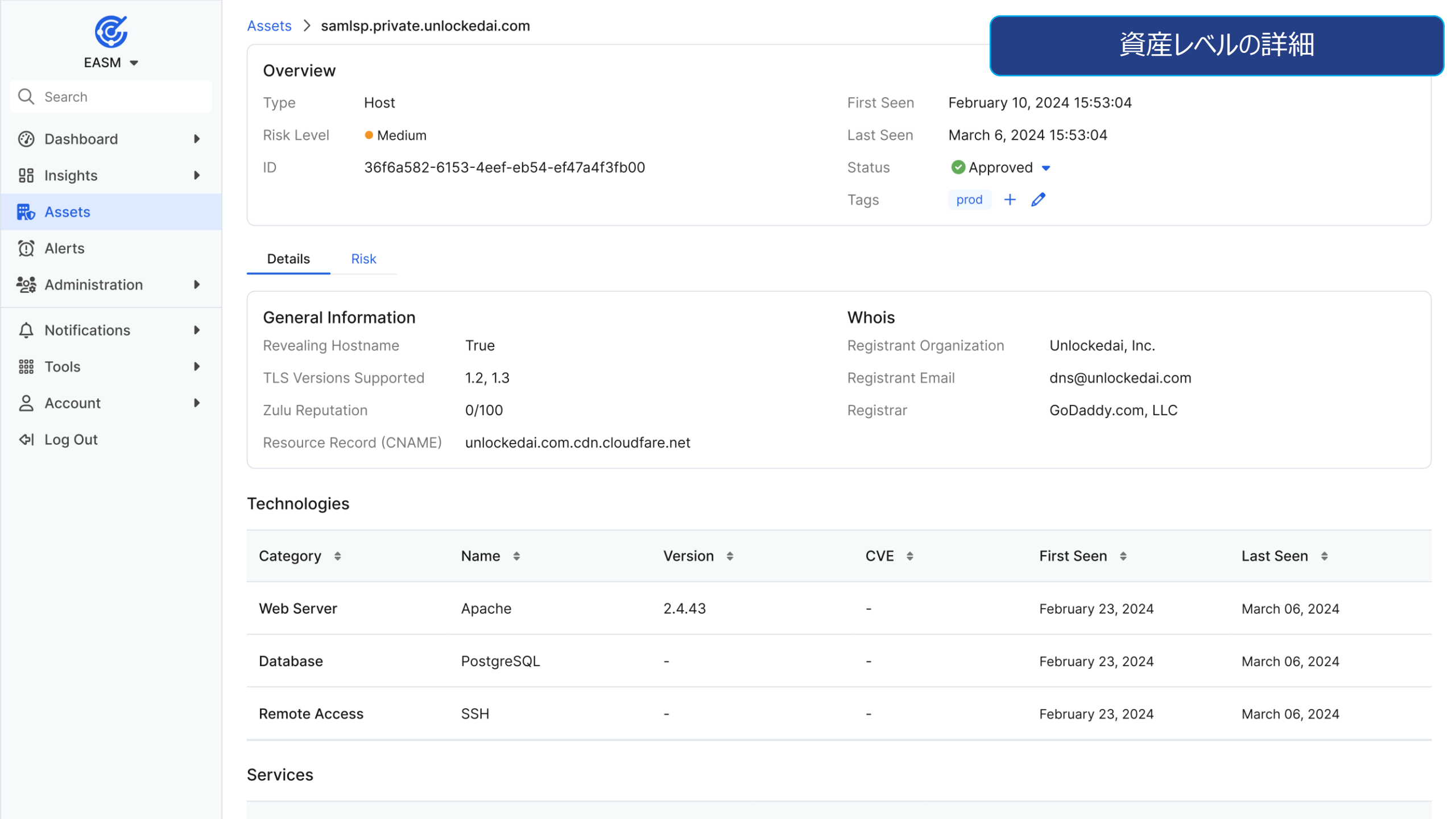
Top 5 Exposed VPN Applicances

View All VPN Appliances >


EASM
Search
Dashboard
Insights
Assets
Alerts
Administration
Notifications
Tools
Account
Log Out
Assets
Last scanned on March 10, 2024
Organization
AcmeHealthcare
公開されたすべての資産のリスクを評価
Status = Approved
First Seen
Risk Level
Name
Type
Risk Level
Findings Count
Status
First Seen
Last Seen
Tags
https://vpn2.a... Web Page Critical 1 Approved February 18, 2... April 16, 2024 remote-access
https://samlsp... Web Page Critical 1 Approved January 10, 2024 March 6, 2024 -
https://cicd.pri... Web Page Criticial 3 Approved January 17, 2024 March 8, 2024 -
https://second... Web Page High 3 Approved January 17, 2... March 08, 2... -
129.215.22.63 IP Address High 3 Approved February 23, 2... March 6, 2024 us-east-2
vpn2.acme.net Host Medium 1 Approved February 18, 2... April 16, 2024 remote-access
samlsp.private... Host Medium 1 Approved February 10, 2... March 6, 2024 prod
430e9afca67a... Certificate Medium 2 Approved February 14, 2... March 6, 2024 non-prod
29.47.73.52 IP Address Medium 1 Approved February 23, 2... March 6, 2024 eu-west-1
safemarch.net Domain Low 1 Approved January 5, 2024 March 8, 2024 non-prod
acme.com Domain Minimal 0 Approved February 29, 2... March 5, 2024 parked
acme.net Domain Minimal 0 Approved January 5, 2024 March 8, 2024 prod


EASM
Search
Dashboard
Insights
Assets
Alerts
Administration
Notifications
Tools
Account
Log Out
Assets
Status = Approved
First Seen
Name
Type
https://vpn2.a...
Web Page
https://sam...
https://cico...
Web Page
https://second...
Web Page
129.215.22.63
IP Address
vpn2.acme.net
Host
samlsp.private...
Host
430e9afca67a...
Certificate
29.47.73.52
IP Address
safemarch.net
Domain
acme.com
Domain
acme.net
Domain
unlockedai.com
Domain
資産の概要とリスクの調査結果を
すばやく確認
samlsp.private.unlockedai.com
Type: Host
Asset Details
Findings (1)
Risk Level
Medium
First Seen
February 10, 2024 15:53:04
Last Seen
March 6, 2024 15:53:04
WHOIS Registrant Organization
Unlockedai, Inc.
WHOIS Registrar
GoDaddy.com, LLC
Technologies
Apache httpd
Services
SSH:22, HTTP:80, HTTP:443
SSL/TLS Versions Supported
1.2
Country
United States
IP Address
206.32.138.12
Revealing Hostname
True
Status
Approved
Tags
prod


EASM
Search
Dashboard
Insights
Assets
Alerts
Administration
Notifications
Tools
Account
Log Out
Assets
Status = Appro
Name
https://vpn2.a...
https://sam...
https://cico...
https://second...
129.215.22.63
vpn2.acme.net
samlsp.private...
430e9afca67a...
29.47.73.52
safemarch.net
acme.com
acme.net
unlockedai.com
Domain
Minimal
0
samlsp.private.unlockedai.com
Type: Host
Asset Details
Findings (1)
資産の概要とリスクの調査結果を
すばやく確認
Risk Level
Medium
Risk Score
68
First Seen
February 23, 2024 15:53:04
Last Seen
March 6, 2024 15:53:04
Status
Reviewed
View all findings


EASM
Search
Dashboard
Insights
Assets
Alerts
Administration
Notifications
Tools
Account
Log Out
Assets > samlsp.private.unlockedai.com
資産レベルの詳細
Overview
Type Host
Risk Level Medium
ID 36f6a582-6153-4eef-eb54-ef47a4f3fb00
First Seen February 10, 2024 15:53:04
Last Seen March 6, 2024 15:53:04
Status Approved
Tags prod
Details
Risk
General Information
Revealing Hostname True
TLS Versions Supported 1.2, 1.3
Zulu Reputation 0/100
Resource Record (CNAME) unlockedai.com.cdn.cloudfare.net
Whois
Registrant Organization Unlockedai, Inc.
Registrant Email dns@unlockedai.com
Registrar GoDaddy.com, LLC
Technologies
Category
Name
Version
CVE
First Seen
Last Seen
Web Server
Apache
2.4.43
-
February 23, 2024
March 06, 2024
Database
PostgreSQL
-
-
February 23, 2024
March 06, 2024
Remote Access
SSH
-
-
February 23, 2024
March 06, 2024
Services

資産レベルの詳細

20	SSH	Open	February 23, 2024	March 06, 2024
80	HTTP	Open	February 23, 2024	March 06, 2024
443	HTTPS	Open	February 23, 2024	March 06, 2024

SSL/TLS Ceritificates

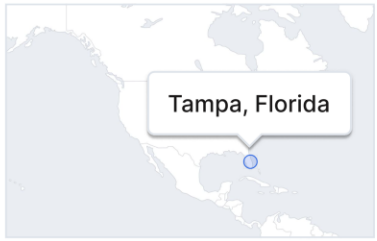
Asset Name	Subject Common Name	Issued	Expires	First Seen	Last Seen	Recent
430e9afca67a8a1f7fad20c7780635796...	*.unlockedai.com	September 05, 2023	October 06, 2024	February 14, 2024	March 06, 2024	Yes
57ac0079b57d1a7f182a03b4779ea6da5...	samlsp.private.unlockeda...	February 27, 2024	February 23, 2025	March 01, 2024	March 06, 2024	Yes

Clouds

CDN	Cloudflare
CSP	AWS

Location

Country	United States
State/Province	Florida
City	Tampa
IP Address	206.32.138.12



Discovery Chain

Seed Domain: unlockedai.com

↳ Attribute: Registrant Organization: Unlockedai, Inc.

↳ IP Block: 206.32.138.0/24

↳ IP Address: 206.32.138.12

↳ Host: samlsp.private.unlockedai.com

Discovery Information

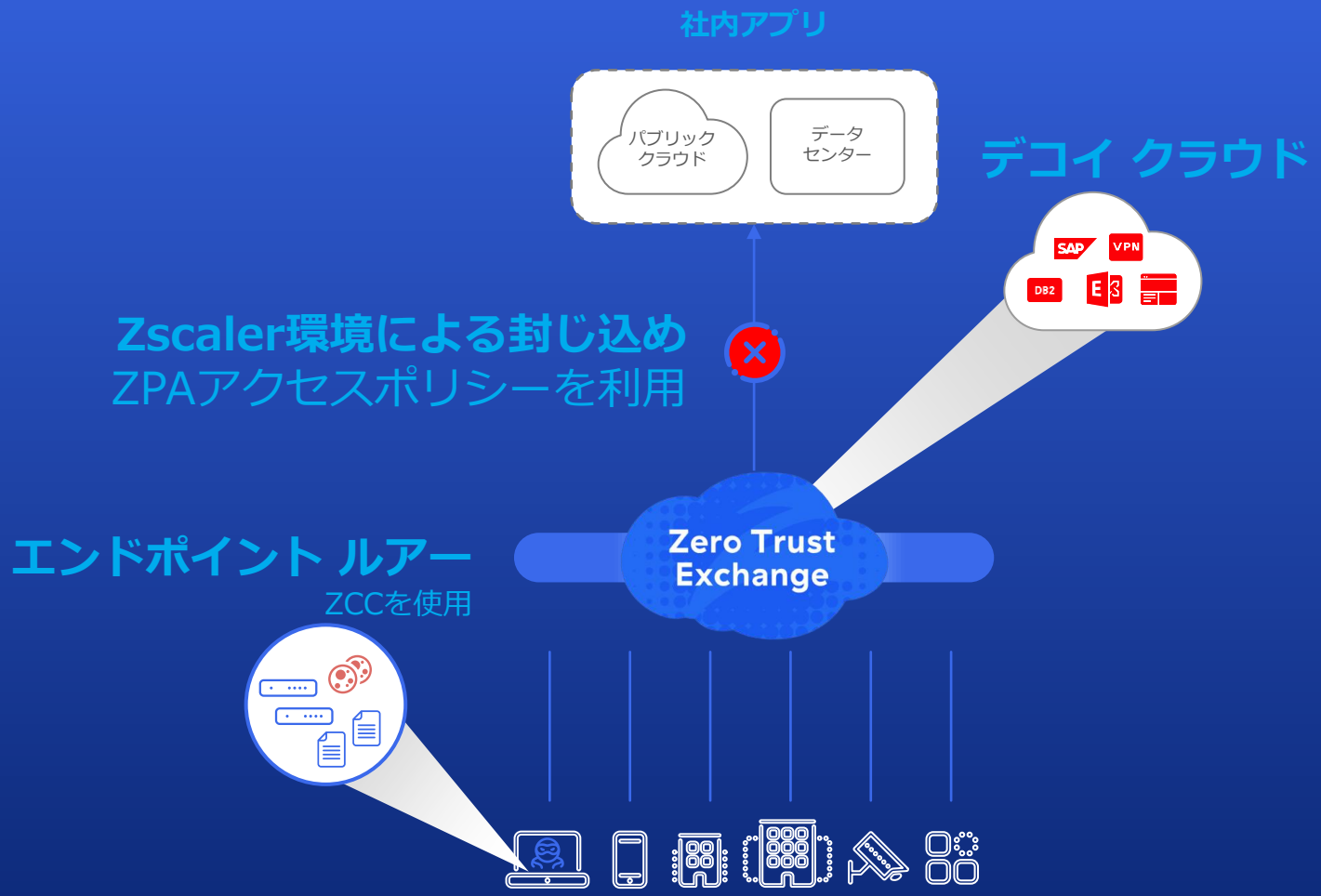
Profile	SecOps
Seed	unlockedai.com
First Seen	February 23, 2024
Last Seen	March 06, 2024

提供中

デセプション

脅威インテリジェンスを活用したデコイ

デセプション おとり技術を用いた攻撃検知と封じ込め (ゼロトラスト デコイモデルの例)



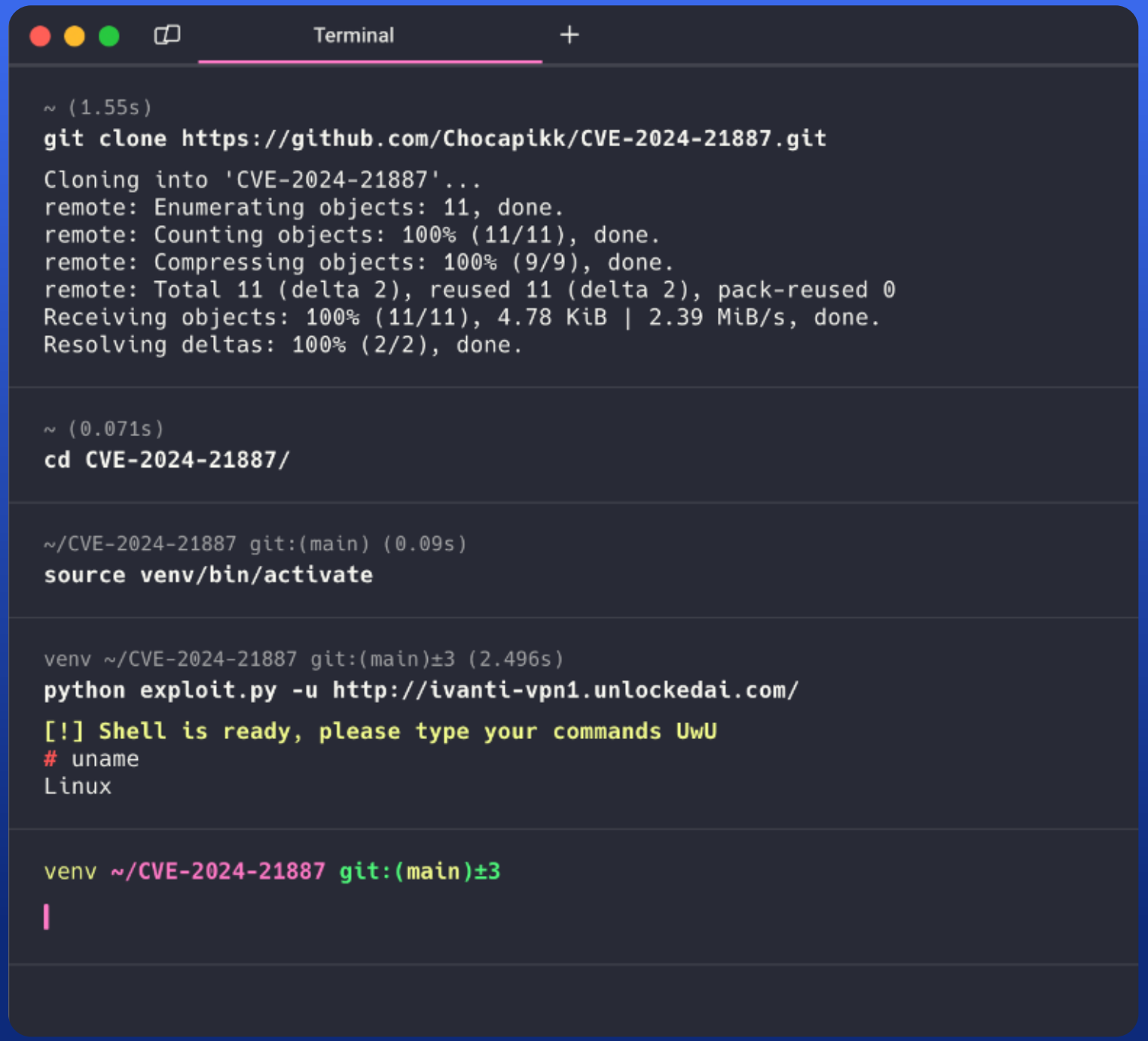
簡単な導入
VMやアプリは不要。Zscalerの統合
エンドポイントエージェントを使用

ネットワークの変更不要
VLANトランキング/SPANポート/GREトンネル不要

Zscaler環境での封じ込め
ZPA ポリシーにより侵害されたユーザーを遮断

脆弱なVPNに対する攻撃を検出

CVEの悪用を検出



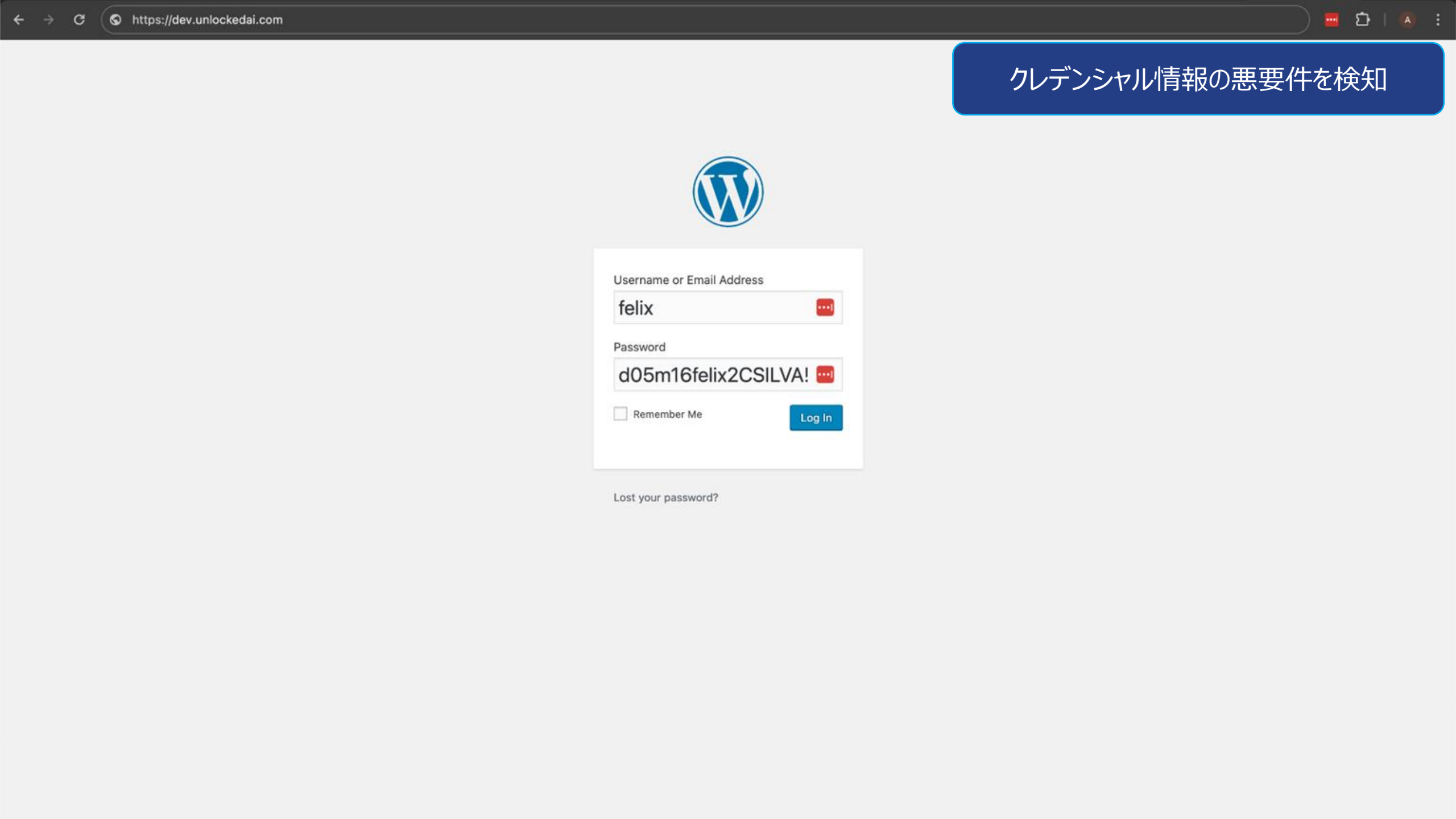
脆弱なVPNに対する攻撃を検出

CVEの悪用を検出


Investigate
脆弱なVPNに対する攻撃を検出
CVEの悪用を検出
Add Tag
RISK SCORE
125
FIRST EVENT
03 JUN 2024 | 11:51 +05:30
LAST EVENT
10 JUN 2024 | 12:00 +05:30
THREATPARSE
Possible exploitation of vulnerability in Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) (CVE-2024-21887)
Web application access
Network connection initiated towards a decoy
TRIAGE INCIDENTS
No Triage Data Available
Actions
View Extended Details
ip-10-123-34-101
ivanti-vpn1
default
rayclank-appliance-1
rayclank
10 Jun 2024 - 11:49
10 Jun 2024 - 11:52
10 Jun 2024 - 11:55
10 Jun 2024 - 11:58


クレデンシャル情報の悪要件を検知
Network Decoys
Deploy decoy systems in your internal network, internal DMZ segments, cloud, and Zero Trust environments.
Investigate
Orchestrate
Miragemaker
Deceive
ITDR
Settings
Search
Internal
Zero Trust Network
Export Decoy Configuration
Add Decoys
FQDN and IP Personality Network Decoy Groups Network Name Actions
1 corebank-staging.unlockedai.com 10.123.2.102 Finance - Finacle Web WEB default VLAN 502 DHCP
2 dev.unlockedai.com 10.123.2.100 Development - Developer Portals Web WEB Default Automatic Decoys VLAN 502 DHCP
3 ivanti-vpn1.unlockedai.com 10.123.2.101 Common - VPN WEB default VLAN 502 DHCP
4 globalprotect-prod.unlockedai.com 10.123.2.103 Common - VPN WEB Artificial Intelligence (AI) Dynamic VLAN 502 DHCP
5 webhost.unlockedai.com 10.123.2.105 Deception AI WEB SSH Artificial Intelligence (AI) Dynamic VLAN 502 DHCP
6 sales-llm.unlockedai.com 10.123.2.104 Detect attacks on GenAI Infrastructure WEB Artificial Intelligence (AI) Dynamic VLAN 502 DHCP
« PREV
Total: 6 Page 1 of 1
NEXT »
Copyright©2024 Zscaler Inc. All rights reserved. | Version develop-2024-05-24T09:27:05 | Database Version: c97c06876421 | Patents

クレデンシャル情報の悪要件を検知

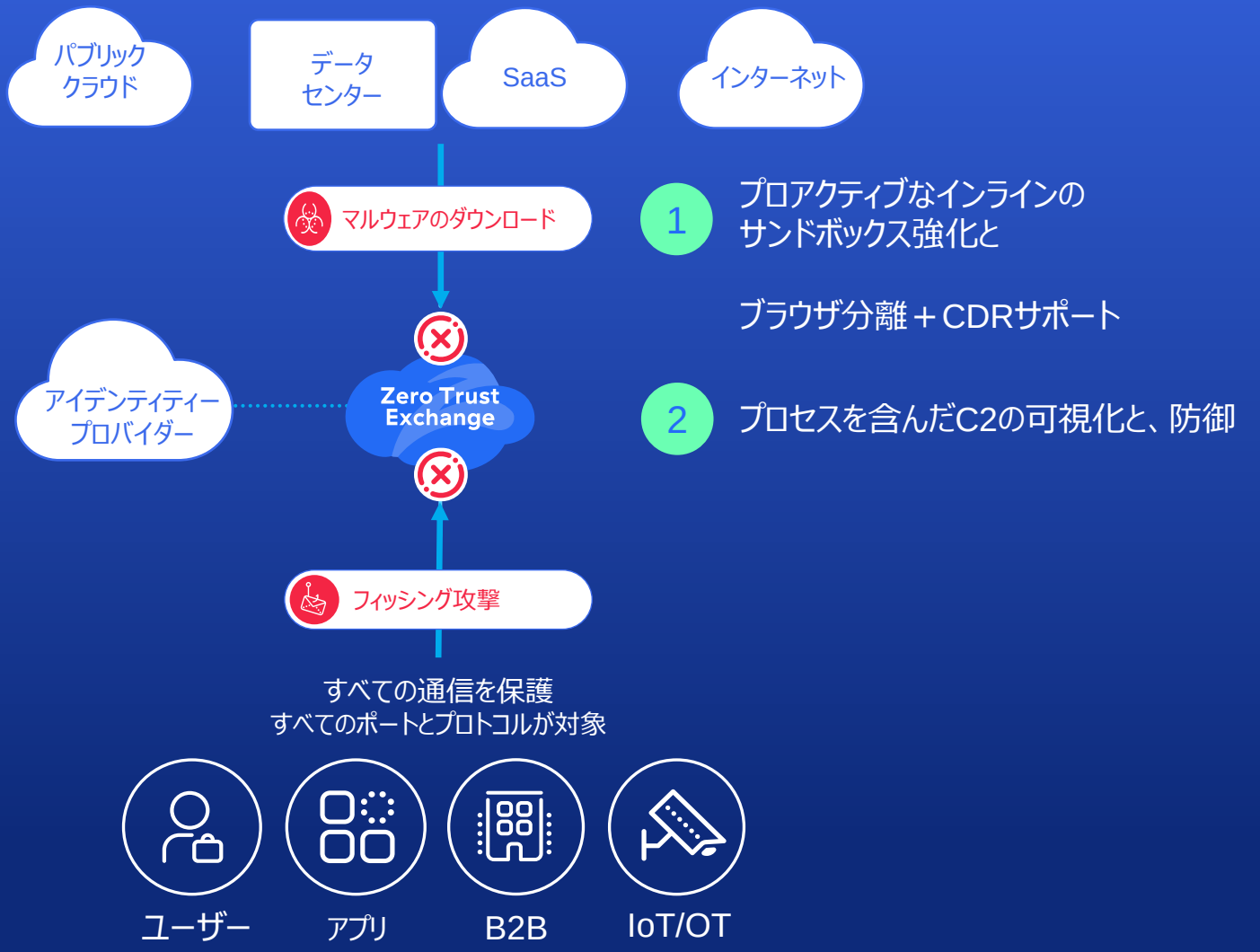



Investigate
Investigate
Orchestrate
Miragemaker
Deceive
ITDR
Settings
Search
クレデンシャル情報の悪要件を検知
IP-10-123-34-101
10.123.34.101
+ Add Tag
RISK SCORE
225
FIRST EVENT
03 JUN 2024 | 11:51 +05:30
LAST EVENT
10 JUN 2024 | 12:15 +05:30
THREATPARSE
• Possible login using credentials stuffed or obtained from data breach
• Web application access
• Network connection initiated towards a decoy
TRIAGE INCIDENTS
No Triage Data Available
Actions
View Extended Details
ivanti-vpn1
default
corebank-staging
ip-10-123-34-101
rayclank-appliance-1
rayclank
dev
Default Automatic Decoys
10 Jun 2024 - 12:05
10 Jun 2024 - 12:08
10 Jun 2024 - 12:11
10 Jun 2024 - 12:14

攻撃対象領域の最小化 | 不正侵入の防止 | ラテラル ムーブメントの防止 | 情報漏洩の防止

1. リモート ユーザー向けの
インバウンドVPNを廃止
2. すべてをZero Trust Exchangeの
背後に隠し、攻撃対象領域を排除
3. 攻撃対象領域を把握

攻撃対象領域の最小化 | **不正侵入の防止** | ラテラル ムーブメントの防止 | 情報漏洩の防止



1 プロアクティブなインラインの
サンドボックス強化と

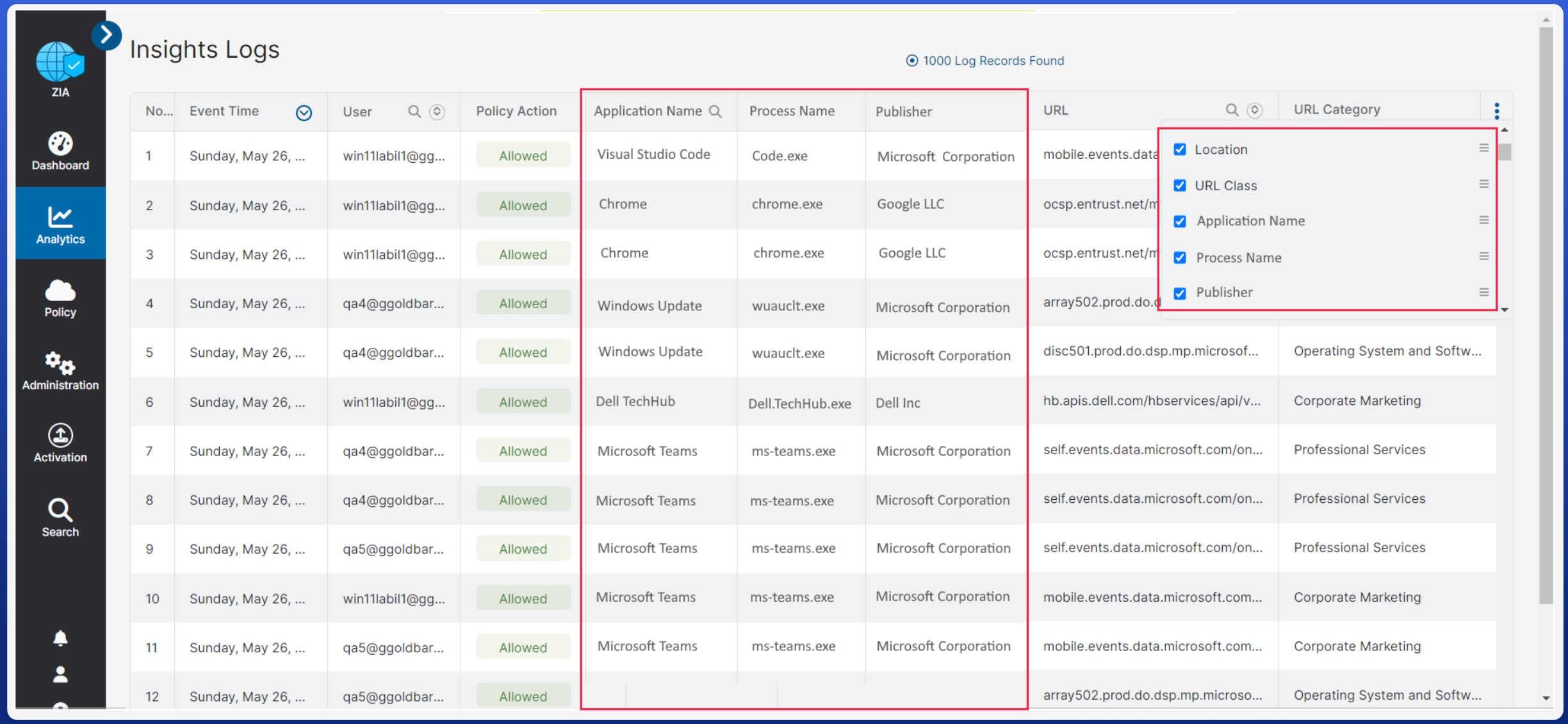
ブラウザ分離＋CDRサポート

2 プロセスを含んだC2の可視化と、防御

C2の検出強化と
プロセス関連付け

プロセストラフィックの異常と未知のC2を検出するイノベーション

SOCを支援



No...	Event Time	User	Policy Action	Application Name	Process Name	Publisher	URL	URL Category
1	Sunday, May 26, ...	win11labil1@gg...	Allowed	Visual Studio Code	Code.exe	Microsoft Corporation	mobile.events.data	
2	Sunday, May 26, ...	win11labil1@gg...	Allowed	Chrome	chrome.exe	Google LLC	ocsp.entrust.net/m	
3	Sunday, May 26, ...	win11labil1@gg...	Allowed	Chrome	chrome.exe	Google LLC	ocsp.entrust.net/m	
4	Sunday, May 26, ...	qa4@ggoldbar...	Allowed	Windows Update	wuauclt.exe	Microsoft Corporation	array502.prod.do.d	
5	Sunday, May 26, ...	qa4@ggoldbar...	Allowed	Windows Update	wuauclt.exe	Microsoft Corporation	disc501.prod.do.dsp.mp.microsof...	Operating System and Softw...
6	Sunday, May 26, ...	win11labil1@gg...	Allowed	Dell TechHub	Dell.TechHub.exe	Dell Inc	hb.apis.dell.com/hbservices/api/v...	Corporate Marketing
7	Sunday, May 26, ...	qa4@ggoldbar...	Allowed	Microsoft Teams	ms-teams.exe	Microsoft Corporation	self.events.data.microsoft.com/on...	Professional Services
8	Sunday, May 26, ...	qa4@ggoldbar...	Allowed	Microsoft Teams	ms-teams.exe	Microsoft Corporation	self.events.data.microsoft.com/on...	Professional Services
9	Sunday, May 26, ...	qa5@ggoldbar...	Allowed	Microsoft Teams	ms-teams.exe	Microsoft Corporation	self.events.data.microsoft.com/on...	Professional Services
10	Sunday, May 26, ...	win11labil1@gg...	Allowed	Microsoft Teams	ms-teams.exe	Microsoft Corporation	mobile.events.data.microsoft.com...	Corporate Marketing
11	Sunday, May 26, ...	qa5@ggoldbar...	Allowed	Microsoft Teams	ms-teams.exe	Microsoft Corporation	mobile.events.data.microsoft.com...	Corporate Marketing
12	Sunday, May 26, ...	qa5@ggoldbar...	Allowed				array502.prod.do.dsp.mp.microso...	Operating System and Softw...

近日
リリース
予定

サンドボックス

macOSファイルのサポート

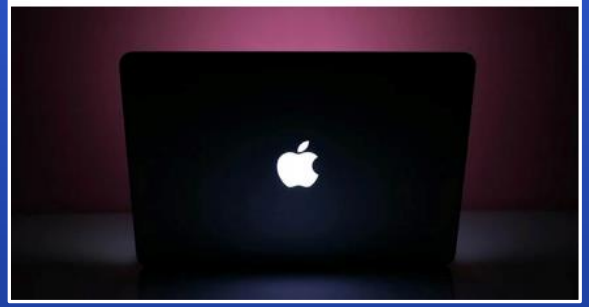
macOSを標的とする攻撃者の増加

The Hacker News

Home | Newsletter | Webinars

Researchers Discover New Sophisticated Toolkit Targeting Apple macOS Systems

Jun 19, 2023 Ravie Lakshmanan



Macworld

MAC IPHONE IPAD APPLE WATCH

Scary 'MacStealer' malware goes after iCloud passwords and credit card data

Security community is abuzz about Telegram-based intruder.

BLEEPINGCOMPUTER

Home > News > Security > New CloudMensis malware backdoors Macs to steal victims' data

New CloudMensis malware backdoors Macs to steal victims' data

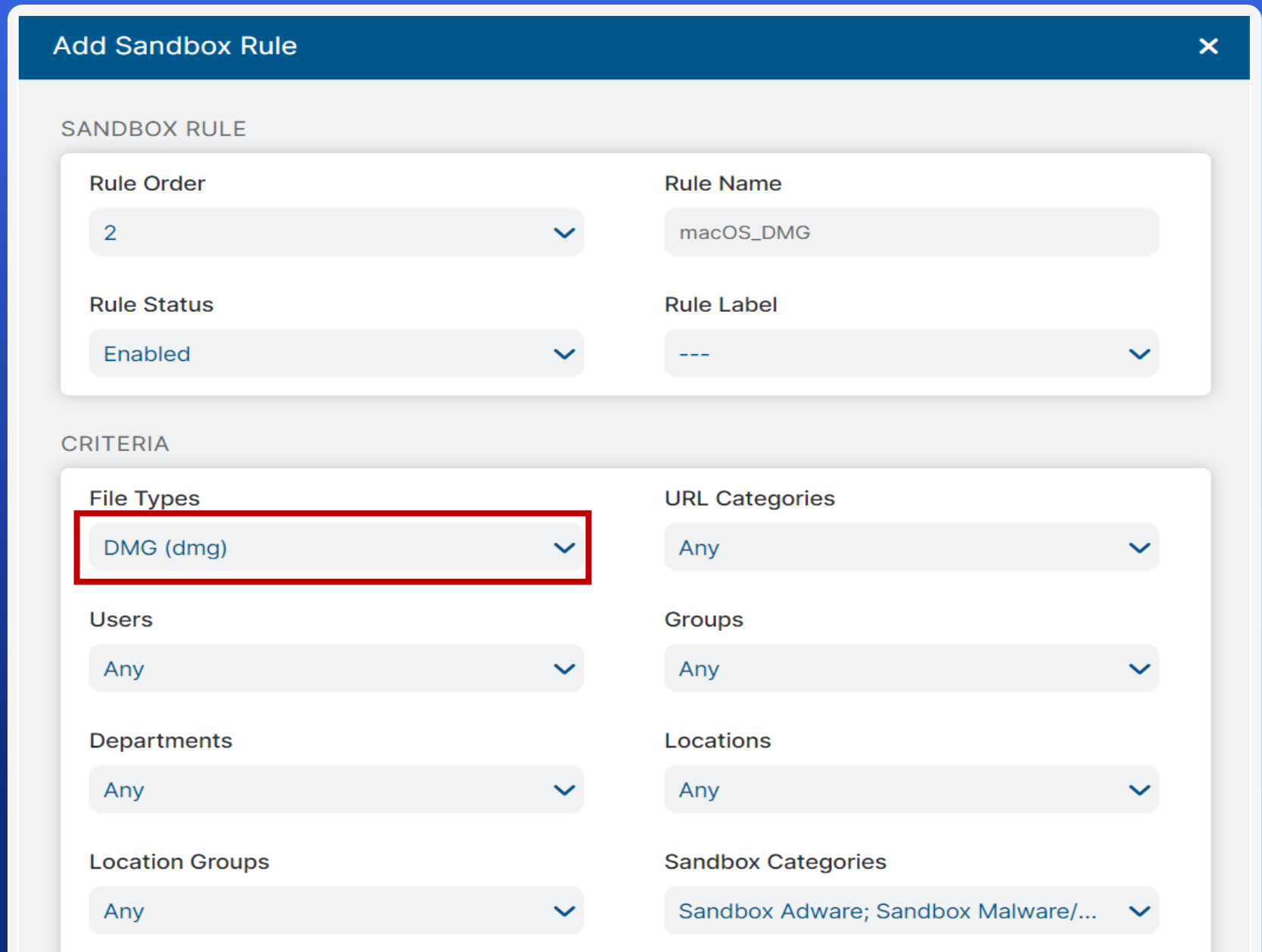
SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

MALWARE & THREATS

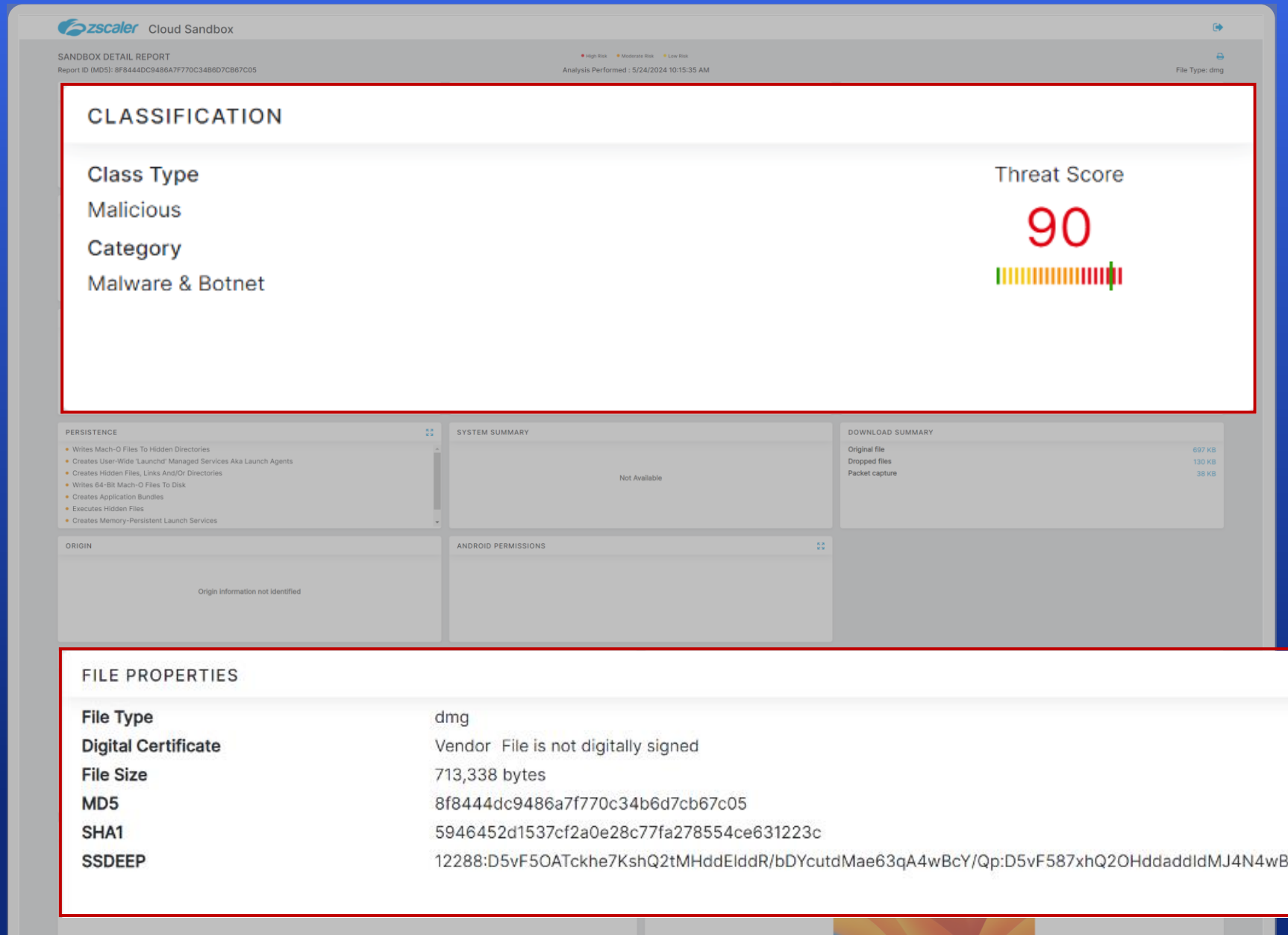
'Atomic macOS Stealer' Malware Delivered via Malvertising Campaign

A malware named Atomic macOS Stealer (AMOS) has been delivered to users via a malvertising campaign.

サンドボックスでのmacOSファイルのサポート



サンドボックスでのmacOSファイルのサポート



近日
リリース
予定

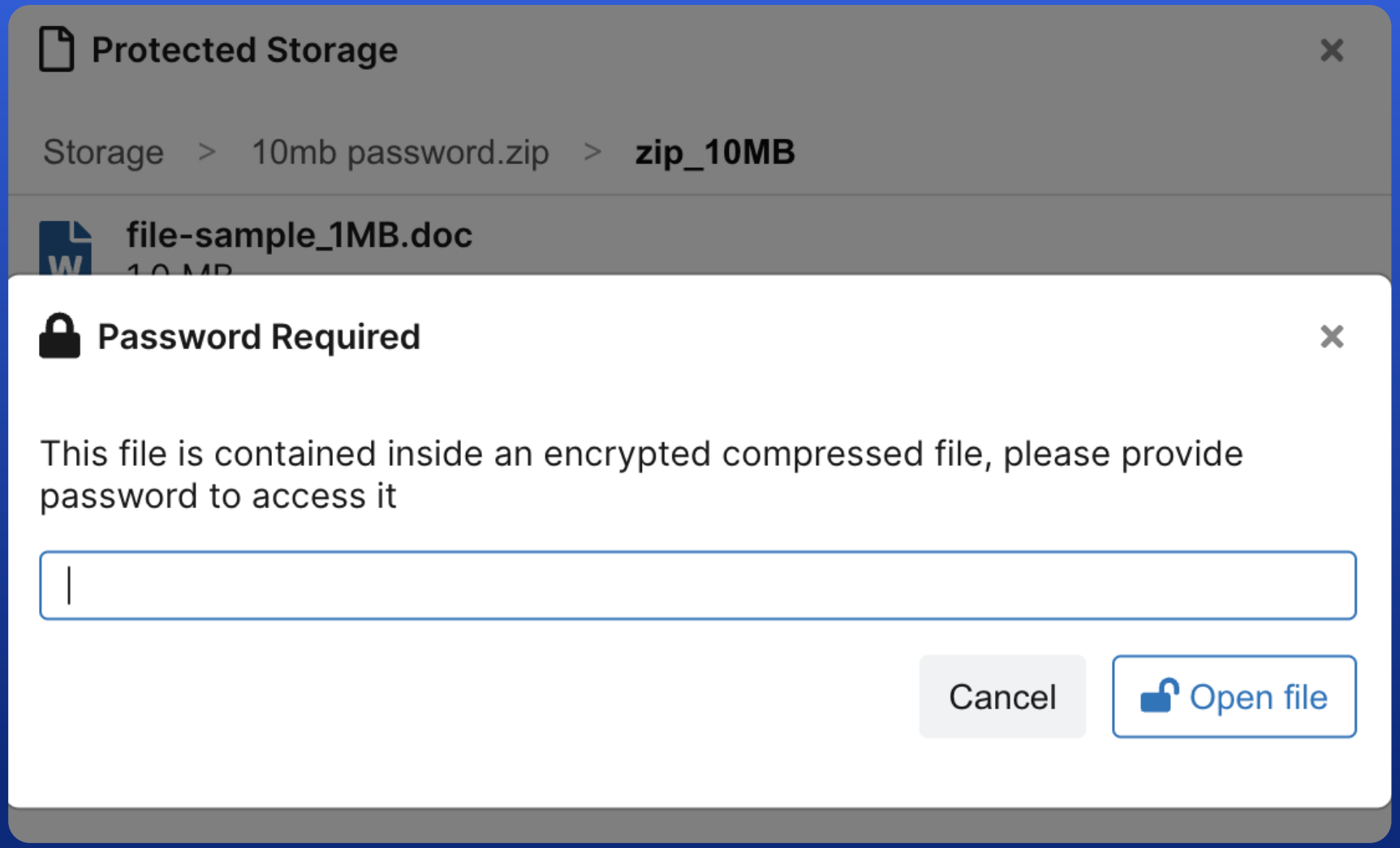
ブラウザ分離

パスワードで保護されたファイルのサポート
コンテンツの無害化と再構築(CDR)レベル3

ファイルの分離とCDR
コンテンツの無害化と再構築

ドキュメントの表示
(パスワードで保護されたファイル)
ブラウザー内で閲覧

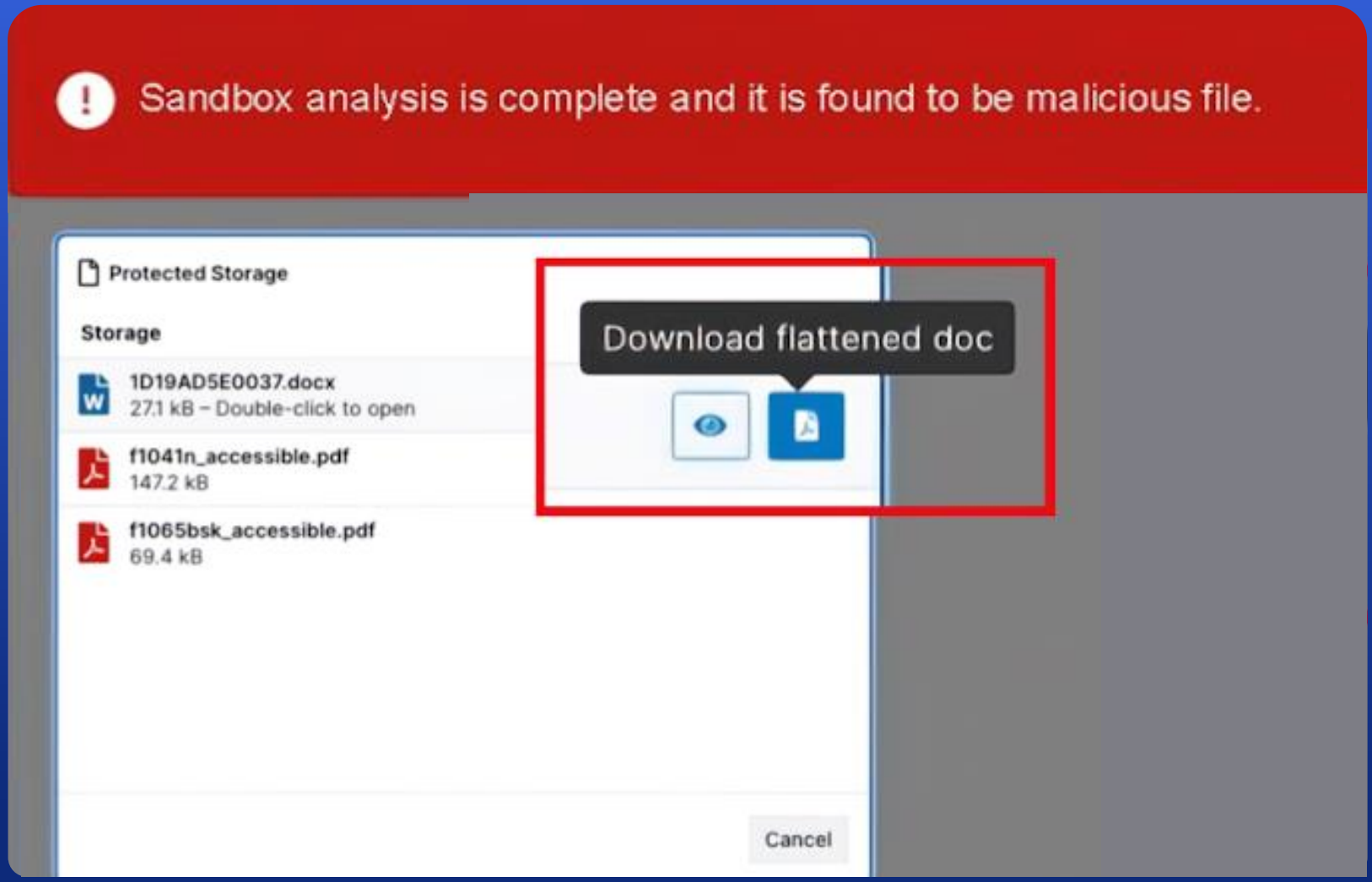
「即時表示」
サンドボックス分析中の
閲覧



ファイルの分離とCDR
コンテンツの無害化と再構築

無害化されたPDFの
ダウンロード
レベル1のCDR

xlsx、docx、pptxなどの
PDFへの変換

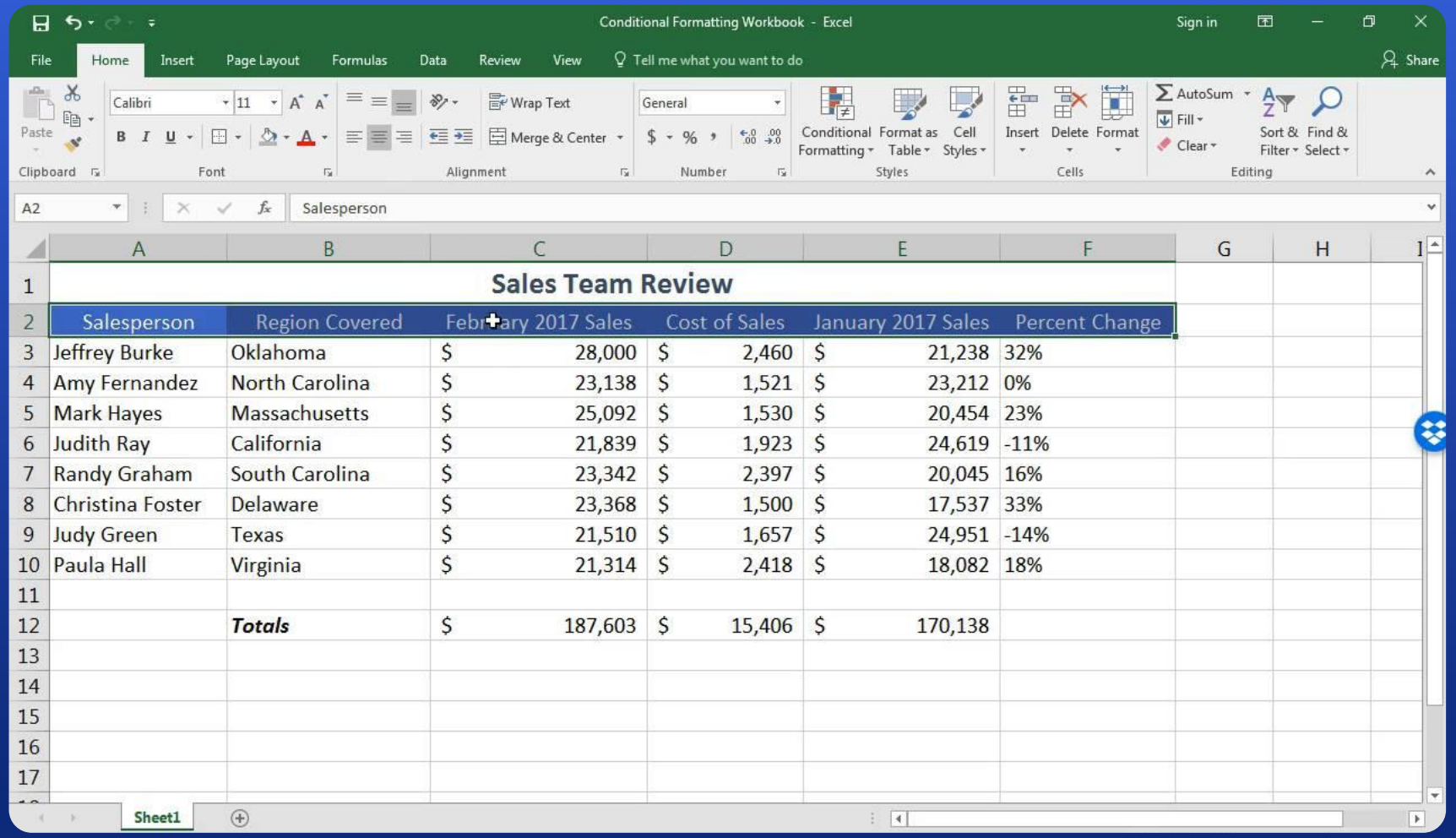


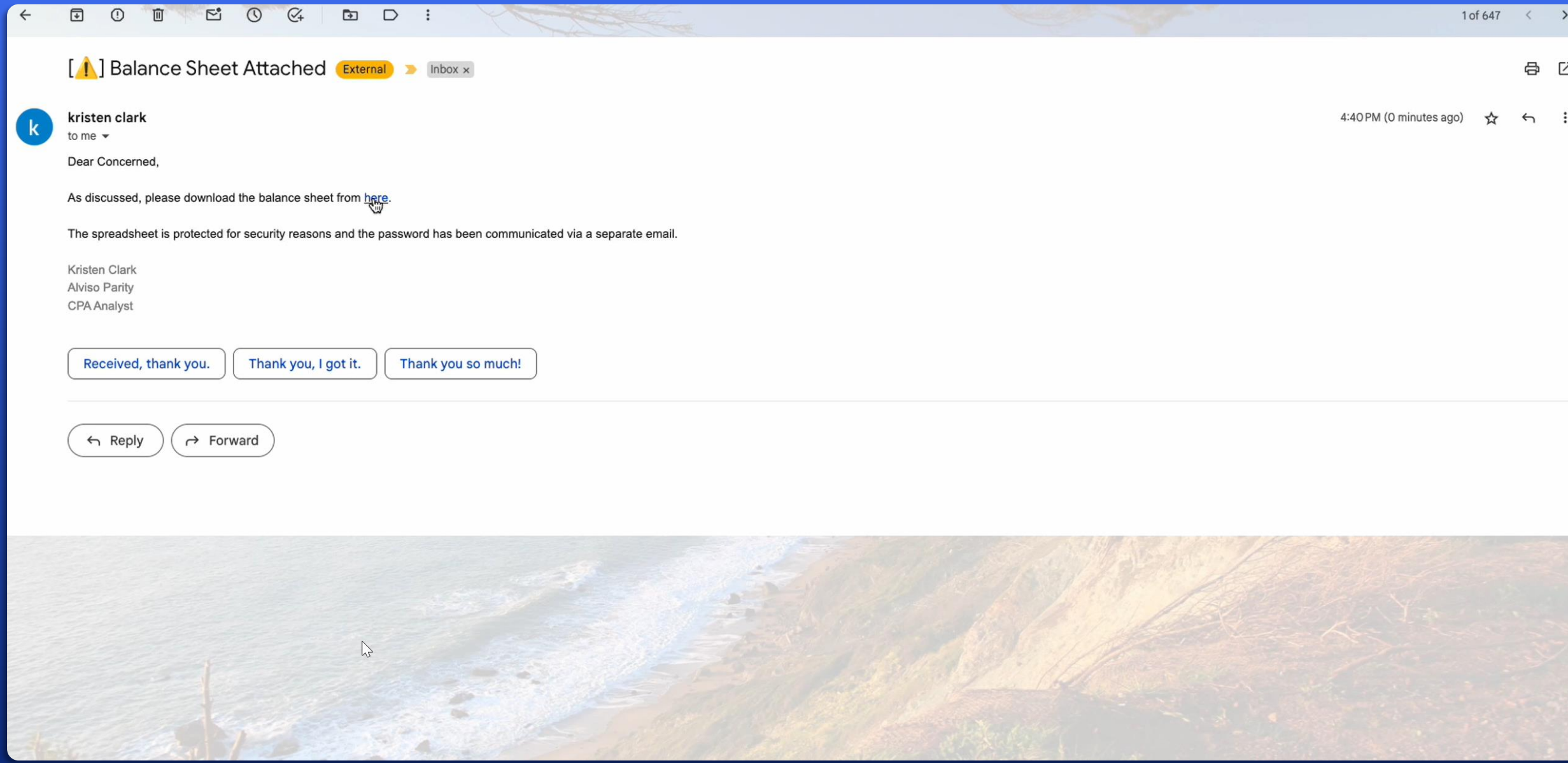
ファイルの分離とCDR
コンテンツの無害化と再構築

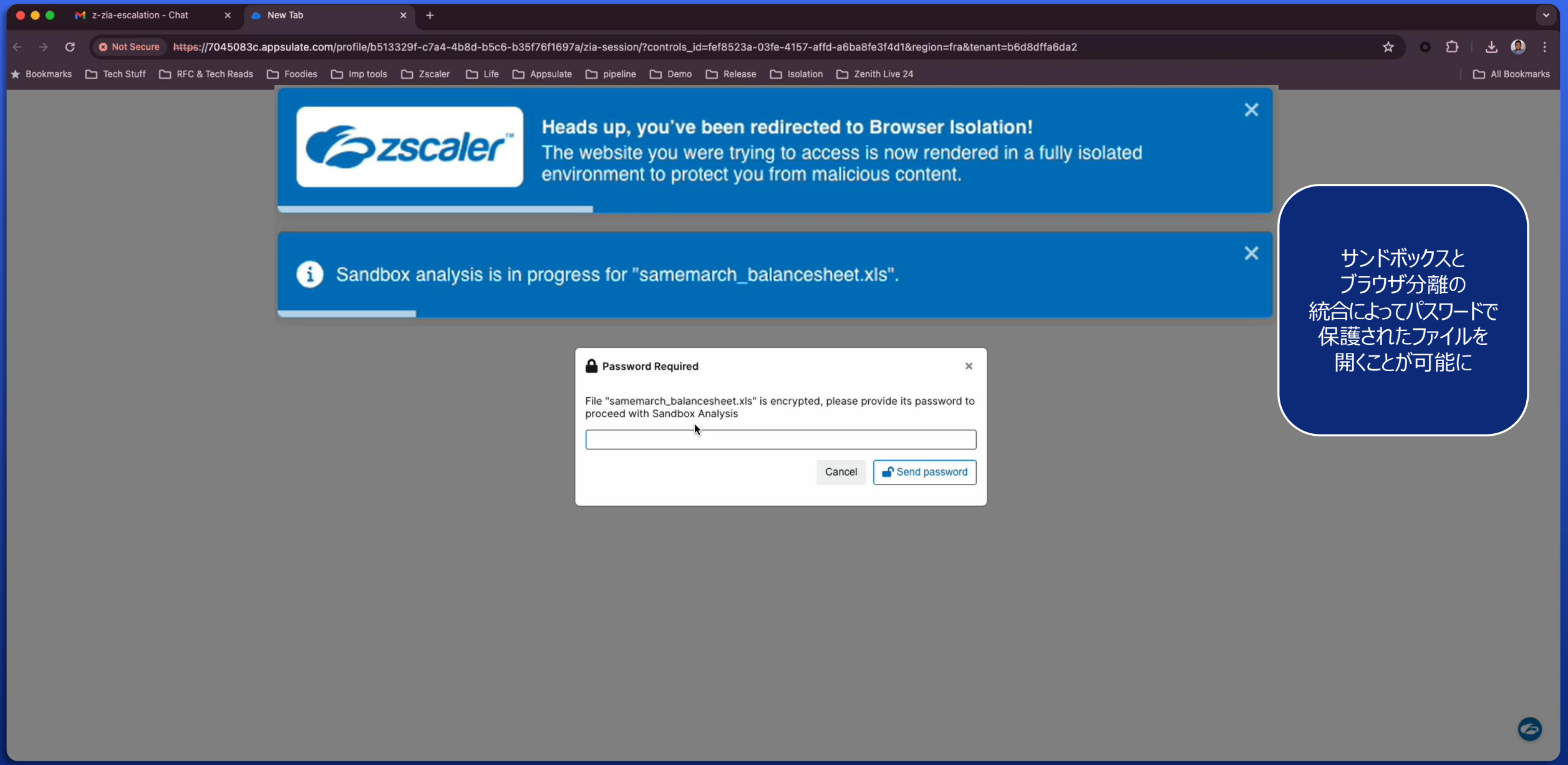
無害化されたオリジナルの
形式でダウンロード
レベル3のCDR

=>

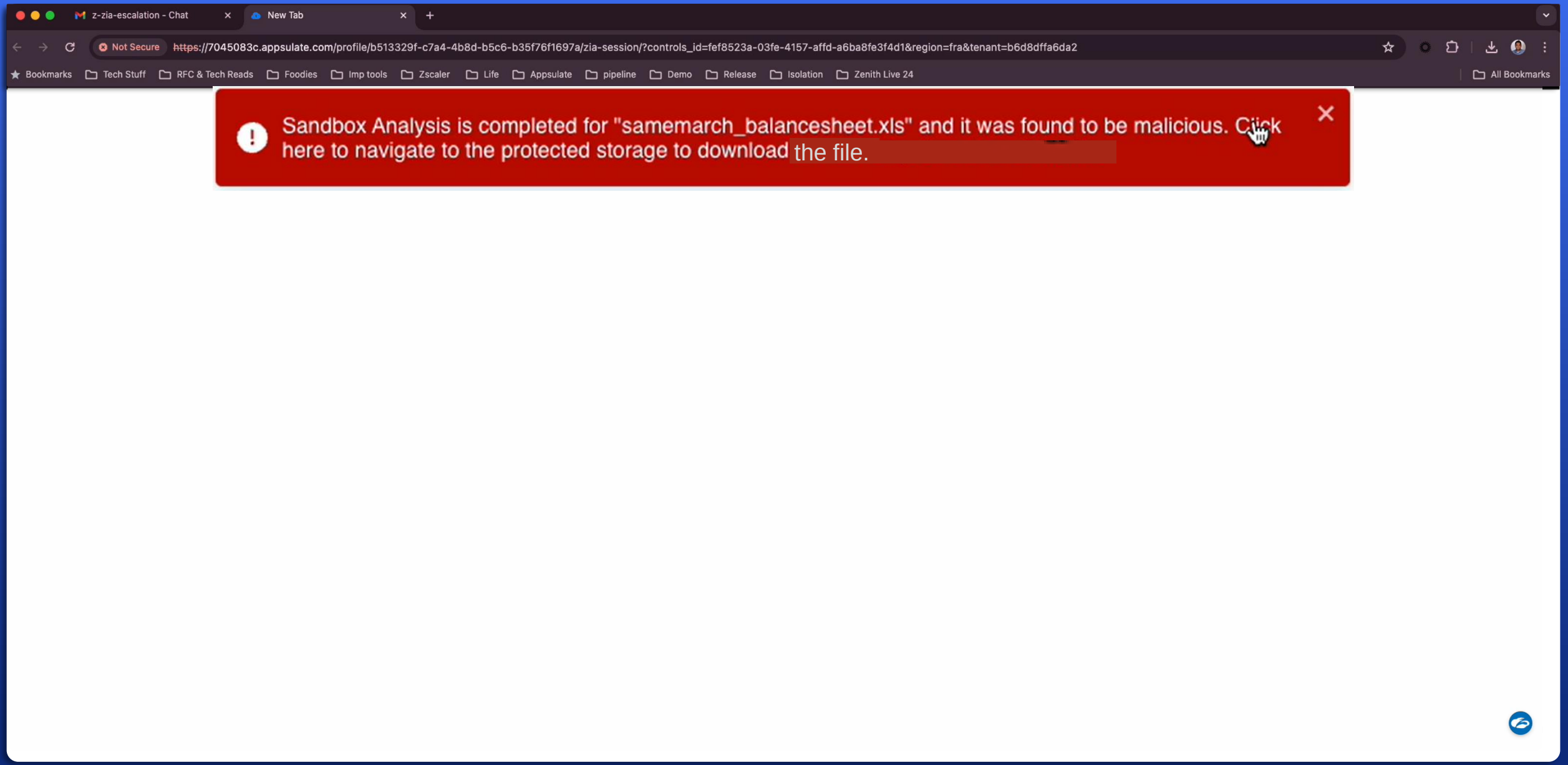
Votiroとのインテグレーションを
通じて提供

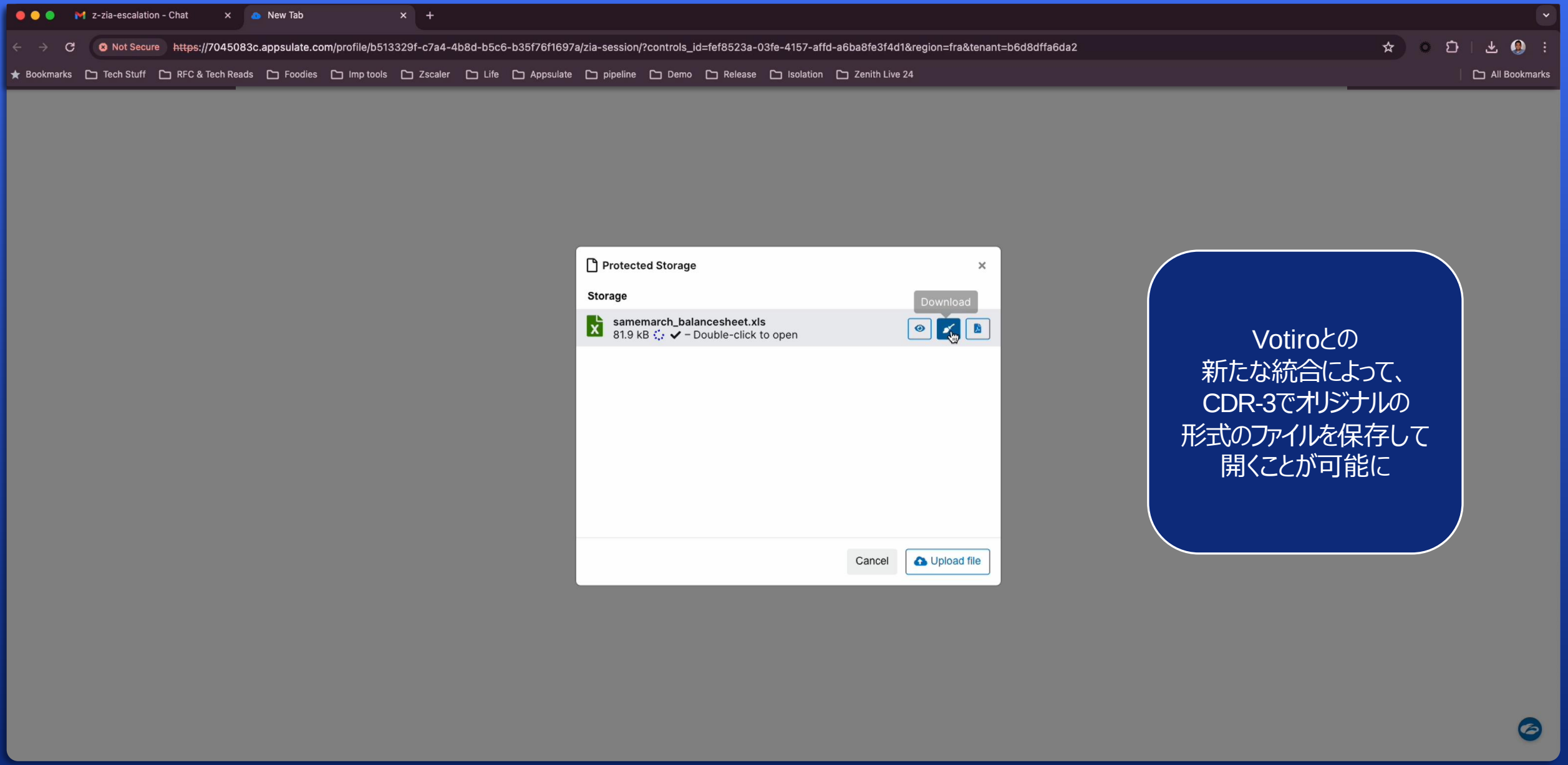



1 of 647
[⚠] Balance Sheet Attached
External
Inbox ×
kristen clark
to me
4:40 PM (0 minutes ago)
Dear Concerned,
As discussed, please download the balance sheet from here.
The spreadsheet is protected for security reasons and the password has been communicated via a separate email.
Kristen Clark
Alviso Parity
CPA Analyst
Received, thank you.
Thank you, I got it.
Thank you so much!
Reply
Forward

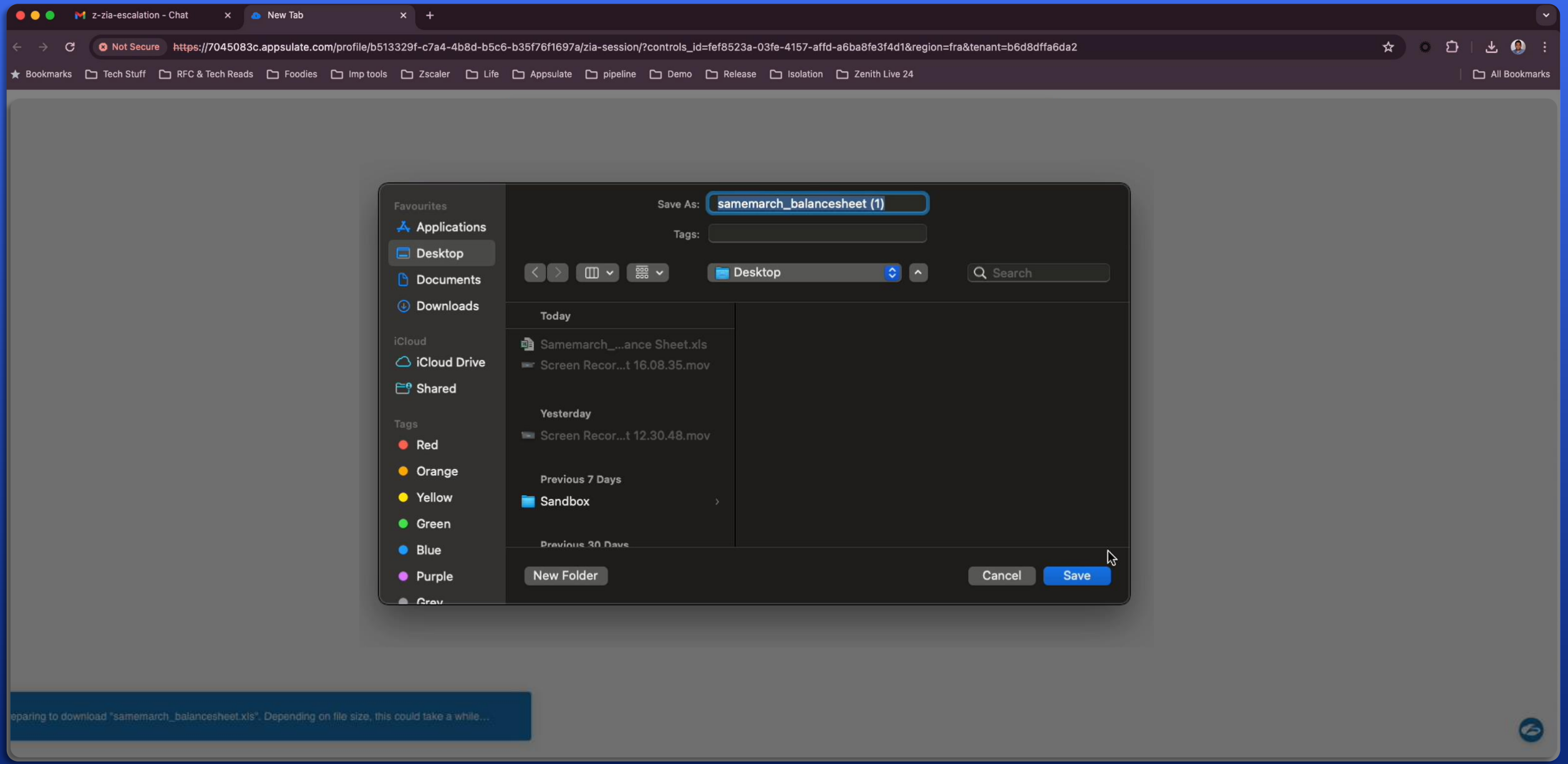


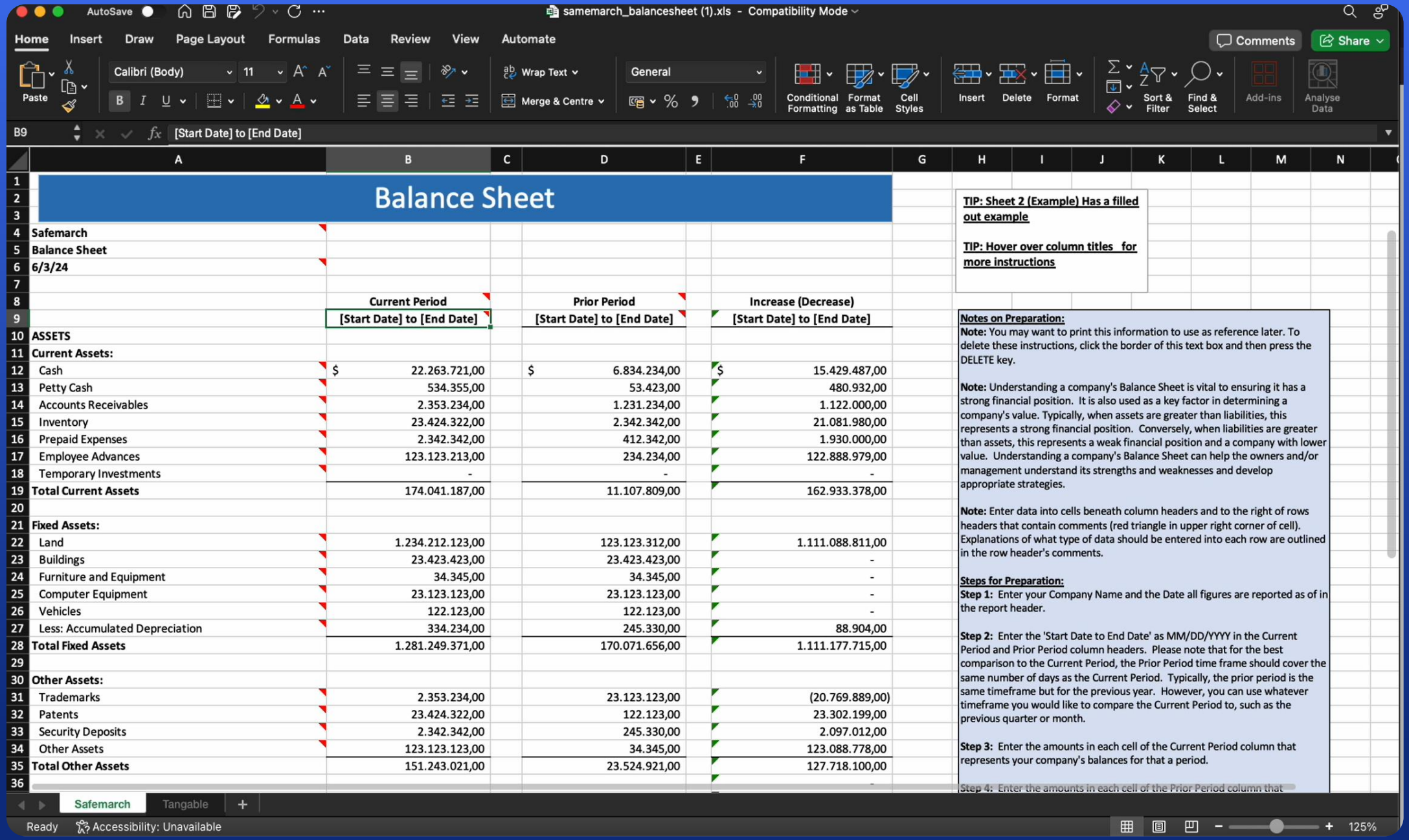
サンドボックスと
ブラウザ分離の
統合によってパスワードで
保護されたファイルを
開くことが可能に


z-zia-escalation - Chat
New Tab
Not Secure
https://7045083c.appsulate.com/profile/b513329f-c7a4-4b8d-b5c6-b35f76f1697a/zia-session/?controls_id=fef8523a-03fe-4157-affd-a6ba8fe3f4d1&region=fra&tenant=b6d8dffa6da2
Bookmarks
Tech Stuff
RFC & Tech Reads
Foodies
Imp tools
Zscaler
Life
Appsulate
pipeline
Demo
Release
Isolation
Zenith Live 24
All Bookmarks
Sandbox Analysis is completed for "samemarch_balancesheet.xls" and it was found to be malicious. Click here to navigate to the protected storage to download the file.



Votiroとの
新たな統合によって、
CDR-3でオリジナルの
形式のファイルを保存して
開くことが可能に

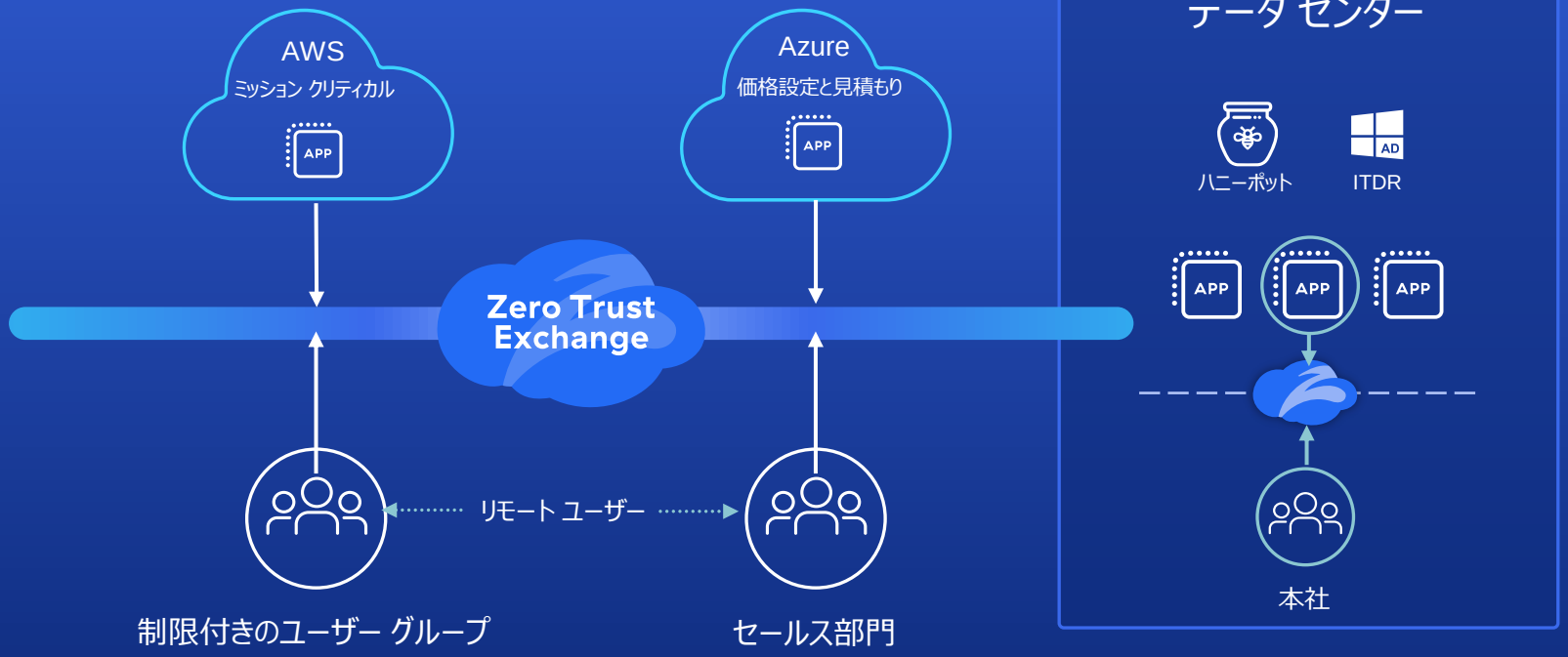

z-zia-escalation - Chat
New Tab
Not Secure
https://7045083c.appsulate.com/profile/b513329f-c7a4-4b8d-b5c6-b35f76f1697a/zia-session/?controls_id=fef8523a-03fe-4157-affd-a6ba8fe3f4d1&region=fra&tenant=b6d8dffa6da2
Bookmarks
Tech Stuff
RFC & Tech Reads
Foodies
Imp tools
Zscaler
Life
Appsulate
pipeline
Demo
Release
Isolation
Zenith Live 24
All Bookmarks
Favourites
Applications
Desktop
Documents
Downloads
iCloud
iCloud Drive
Shared
Tags
Red
Orange
Yellow
Green
Blue
Purple
Grey
Save As:
samemarch_balancesheet (1)
Tags:
Desktop
Search
Today
Samemarch_...ance Sheet.xls
Screen Recor...t 16.08.35.mov
Yesterday
Screen Recor...t 12.30.48.mov
Previous 7 Days
Sandbox
New Folder
Cancel
Save
eparing to download "samemarch_balancesheet.xls". Depending on file size, this could take a while...


samemarch_balancesheet (1).xls - Compatibility Mode
Home Insert Draw Page Layout Formulas Data Review View Automate
Comments Share
B9 [Start Date] to [End Date]
Balance Sheet
Safemarch
Balance Sheet
6/3/24
Current Period [Start Date] to [End Date]
Prior Period [Start Date] to [End Date]
Increase (Decrease) [Start Date] to [End Date]
ASSETS
Current Assets:
Cash $ 22.263.721,00 $ 6.834.234,00 $ 15.429.487,00
Petty Cash 534.355,00 53.423,00 480.932,00
Accounts Receivables 2.353.234,00 1.231.234,00 1.122.000,00
Inventory 23.424.322,00 2.342.342,00 21.081.980,00
Prepaid Expenses 2.342.342,00 412.342,00 1.930.000,00
Employee Advances 123.123.213,00 234.234,00 122.888.979,00
Temporary Investments - - -
Total Current Assets 174.041.187,00 11.107.809,00 162.933.378,00
Fixed Assets:
Land 1.234.212.123,00 123.123.312,00 1.111.088.811,00
Buildings 23.423.423,00 23.423.423,00 -
Furniture and Equipment 34.345,00 34.345,00 -
Computer Equipment 23.123.123,00 23.123.123,00 -
Vehicles 122.123,00 122.123,00 -
Less: Accumulated Depreciation 334.234,00 245.330,00 88.904,00
Total Fixed Assets 1.281.249.371,00 170.071.656,00 1.111.177.715,00
Other Assets:
Trademarks 2.353.234,00 23.123.123,00 (20.769.889,00)
Patents 23.424.322,00 122.123,00 23.302.199,00
Security Deposits 2.342.342,00 245.330,00 2.097.012,00
Other Assets 123.123.123,00 34.345,00 123.088.778,00
Total Other Assets 151.243.021,00 23.524.921,00 127.718.100,00
TIP: Sheet 2 (Example) Has a filled out example
TIP: Hover over column titles for more instructions
Notes on Preparation:
Note: You may want to print this information to use as reference later. To delete these instructions, click the border of this text box and then press the DELETE key.
Note: Understanding a company's Balance Sheet is vital to ensuring it has a strong financial position. It is also used as a key factor in determining a company's value. Typically, when assets are greater than liabilities, this represents a strong financial position. Conversely, when liabilities are greater than assets, this represents a weak financial position and a company with lower value. Understanding a company's Balance Sheet can help the owners and/or management understand its strengths and weaknesses and develop appropriate strategies.
Note: Enter data into cells beneath column headers and to the right of rows headers that contain comments (red triangle in upper right corner of cell). Explanations of what type of data should be entered into each row are outlined in the row header's comments.
Steps for Preparation:
Step 1: Enter your Company Name and the Date all figures are reported as of in the report header.
Step 2: Enter the 'Start Date to End Date' as MM/DD/YYYY in the Current Period and Prior Period column headers. Please note that for the best comparison to the Current Period, the Prior Period time frame should cover the same number of days as the Current Period. Typically, the prior period is the same timeframe but for the previous year. However, you can use whatever timeframe you would like to compare the Current Period to, such as the previous quarter or month.
Step 3: Enter the amounts in each cell of the Current Period column that represents your company's balances for that a period.
Safemarch Tangable
Ready Accessibility: Unavailable
125%

攻撃対象領域の最小化 | 不正侵入の防止 | ラテラル ムーブメントの防止 | 情報漏洩の防止

1 ユーザーとアプリ間のセグメンテーション

AI活用型のポリシー推奨



3 ハニーポットを使用

水平移動する攻撃者をデコイであぶり出し

4 ITDRを実装

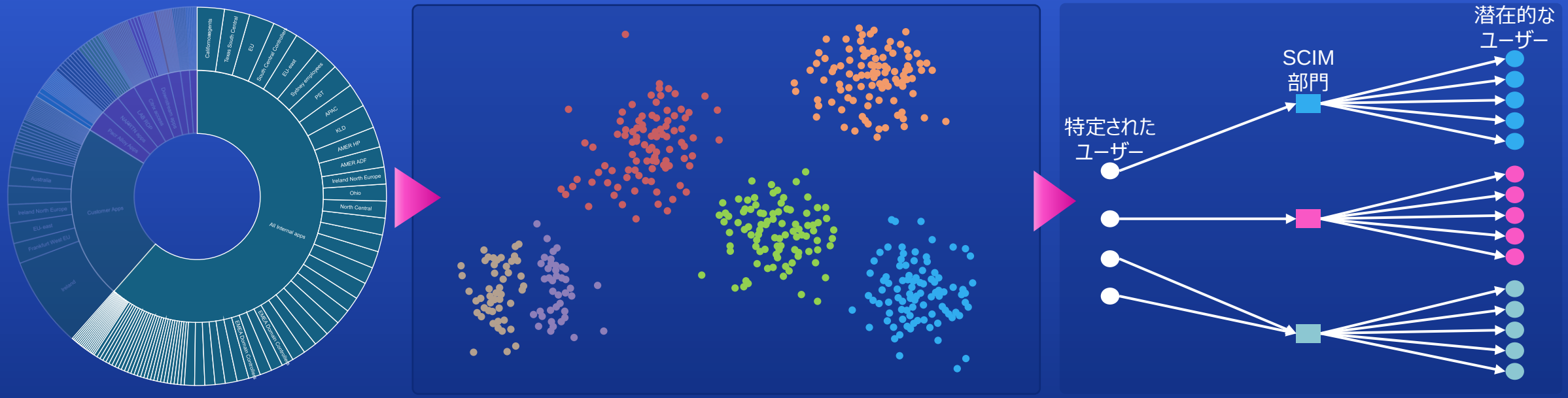
ADの設定ミス、脆弱性、権限昇格を特定

2 オフィスからアプリへのゼロトラスト アクセス

提供開始

インテリジェント アプリ セグメンテーション

AI/MLを活用したセグメンテーションの推奨



分散セグメント クラスターの形成

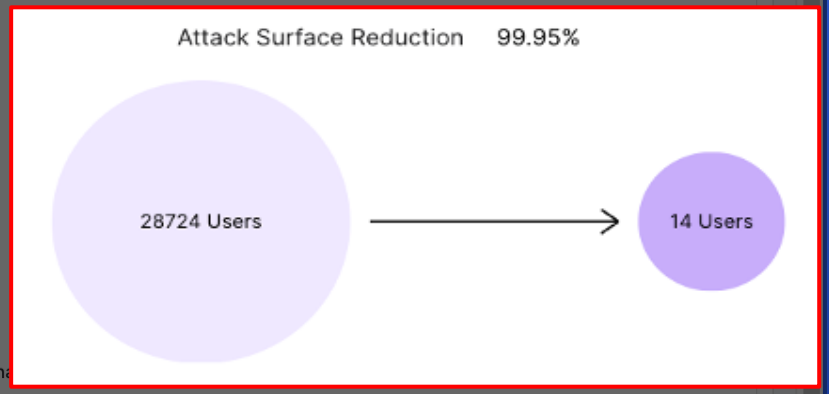
AI/MLを活用したセグメンテーションの推奨

Potential Users	28724
Recommended Users	Existing SCIM Synced Departments irl pcg facilities 14 Users (1 users accessed the recommended applications during the observation period)

Review 6 Policies 7

99.95%

Potential Users	28724
Recommended Users	Existing SCIM Synced Departments irl pcg facilities 14 Users (1 users accessed the recommended applications during the observation period)
Number of Transactions	2
Number of Defined Application Segments	1
TCP Port Ranges	["8003-8003"]
Grouping Reasons	PORTS AND PROTOCOLS SIMILARITY: TCP: 8003
Descriptions	PORTS AND PROTOCOLS SIMILARITY: Consists of Microsoft Endpoint Configuration Mana



Application	Defined Application Segment	Port and Protocol	Server IP
cxtqnv2.test5.zero-trust.cloud	Wildcard Discovery	TCP: 8003 UDP:	10.100.66.4
ckty0n2.test5.zero-trust.cloud	Wildcard Discovery	TCP: 8003 UDP:	10.215.64.224
2hqxhk2.test5.zero-trust.cloud	Wildcard Discovery	TCP: 8003 UDP:	10.10.71.166

UDP:

Next Previous Skip Cancel

Zscaler Identity Protection (ITDR)

アイデンティティの攻撃対象領域を削減するZscaler Identity Protection

89%

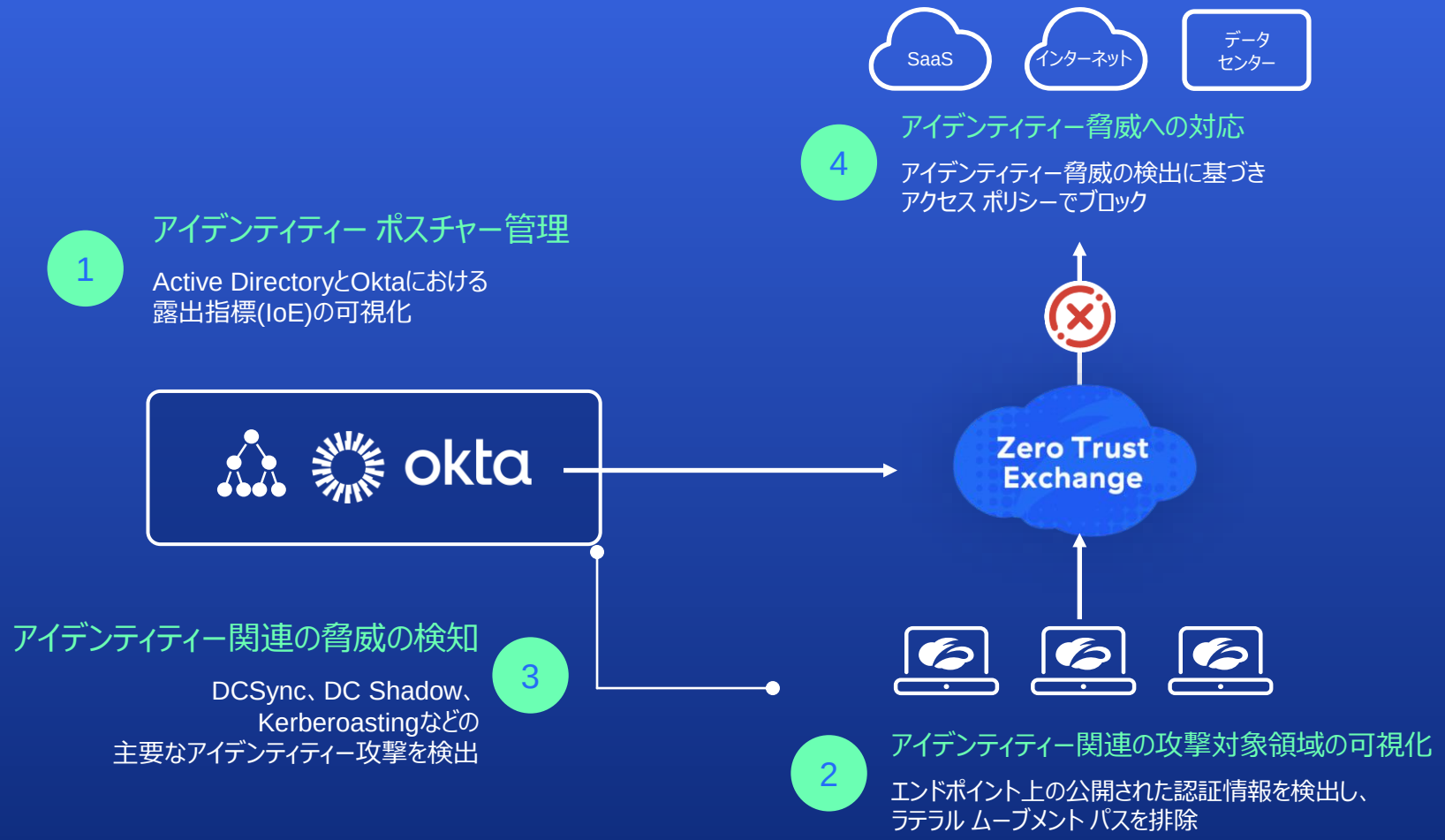
2022年にアイデンティティー攻撃を受けた組織の割合

583%

Kerberoastingのような AD攻撃の増加率

9/10

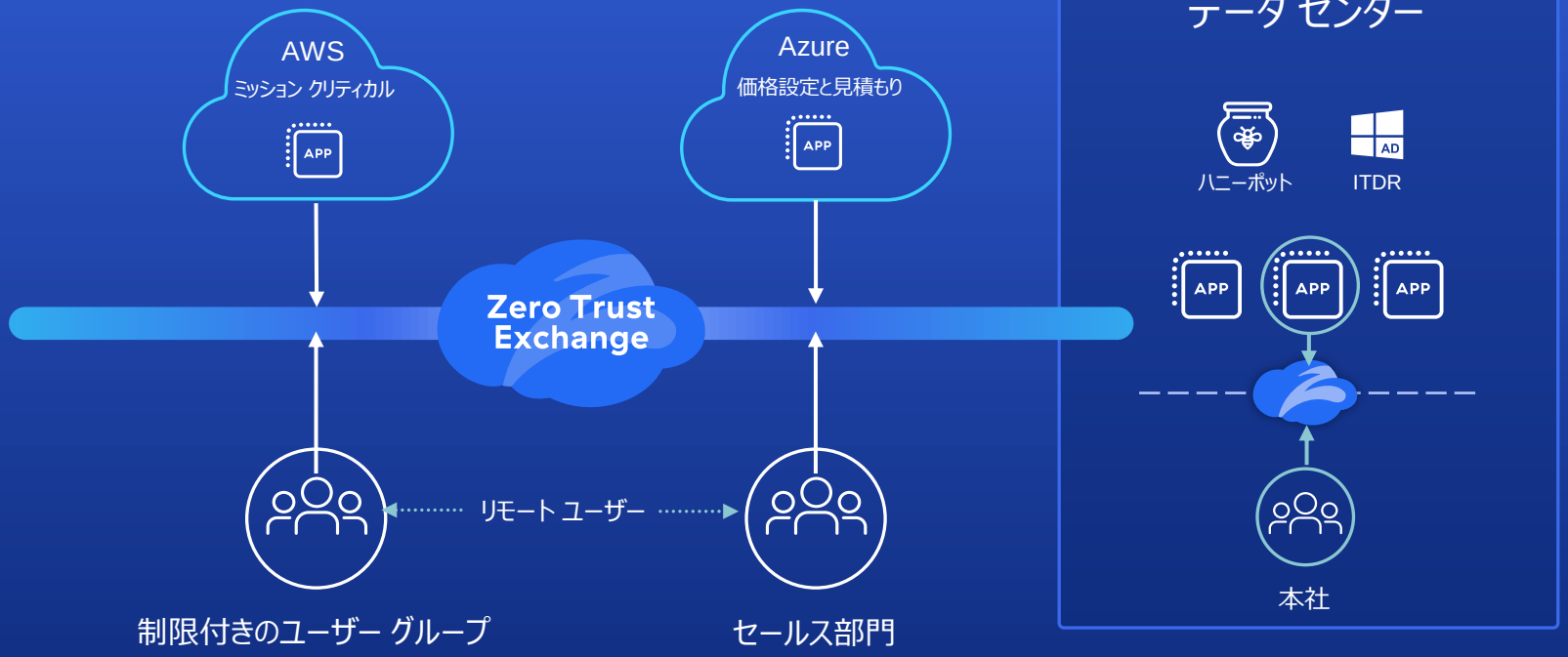
Active Directory/IDPの侵害を伴うランサムウェア攻撃の割合



攻撃対象領域の最小化 | 不正侵入の防止 | ラテラル ムーブメントの防止 | 情報漏洩の防止

1 ユーザーとアプリ間のセグメンテーション

AI活用型のポリシー推奨



3 ハニーポットを使用

水平移動する攻撃者をデコイであぶり出し

4 ITDRを実装

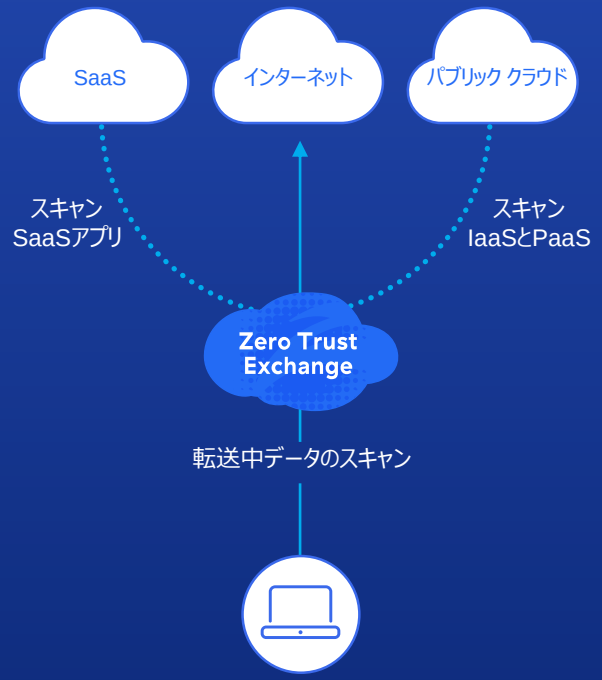
ADの設定ミス、脆弱性、権限昇格を特定

2 オフィスからアプリへのゼロトラスト アクセス

攻撃対象領域の最小化 | 不正侵入の防止 | ラテラル ムーブメントの防止 | **情報漏洩の防止**

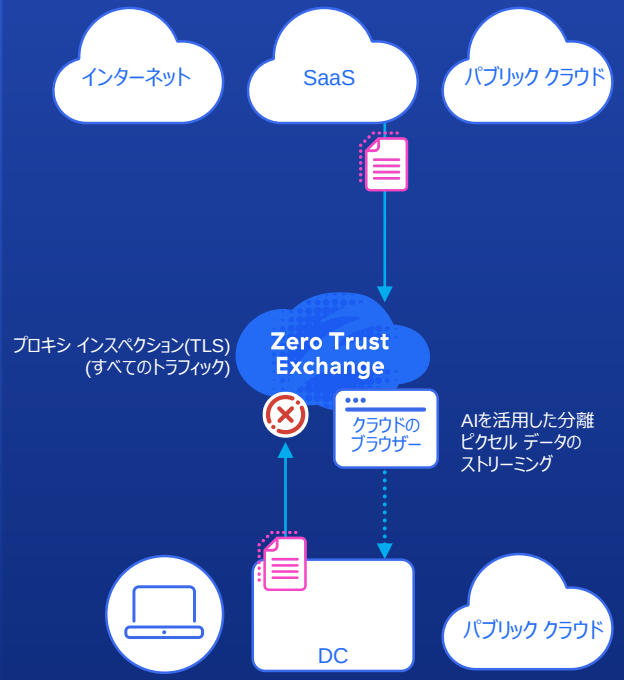
AIを活用したデータ検出

機密データやリスクの高いアプリはないか？



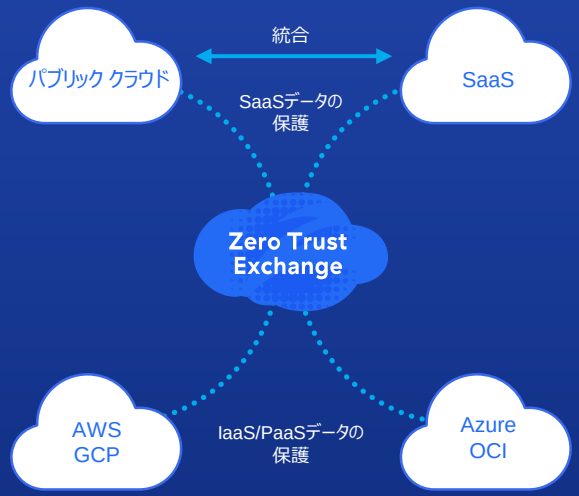
転送中データの保護

すべてのチャネルでデータ漏洩を防止しているか？



保存データの保護

正しく構成されているか？公開されていないか？



Cyber Ratingsによる2024年のSSEテスト

Zscaler:トップクラスの脅威検出効率

zscaler™

AAA

3rd–party SSE
threat protection test

Cyber Ratings .org

CYBER RATINGS.ORG

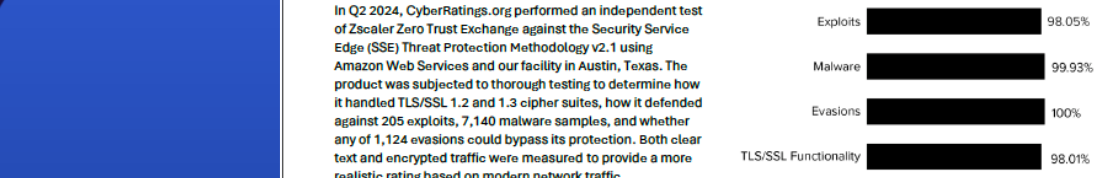
CYBER RATINGS.ORG SSE | 2024

Zscaler Zero Trust Exchange AAA

OVERVIEW

In Q2 2024, CyberRatings.org performed an independent test of Zscaler Zero Trust Exchange against the Security Service Edge (SSE) Threat Protection Methodology v2.1 using Amazon Web Services and our facility in Austin, Texas. The product was subjected to thorough testing to determine how it handled TLS/SSL 1.2 and 1.3 cipher suites, how it defended against 205 exploits, 7,140 malware samples, and whether any of 1,124 evasions could bypass its protection. Both clear text and encrypted traffic were measured to provide a more realistic rating based on modern network traffic.

98.0% PROTECTION RATE



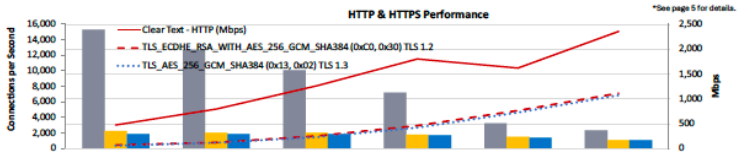
THREAT PREVENTION

Threats:	Blocked	Tested
Exploits	201	205
Malware	7135	7140
Wild Malware – w/o Reputation	6191	6195
Wild Malware – w/ Reputation	944	945
Evasions	1124	1124
HTTP	602	602
HTML	108	108
Malware Evasions	290	290
Java	64	64
Combination	60	60

TLS/SSL DECRYPTION FUNCTIONALITY

Version	Prevalence	Cipher Suites	Results
TLS 1.3	66.51%	(0x13, 0x02)	Supported
TLS 1.2	11.85%	(0xC0, 0x30)	Supported
TLS 1.2	9.26%	(0xC0, 0x2F)	Supported
TLS 1.3	8.07%	(0x13, 0x01)	Supported
TLS 1.2	1.72%	(0xCC, 0xA8)	Not Supported
TLS 1.2	0.68%	(0xC0, 0x28)	Supported
TLS 1.3	0.55%	(0x13, 0x03)	Supported
TLS 1.2	0.42%	(0xC0, 0x2C)	Supported*
TLS 1.2	0.27%	(0xCC, 0xA9)	Not Supported
TLS 1.2	0.20%	(0xC0, 0x2B)	Supported*

THROUGHPUT



HTTP & HTTPS Performance	Clear Text (HTTP)		TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30) TLS 1.2		TLS_AES_256_GCM_SHA384 (0x13, 0x02) TLS 1.3	
Max Connections per Second (CPS)	CPS	Mbps	CPS	Mbps	CPS	Mbps
32,000 CPS	15,330	478	2,246	71	1,899	59
16,000 CPS	12,698	794	2,229	139	1,897	119
8,000 CPS	10,113	1,264	2,224	278	1,857	232
4,000 CPS	7,211	1,803	1,842	461	1,688	422
2,000 CPS	3,242	1,621	1,526	763	1,448	724
1,000 CPS	2,363	2,363	1,112	1,112	1,073	1,073

Zero Trust Exchangeが最高評価のAAAを獲得

回避技術に対する耐性

100%

1124/1124

エクスプロイトの阻止率

98.1%

201/205

実環境に存在するマルウェアの
阻止率

99.9%

7135/7140

全体的なセキュリティの
有効性

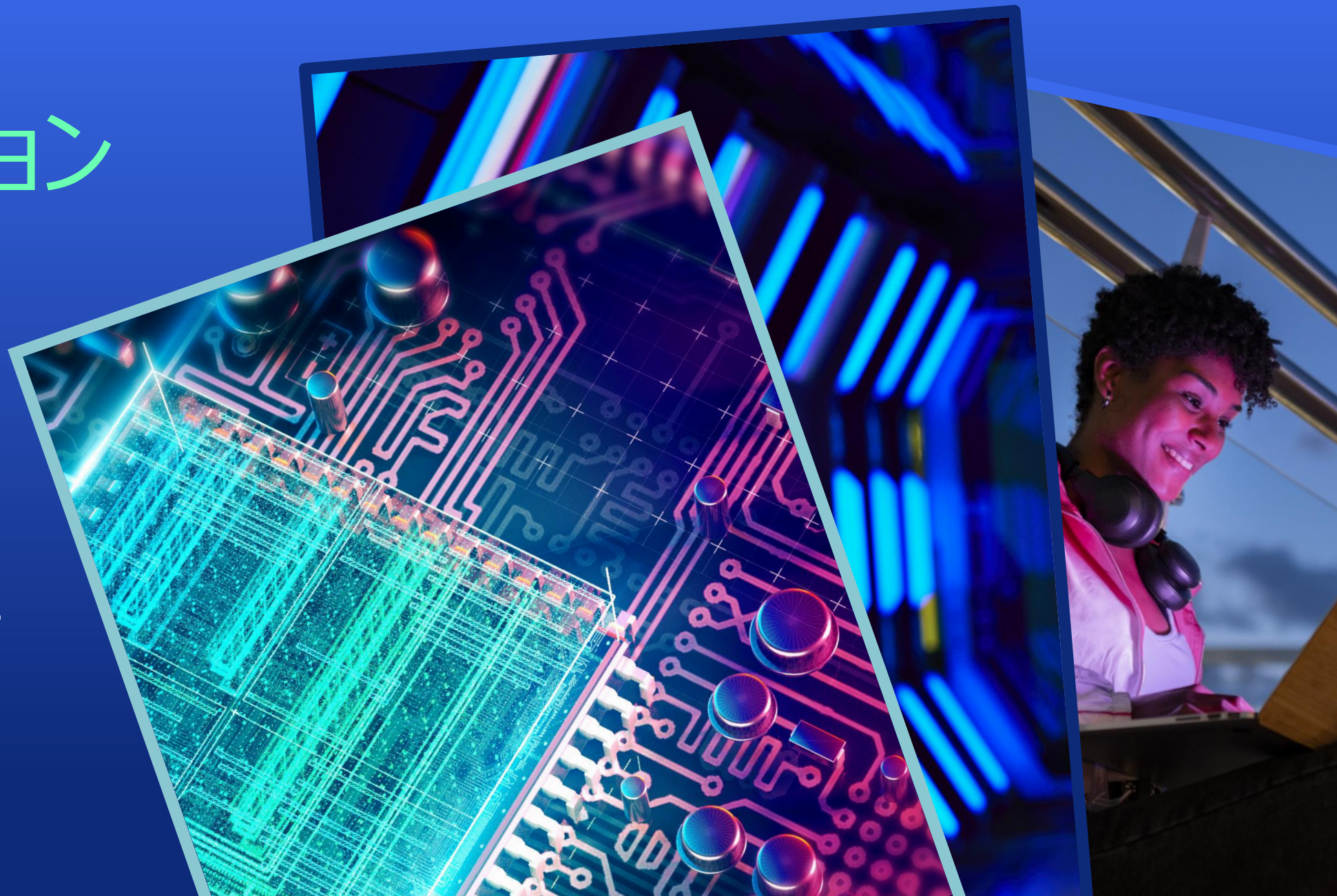
98.0%

CYBER RATINGS.ORG

画期的なイノベーション

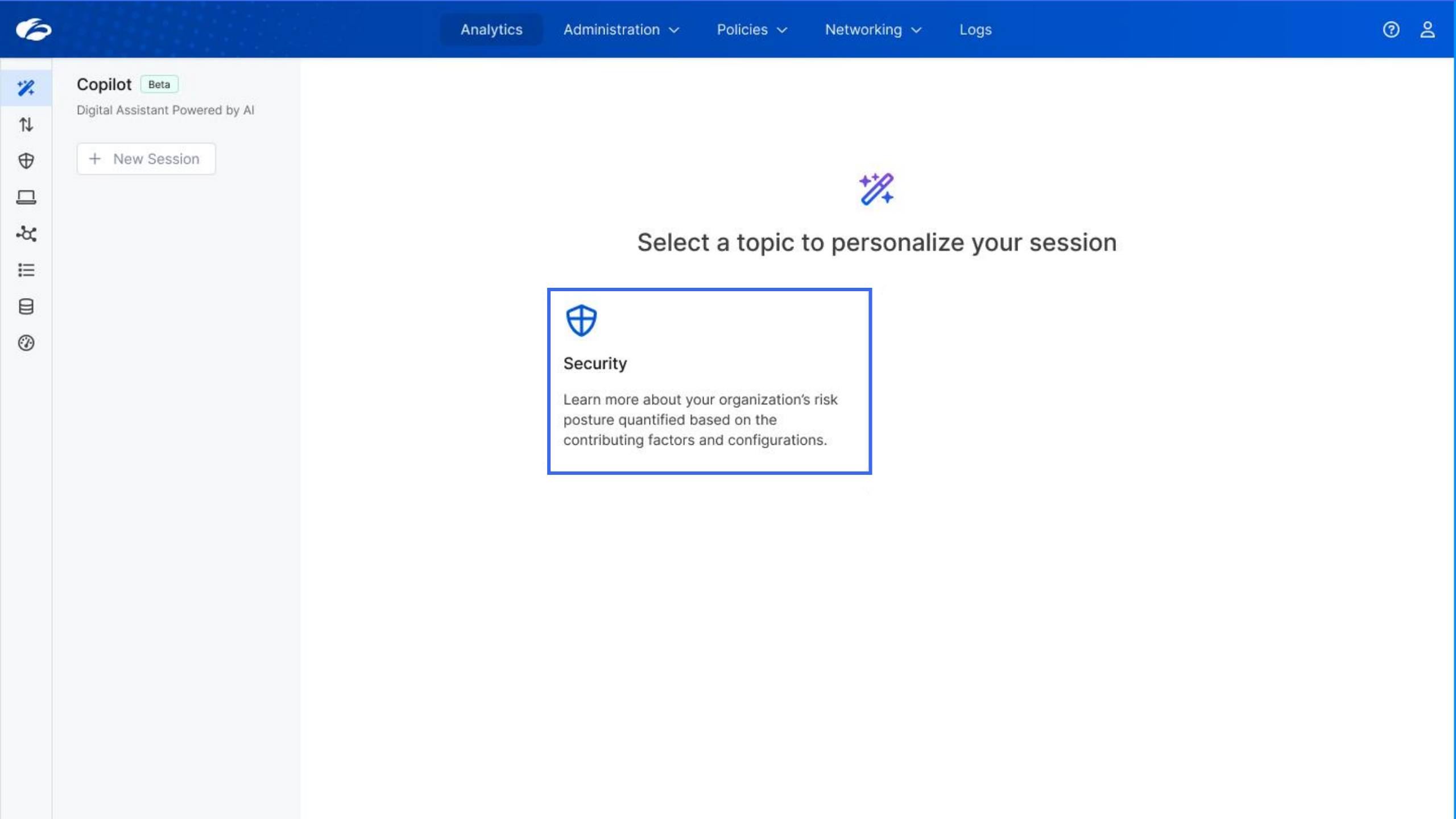
セキュリティCopilot

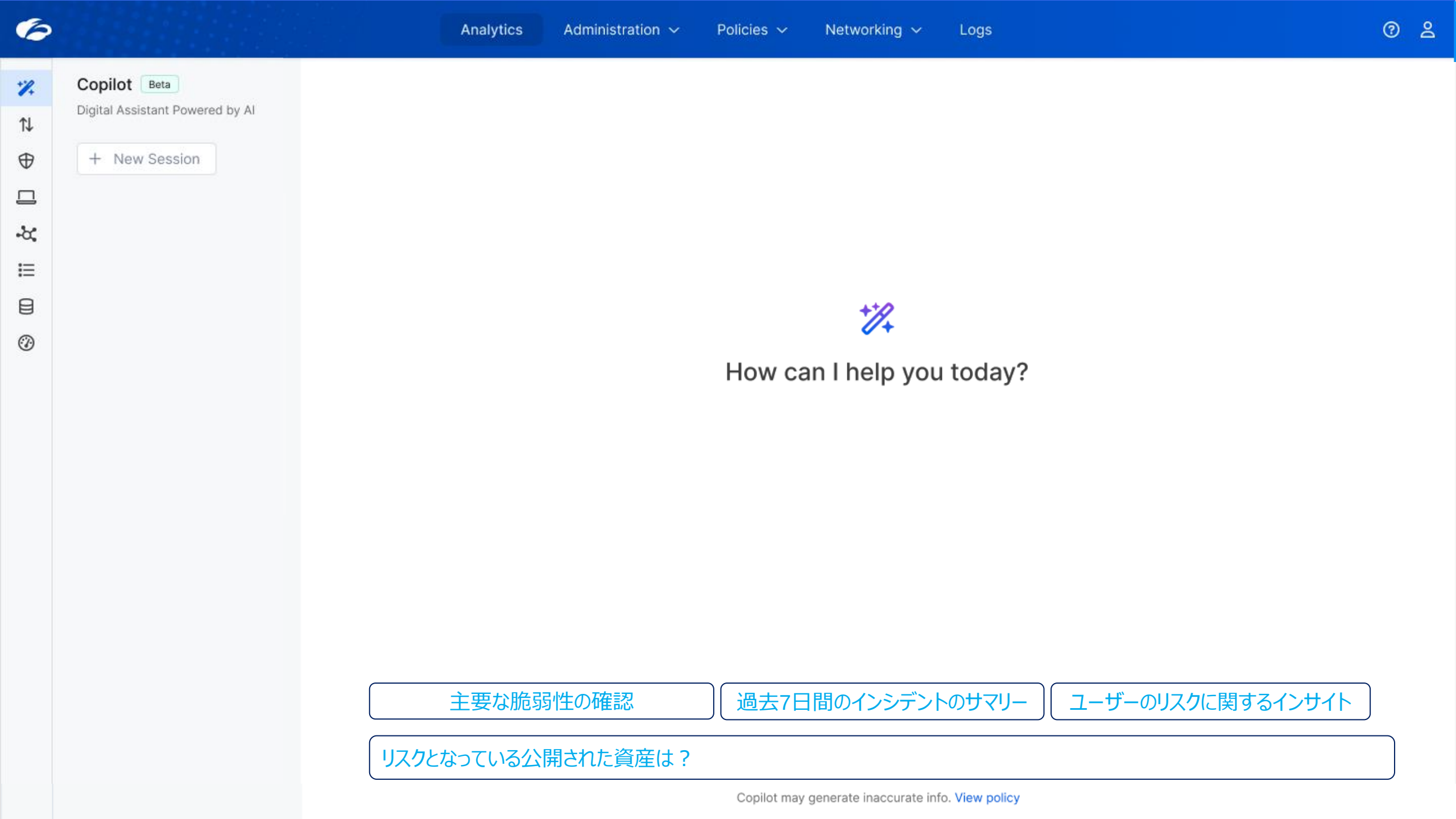
Breach Predictor

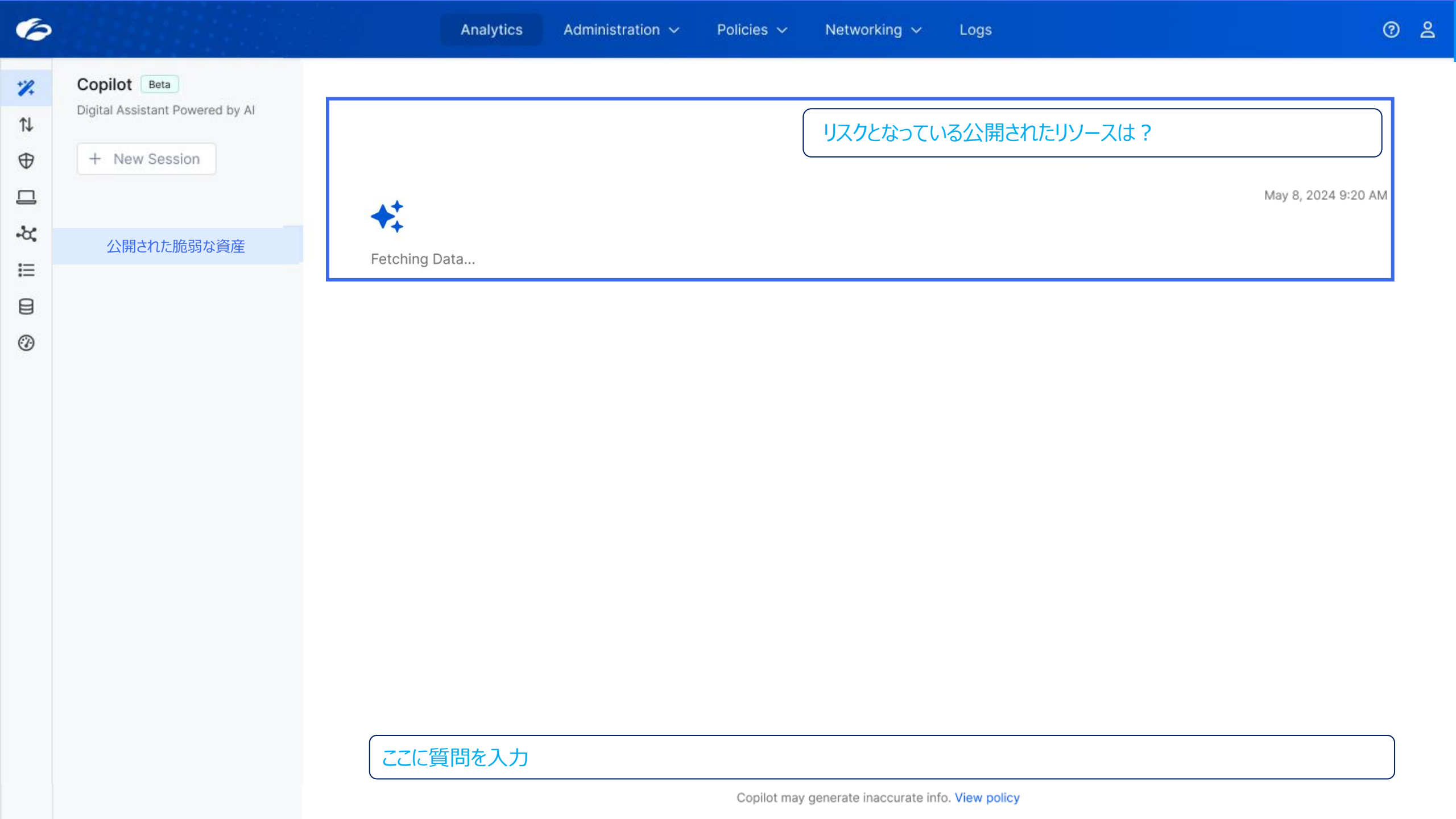


近日
リリース
予定

セキュリティCopilot


Analytics
Administration
Policies
Networking
Logs
Copilot
Beta
Digital Assistant Powered by AI
New Session
Select a topic to personalize your session
Security
Learn more about your organization's risk posture quantified based on the contributing factors and configurations.


Analytics
Administration
Policies
Networking
Logs
Copilot
Beta
Digital Assistant Powered by AI
New Session
How can I help you today?
主要な脆弱性の確認
過去7日間のインシデントのサマリー
ユーザーのリスクに関するインサイト
リスクとなっている公開された資産は？
Copilot may generate inaccurate info. View policy


Analytics
Administration
Policies
Networking
Logs
Copilot
Beta
Digital Assistant Powered by AI
New Session
公開された脆弱な資産
リスクとなっている公開されたリソースは？
May 8, 2024 9:20 AM
Fetching Data...
ここに質問を入力
Copilot may generate inaccurate info. View policy

Copilot Beta

Digital Assistant Powered by AI

+ New Session

Today

公開された脆弱な資産

リスクとなっている公開されたリソースは？

May 8, 2024 9:20 AM

リスク スコアを増大させている公開された資産の一覧を表示します。

Factor	Category	Your Score ↓
Outdated SSL / TLS servers	External Attack Surface	5.00 /5.00
VPN Usage Observed	External Attack Surface	5.00 /5.00
Known Vulnerabilities (CVEs)	External Attack Surface	1.25 /6.25
Exposed Servers (Services Exposed)	External Attack Surface	1.00 /5.00
Public Cloud - Exposed instances	External Attack Surface	1.00 /2.50

Good Okay Poor | User volume drives size of points

May 8, 2024 9:21 AM

リスク要因の詳細を教えて

アジアの詳細を教えて

北米のユーザーについて教えて

ここに質問を入力

Copilot Beta

Digital Assistant Powered by AI

+ New Session

Today

公開された脆弱な資産

公開されたサーバーのリスクの修復方法を教えて

May 8, 2024 9:20 AM

承知しました。公開されたサーバーのリスクの修復に役立つ情報を表示します。

May 8, 2024 9:21 AM

公開された資産を名前空間別に教えて

欧州の詳細を教えて

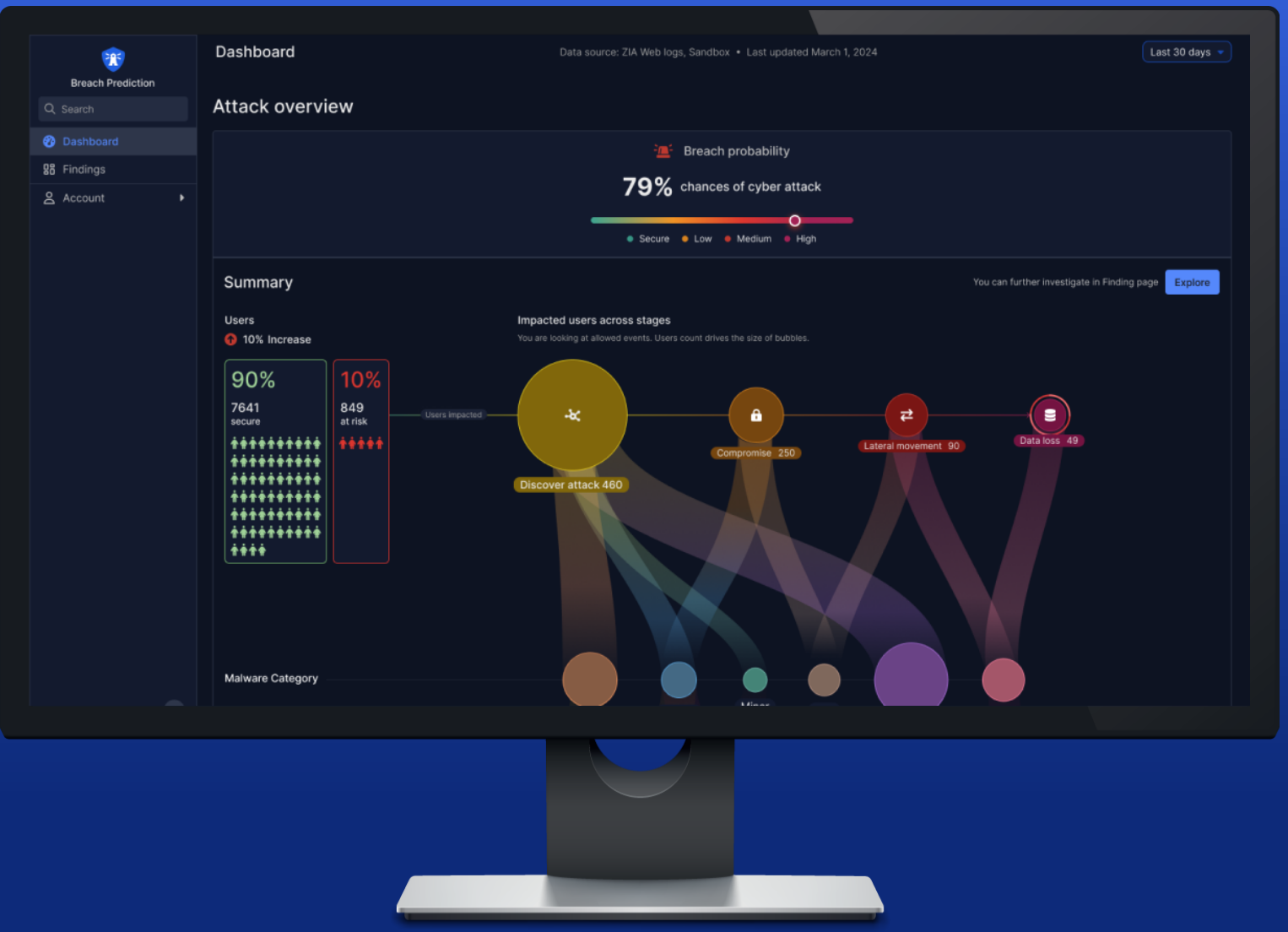
経時的な傾向を教えて

公開されたサーバーのリスクの修復方法を教えて

近日
リリース
予定

Breach Predictor

Breach Predictor とは？



攻撃アクティビティの特定とトラッキング

MITER TTPへの自動的なマッピング

攻撃パスの可視化

侵害ユーザの特定から攻撃遷移の可視化

AI駆動による攻撃予測と阻止

能動的セキュリティ対策

Dashboard

Data source: ZIA Web logs, Sandbox • Last updated May 25, 2024

Last 30 days

Attack overview

Breach probability

79.83% Breach probability

Secure · Low · Medium · High

Summary

You can further investigate in Finding page Explore

Users

500% Increase

97%
156
secure

3%
5
at risk

Impacted users across stages

Users count drives the size of bubbles

Impacted user

Discover attack 0

Compromise 5

Lateral movement 5

Data loss 5

Malware Category

Infostealer/RAT

Breach Prediction

- Dashboard
- Findings
- Account

Dashboard

Data source: ZIA Web logs, Sandbox • Last updated May 25, 2024

Last 30 days

Attack overview

Breach probability

79.83% Breach probability

Secure · Low · Medium · High

Summary

You can further investigate in Finding page Explore

Users

500% increase

97%
156
secure

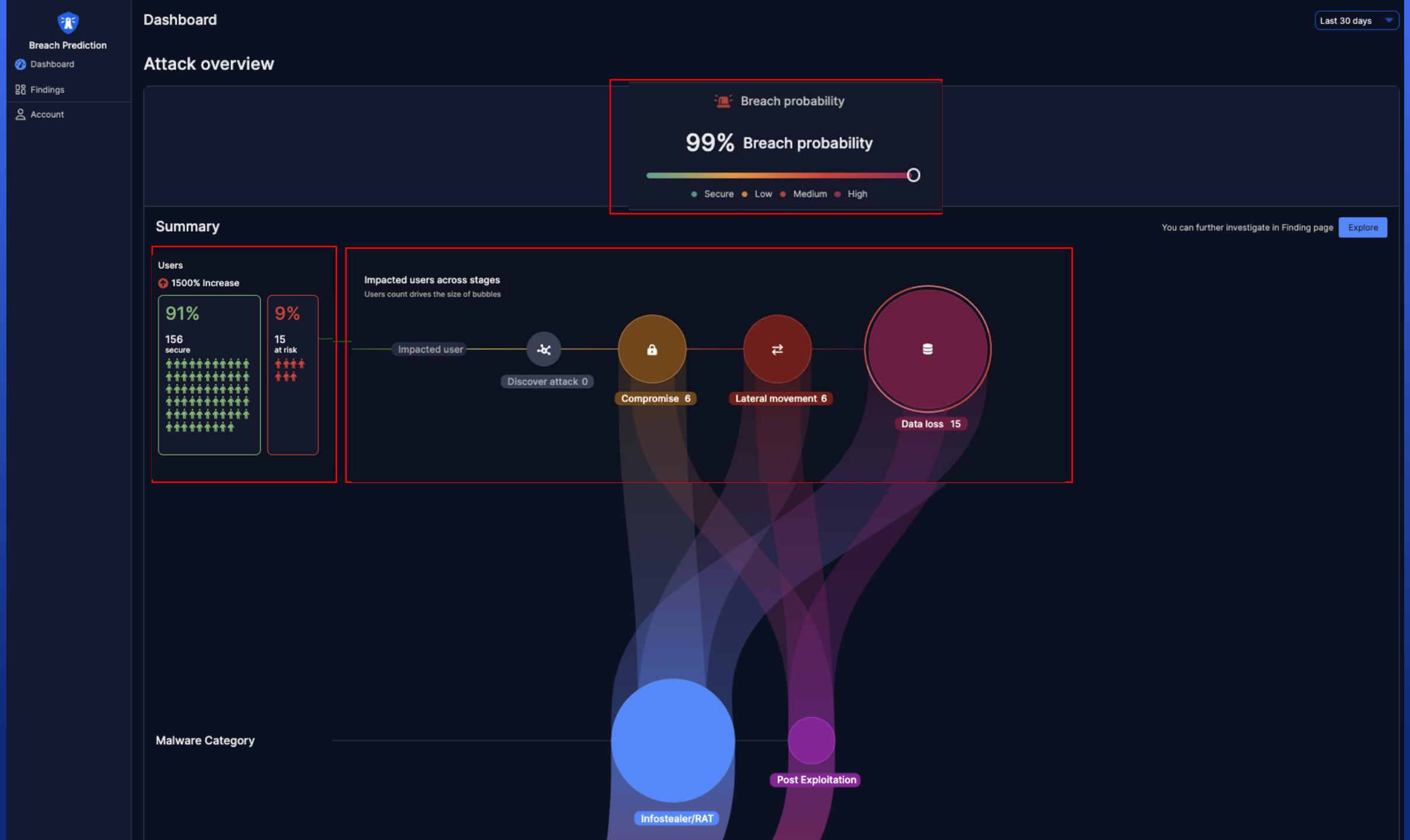
3%
5
at risk

sers across stages
ives the size of bubbles

acted user

Malware Category

Infostealer/RAT


Breach Prediction
Dashboard
Findings
Account
Dashboard
Last 30 days
Attack overview
Breach probability
99% Breach probability
Secure
Low
Medium
High
Summary
You can further investigate in Finding page
Explore
Users
1500% Increase
91%
156
secure
9%
15
at risk
Impacted users across stages
Users count drives the size of bubbles
Impacted user
Discover attack 0
Compromise 6
Lateral movement 6
Data loss 15
Malware Category
Infostealer/RAT
Post Exploitation

Breach Prediction

- Dashboard
- Findings
- Account

Dashboard

Last 30 days

Attack overview

Breach probability

99% Breach probability

Secure · Low · Medium · High

Summary

You can further investigate in Finding page — Explore

Users

1500% Increase

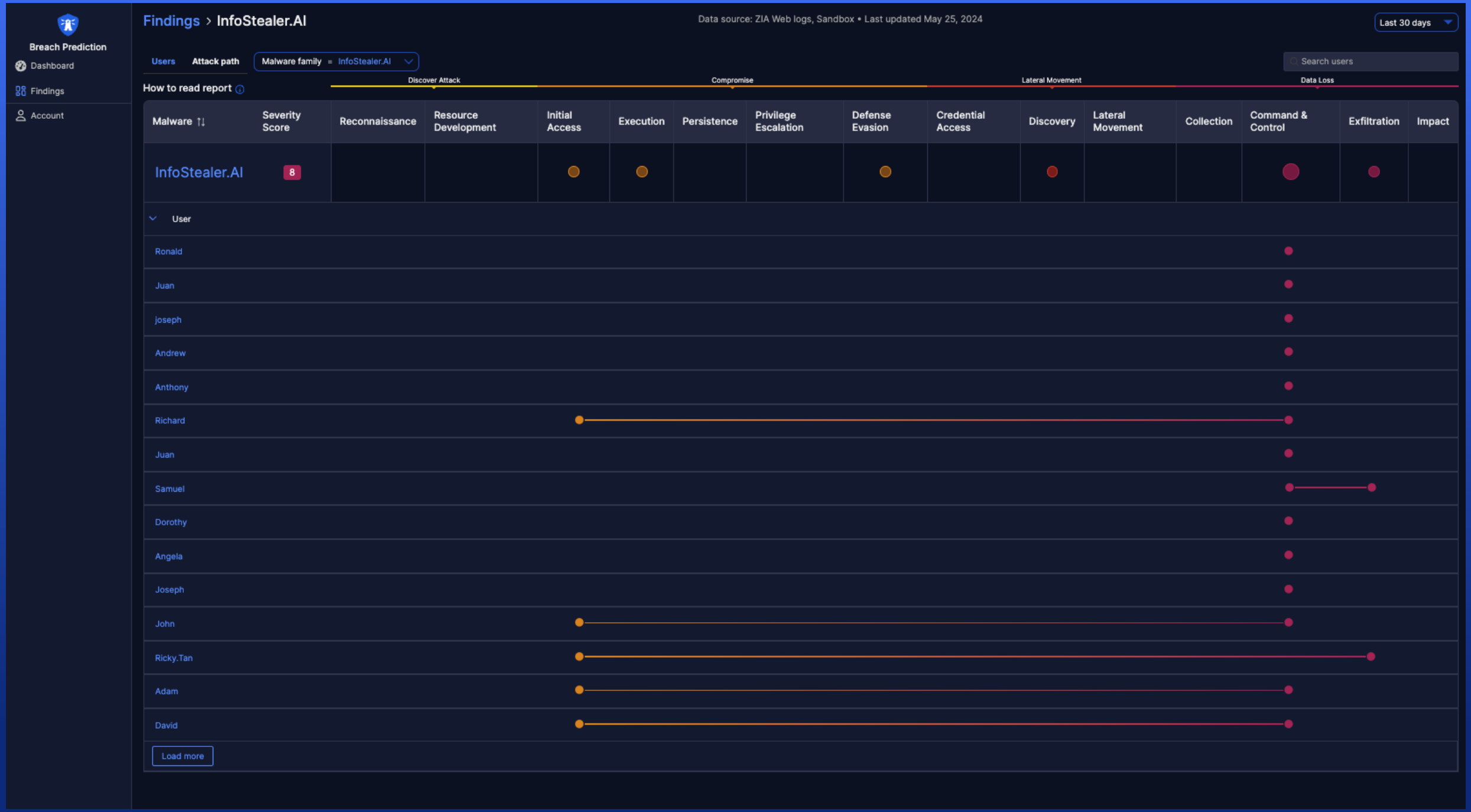
91%
156
secure

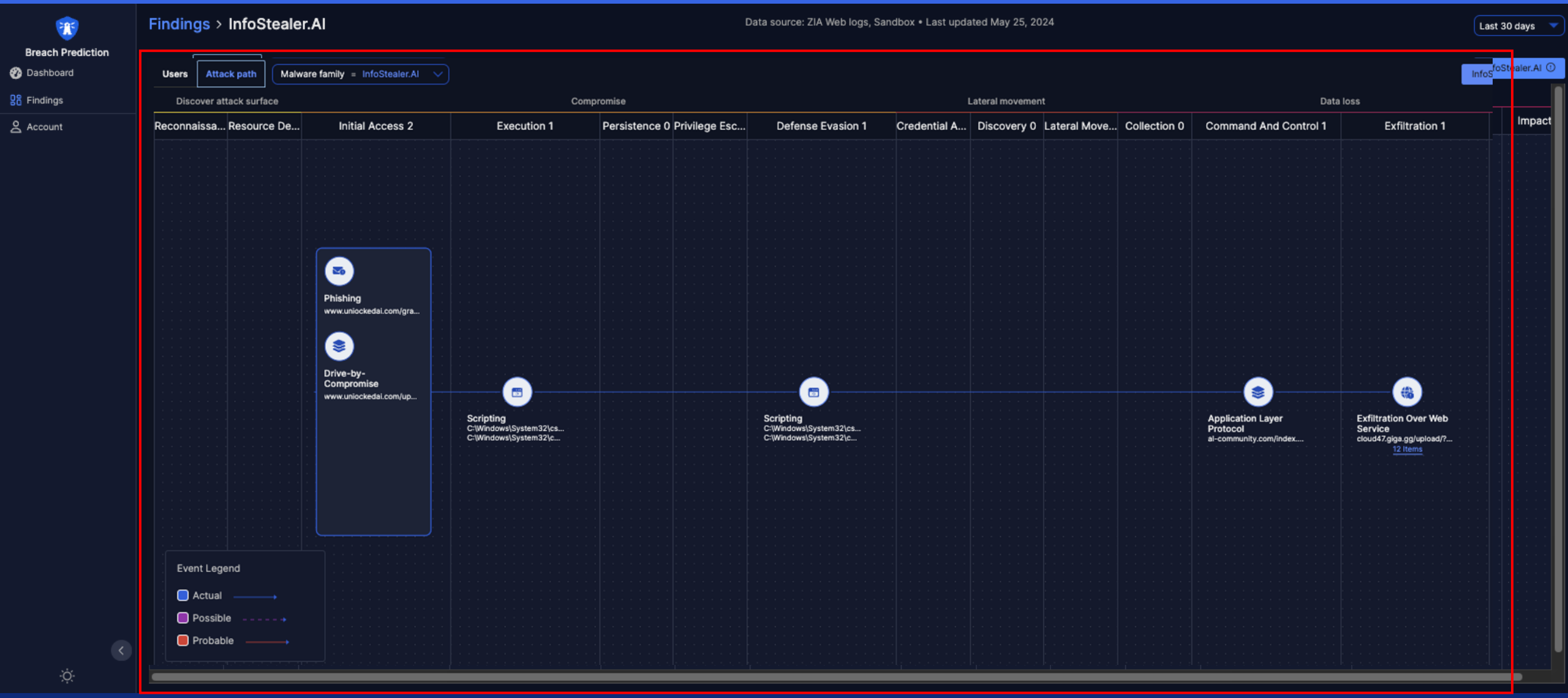
9%
15
at risk

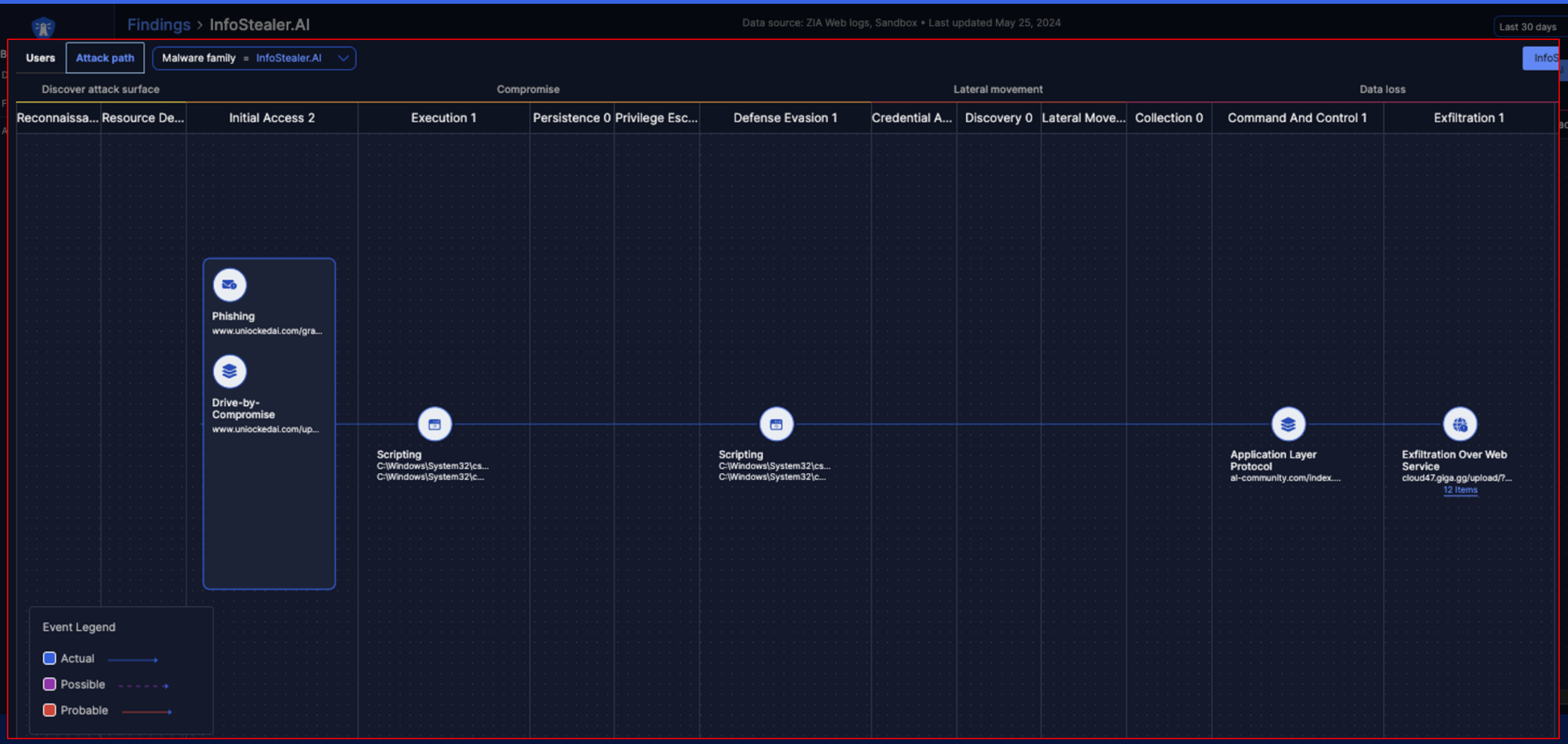
Impacted users across stages

Users count drives the size of bubbles

Malware Category


Breach Prediction
Dashboard
Findings
Account
Findings > InfoStealer.AI
Data source: ZIA Web logs, Sandbox • Last updated May 25, 2024
Last 30 days
Users
Attack path
Malware family = InfoStealer.AI
Search users
How to read report
Discover Attack
Compromise
Lateral Movement
Data Loss
Malware
Severity Score
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact
InfoStealer.AI
8
User
Ronald
Juan
joseph
Andrew
Anthony
Richard
Juan
Samuel
Dorothy
Angela
Joseph
John
Ricky.Tan
Adam
David
Load more


Breach Prediction
Dashboard
Findings
Account
Findings > InfoStealer.AI
Data source: ZIA Web logs, Sandbox • Last updated May 25, 2024
Last 30 days
Users
Attack path
Malware family = InfoStealer.AI
Discover attack surface
Compromise
Lateral movement
Data loss
Reconnaissa...
Resource De...
Initial Access 2
Execution 1
Persistence 0
Privilege Esc...
Defense Evasion 1
Credential A...
Discovery 0
Lateral Move...
Collection 0
Command And Control 1
Exfiltration 1
Impact
Phishing
www.uniockedai.com/gra...
Drive-by-Compromise
www.uniockedai.com/up...
Scripting
C:\Windows\System32\cs...
C:\Windows\System32\c...
Scripting
C:\Windows\System32\cs...
C:\Windows\System32\c...
Application Layer Protocol
ai-community.com/index....
Exfiltration Over Web Service
cloud47.giga.gg/upload/?...
12 items
Event Legend
Actual
Possible
Probable


Findings > InfoStealer.AI
Data source: ZIA Web logs, Sandbox • Last updated May 25, 2024
Last 30 days
Users
Attack path
Malware family = InfoStealer.AI
Discover attack surface
Compromise
Lateral movement
Data loss
Reconnaissa...
Resource De...
Initial Access 2
Execution 1
Persistence 0
Privilege Esc...
Defense Evasion 1
Credential A...
Discovery 0
Lateral Move...
Collection 0
Command And Control 1
Exfiltration 1
Phishing
www.uniockedai.com/gra...
Drive-by-Compromise
www.uniockedai.com/up...
Scripting
C:\Windows\System32\cs...
C:\Windows\System32\c...
Scripting
C:\Windows\System32\cs...
C:\Windows\System32\c...
Application Layer Protocol
ai-community.com/index....
Exfiltration Over Web Service
cloud47.giga.gg/upload/?...
12 Items
Event Legend
Actual
Possible
Probable

おわりに

1	2	3	4
攻撃させない	**侵入させない**	**拡散させない**	**漏らさない**
アプリをZero Trust Exchangeの背後に隠して不可視化	リスクの高いインターネットの接続先に対する脅威対策・分離を実装	ユーザーとアプリ間のセグメンテーションを実装	未承認および未分類の接続先へのデータ転送を制限

- サイバーセキュリティ対策に終わりはなく(ないはず)、今後も**検討事項は増加**する
- 刻一刻と変化するサイバー空間にポイントソリューションで立ち向かうのは**片手落ちと疲弊を招く。**
- 従来の適用範囲にとどまらず、**面・プラットフォームで対策が重要**

ZenithLive24 | zscaler™