MWS 2022 ポストミーティング

BlackHat USA 2022・DEF CON 30 参加報告

～海外実務系カンファレンスのすすめ～

石川 朝久（東京海上ホールディングス株式会社）

自己紹介：石川　朝久（いしかわ　ともひさ）

- **所属　：東京海上ホールディングス株式会社　IT企画部　リスク管理グループ**
- **専門　：不正アクセス技術・インシデント対応・セキュリティ運用・グローバルセキュリティ戦略 etc.**
- **資格　：**博士（工学）, CISSP, CSSLP, CISA, CISM, CDPSE, CFE, PMP, 情報処理安全確保支援士, AWS Security, GIACs
- **経歴　：**
  - 2009.04 – 2019.03　　：某セキュリティ企業
    - 脆弱性診断・侵入テスト（Red Team）・インシデント対応・脆弱性管理・セキュア開発、セキュリティ教育 etc.
    - １年間、米国金融機関セキュリティチームに所属した経験あり
  - 2019.04 – 現在　　：東京海上ホールディングス株式会社
    - CSIRT運用・脅威インテリジェンス分析・グローバルセキュリティ戦略・国内外グループ企業のセキュリティ支援 etc.
- **対外活動（抜粋）：**
  - SANSFIRE 2011 Speaker（2011）
  - DEFCON 24 SE Village Speaker (2016)
  - Internet Week 2018 - 2020 (2018-2020)
  - IPA 情報処理技術者試験委員・情報処理安全確保支援士試験委員（2018~）
  - IPA 「10大脅威執筆者会」メンバー（2010～2014, 2019~）
  - オライリー社『インテリジェンス駆動型インシデントレスポンス』翻訳（2018）
  - オライリー社『初めてのマルウェア解析』翻訳（2020）
  - オライリー社『詳解　インシデントレスポンス』翻訳（2022）
  - オライリー社『マスタリング Ghidra』監訳（2022）
  - 技術評論社　『脅威インテリジェンスの教科書』執筆（2022）

本日お伝えしたいこと

テーマ：海外セキュリティカンファレンスの参加報告＋α

お伝えしたいこと：

- サイバーセキュリティのカンファレンス（Black Hat USA・DEF CON）へ参加したのでその参加報告と注目すべきセキュリティトレンドについて、CSS2022の内容を発展させてお話をします。

アジェンダ：

1. **大会概要**
2. **Black Hat USA詳細**
3. **注目すべきセキュリティトレンド**

注意：

- 帰国時PCR検査で陽性になり、DEF CON参加は途中で取りやめたため、Black Hatのセッションを中心に発表します。
- 本内容は、全て講演者個人の見解を含んでおり、所属企業、部門、その他所属組織の見解を代表するものではありません。
- 製品名・ベンダー名・スクリプトなどが登場した場合、利用については各組織にて検証・判断をお願いします。

1. はじめに（大会概要）

BlackHat USA 2022概要

＜開催概要＞

- 場所・時間：Mandalay Bay @ Las Vegas・August 10 – 11
- 111か国から3万人以上が参加（In-Person：17,400人・Online : 15,488 人以上）
- 日本からの参加者は（体感で）１００名～１５０名程度
- 参加費が高額（約2500ドル）

＜Black Hat の歴史・特徴＞

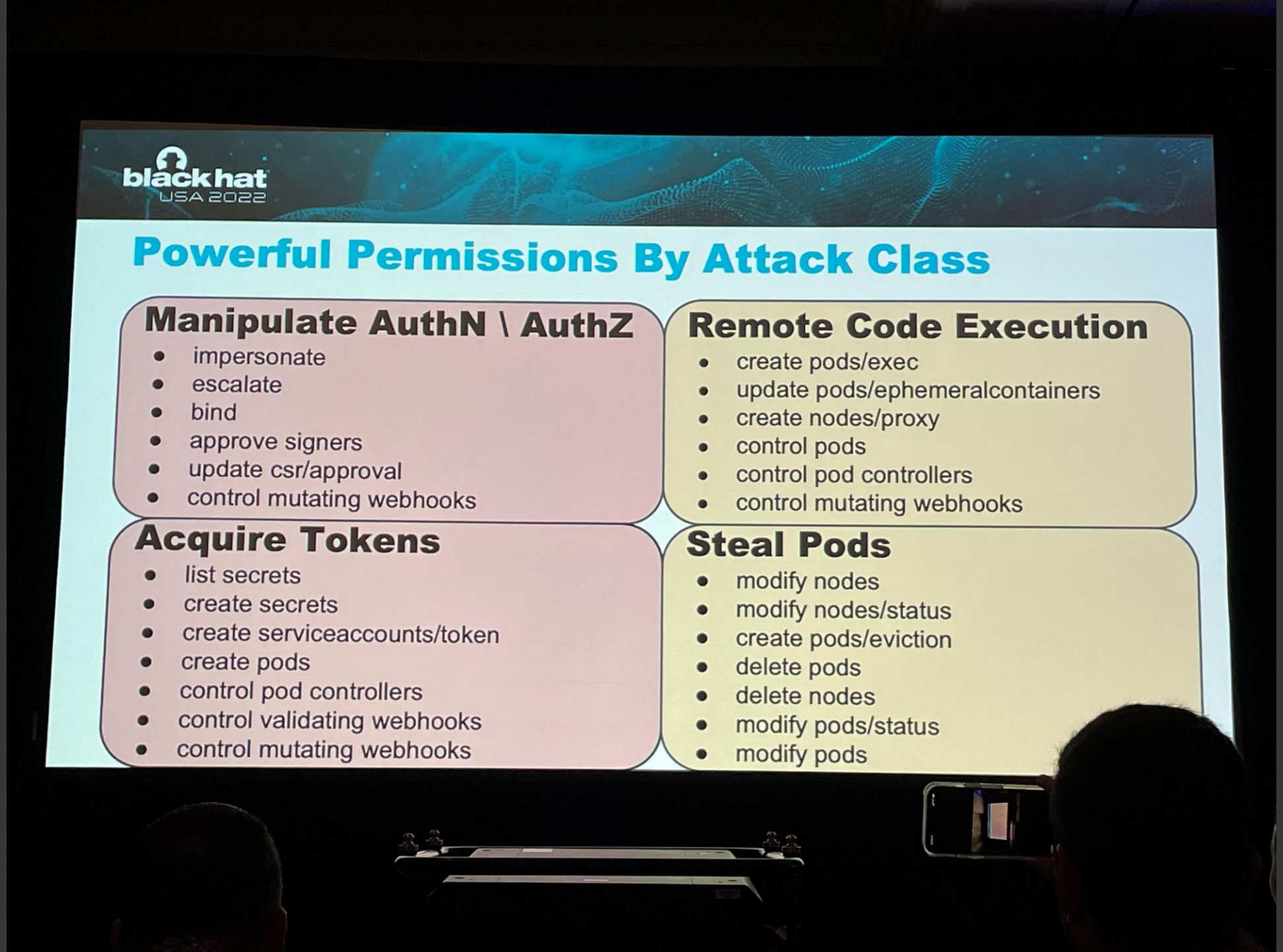
- 1997年より開催されたカンファレンス
  - のちに紹介するDEF CONの方が実は歴史が長い（DEF CON 5と同時開催）
  - 但し、創設者はBlackHatとDEF CONともにJeff Moss氏
  - 現在では、企業向けカンファレンスとしての立ち位置を確立（for Security Professionals）

- 特徴としては、最新の研究動向が発表される（実務系 > 学術系）
- 企業ブースにて、最新のトレンドやスタートアップがもたらす新しい製品動向・トレンドなどをキャッチアップするのに重要な場所となる。

参考：https://www.businesswire.com/news/home/20220819005347/en/Black-Hat-USA-2022-Closes-on-a-Record-Breaking-Event-in-Las-Vegas-Online


Essentials
SUPPLIES · SUNDRIES · GIFTS
BUSINESS HALL
blackha


MANDALAY BAY
LAS VEGAS


black hat
USA 2022
Powerful Permissions By Attack Class
Manipulate AuthN \ AuthZ
impersonate
escalate
bind
approve signers
update csr/approval
control mutating webhooks
Remote Code Execution
create pods/exec
update pods/ephemeralcontainers
create nodes/proxy
control pods
control pod controllers
control mutating webhooks
Acquire Tokens
list secrets
create secrets
create serviceaccounts/token
create pods
control pod controllers
control validating webhooks
control mutating webhooks
Steal Pods
modify nodes
modify nodes/status
create pods/eviction
delete pods
delete nodes
modify pods/status
modify pods

DEF CON 30 概要

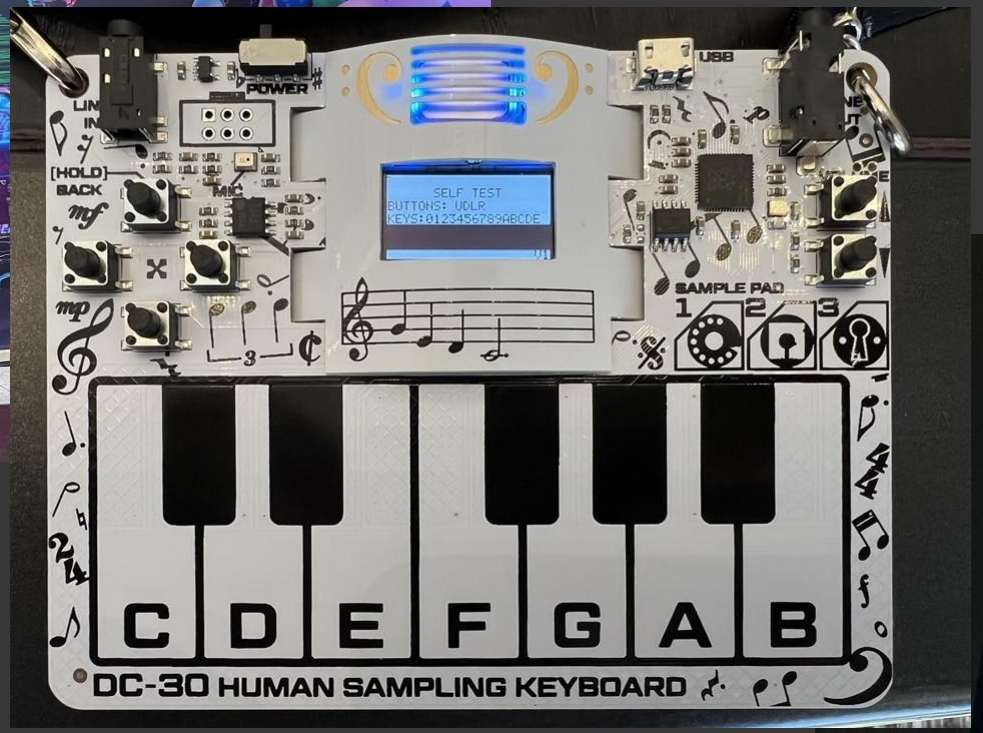
＜開催概要＞

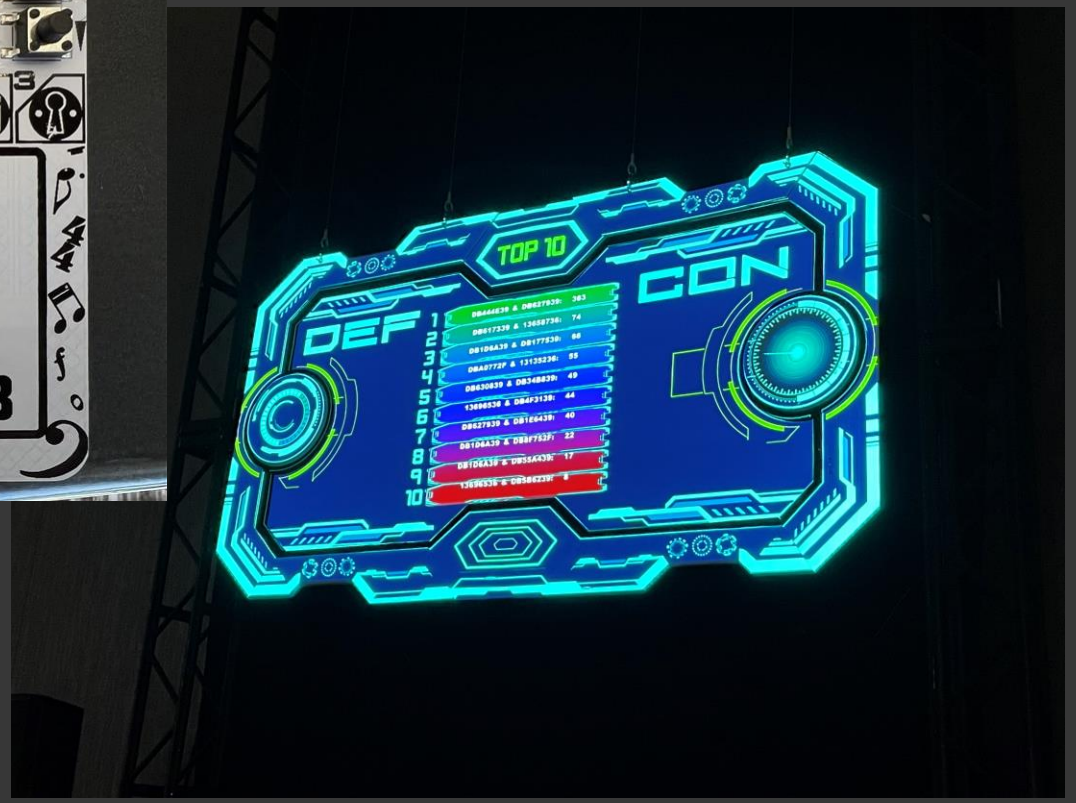
- 場所： Caesars Forum + Flamingo, Harrah's and Linq convention centers @ Las Vegas
- 日時： August 12 – 14
- 同様に、2.5万人以上が参加といわれている
- 参加費（$360）

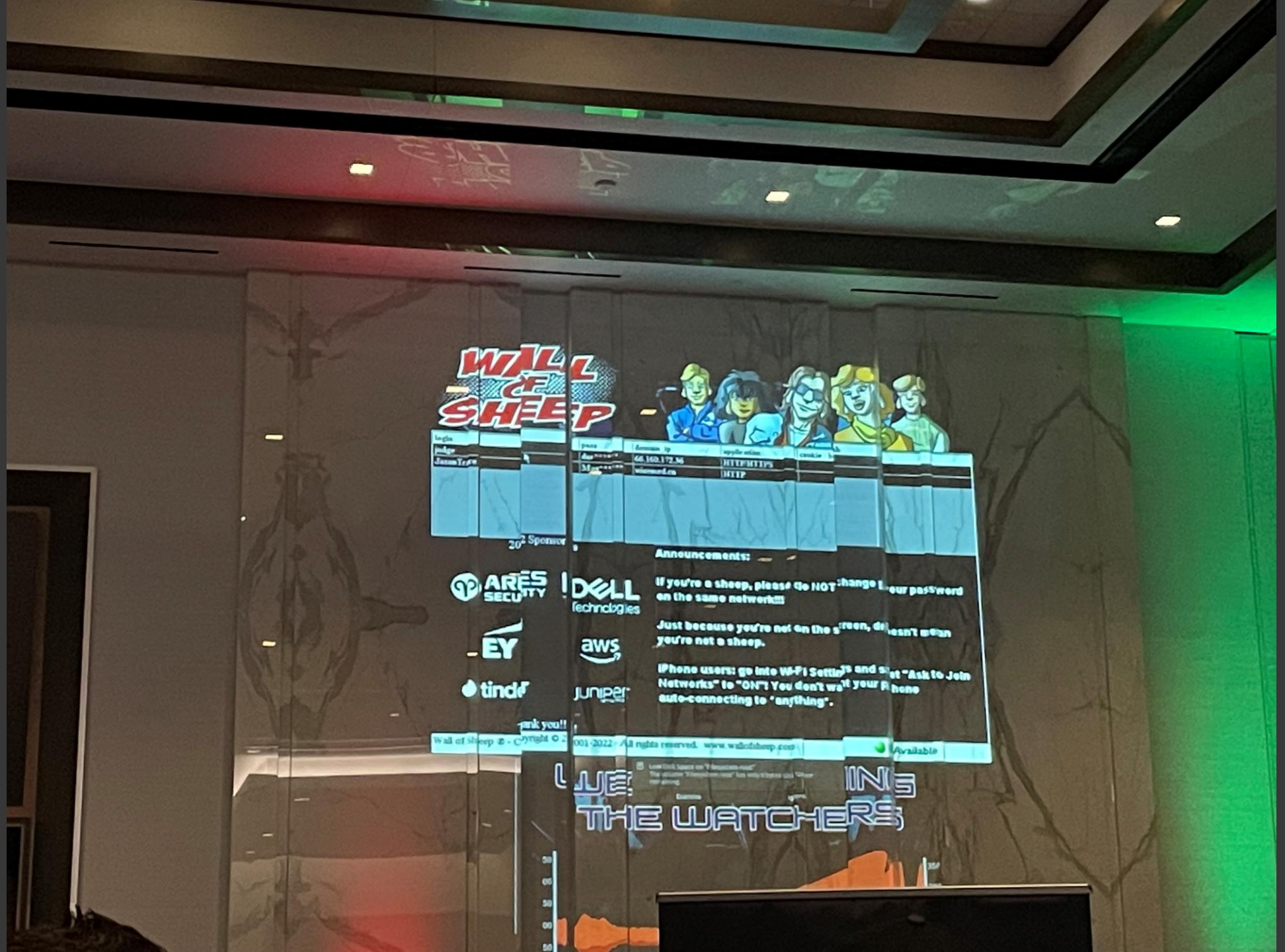
＜DEFCON の歴史・特徴＞

- 1993年より開催されたカンファレンス
  - BlackHat創設者のJeff Moss氏が開催したカンファレンスだが、BlackHatより歴史が古い
- DEF CONは、「後夜祭」的な位置づけ（for Hackers）
  - Briefingセッションはある一方、比較的Black Hatと同じネタも存在する。
- DEF CON CTFなどが行われており、日本のチームも出場している。
- 一方、Villageと呼ばれるテーマ別のセッションなどがあり、こちらの方がより面白い話や交流をすることができる（Skytalk・Car Hacking Village・Picking Villeageなど）
- Hak5など、ペネトレーションテストツールなども入手することも可能
    - 例）Bash Bunny・WiFi-Pineapple


HACKER HOMECOMING
DEFCON
30


POWER
USB
SELF TEST
BUTTONS: UDLR
KEYS:0123456789ABCDE
SAMPLE PAD
1
2
3
C
D
E
F
G
A
B
DC-30 HUMAN SAMPLING KEYBOARD


TOP 10
DEF
CON


WALL OF SHEEP
Announcements:
If you're a sheep, please do NOT change your password on the same network!!!
Just because you're not on the screen, doesn't mean you're not a sheep.
iPhone users: go into Wi-Fi Settings and set "Ask to Join Networks" to "OFF"! You don't want your phone auto-connecting to "anything".
ARES SECURITY
DELL technologies
EY
aws
tinder
juniper
THE WATCHERS


COLD
drinks


PRESS SELECTION TO DISPLAY
PRICE OR SOLD OUT
Sparkling
Diet
OpenWRT
Sugar
FreeBSD
Debian
Rocky Linux
Lite
Rocky Linux
Brew
Server Core
2022


OBD-Kill


LIGHTSPEED
CAPS LOCK
KEY CROC
SMART KEYLOGGER
HAK5
BASH BUNNY
HAK5
WiFi
Pineapple

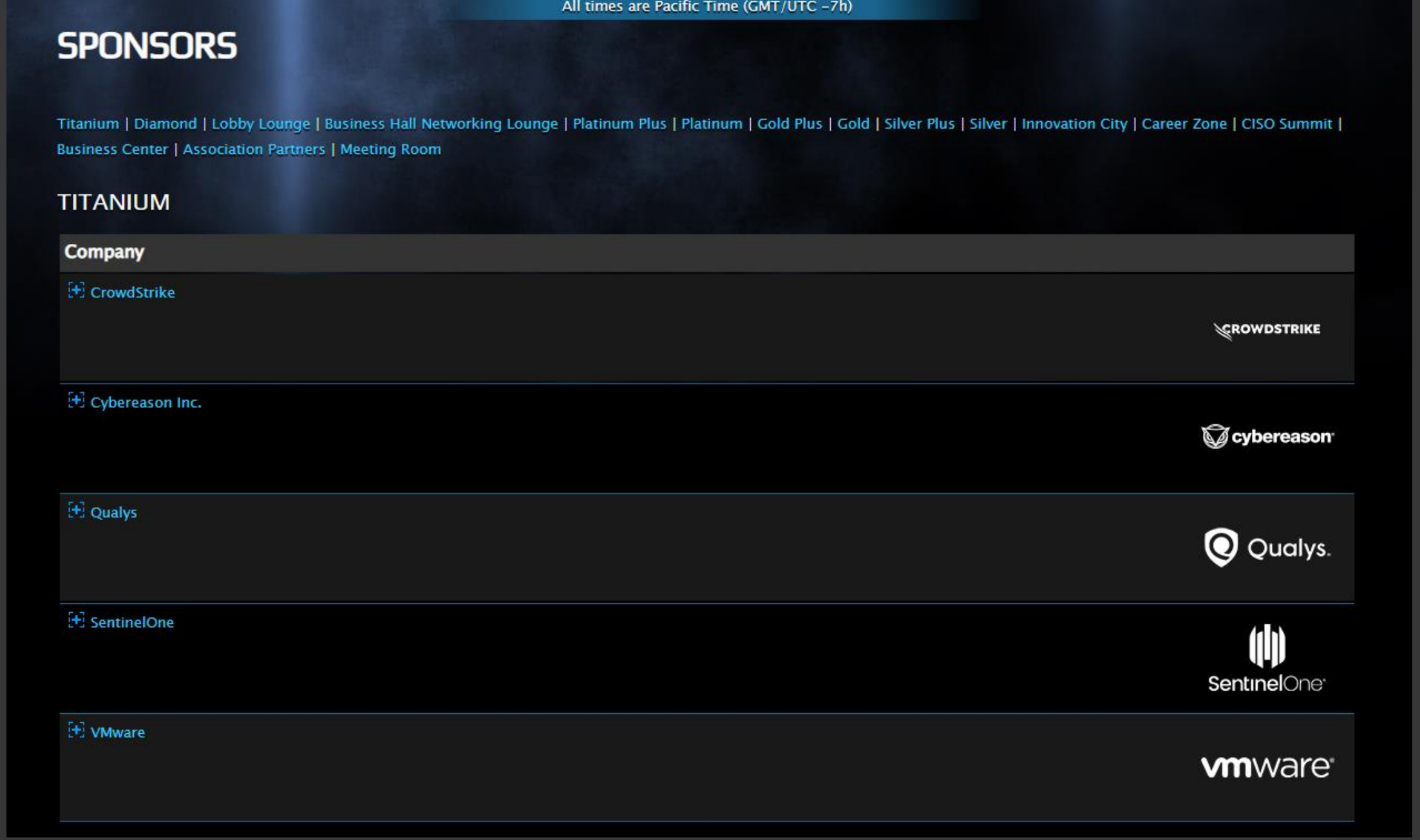
2. BlackHat USA 概要

BlackHat USA 2022概要

4つのセッション（Training・Briefing・Business Hall・ Arsenal）で構成されている。

- **Briefing Session：攻撃・防御の新しいトレンドを把握**
  - 様々な研究発表が行われる。今年は、AzureAD、機械学習、WebAssemblyなど新しい技術に関する攻撃手法などが発表された。
  - https://www.blackhat.com/us-22/briefings/schedule/
  - https://bit.ly/3FnQjHd　（Google Driveに資料をDLしてくれている）

- **Business Hall Session：製品・技術トレンドの把握**
  - スポンサーから、現在の製品トレンドがわかる（次ページ）
  - 各ベンダーが新しい製品・機能を発表する場。特にスタートアップ企業や米国でしか展開していない企業など、新しい技術・アプローチを採用したベンダーとコンタクトすることができる。
    - （セキュリティ態勢の）可視化系製品：
      - SSPM（SaaS Security Posture Management）
      - ASM（Attack Surface Management）
    - （人材不足を補う）自動化製品：
      - XDR（eXtended Detection & Response）
      - SOAR（Security Orchestration and Automation Response）



https://www.blackhat.com/us-22/event-sponsors.html


vmware SECURITY
See what others don't.
Stop what others can't.
CROWDSTRIKE
TREND MICRO
splunk>
paloalto
paloalto
BlackBerry
DARKTRACE
mimecast
VMware Contexa Cafe


CB56
RAPID7
paloalto
CROWDSTRIKE
COZY BEAR
TARGET INDUSTRIES
Academic, Aerospace, Energy, Extractive, Financial Services, Government, Industrials & Engineering, Insurance, Media, NGOs & Nonprofits, Oil & Gas, Pharmaceuticals, Technology

検索

Black Hat USA 2022

Black Hat

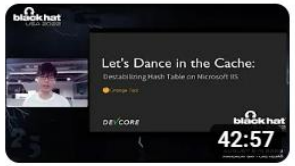
100 本の動画 12,711 回視聴 最終更新日: 2022/12/11

すべて再生 シャッフル

1 

Leveraging the Apple ESF for Behavioral Detections

Black Hat・5130 回視聴・3 週間前

2 

Let's Dance in the Cache - Destabilizing Hash Table on Microsoft IIS

Black Hat・1523 回視聴・3 週間前

3 

Kubernetes Privilege Escalation: Container Escape == Cluster Admin?

Black Hat・3045 回視聴・3 週間前

4 

Is WebAssembly Really Safe? -- Wasm VM Escape and RCE Vulnerabilities Have Been Found in New Way

Black Hat・1241 回視聴・3 週間前

5 

Invisible Finger: Practical Electromagnetic Interference Attack on Touchscreen-based Devices

Black Hat・1308 回視聴・3 週間前

BlackHat USA 2022概要

トレンド１：Active Directory + AzureADへの攻撃

- エンタープライズ環境では、認証＋認可の管理をActive Directory OR Azure ADで実施している。
- そのため、多くの攻撃テクニック（権限昇格・Lateral Movement）は、AD/AADの仕様を悪用しているため、研究が盛んにおこなわれている。

- 例）ADに対する攻撃（Kerberos認証に対する攻撃）
  - Golden Ticket攻撃・Silver Ticket攻撃・Kerberoasting攻撃・AS_REP Roast攻撃
  - ZeroLogin（CVE-2020-1472）、PrintNightmare（CVE-2021-1675 / CVE-2021-34527）
  - https://bit.ly/3VSQGiz

- *Elevating Kerberos to the Next Level*
  - Kerberos認証の悪用は、様々存在するが、その攻撃の多くがLateral Movementなどに焦点を当てられてきた。一方で、本研究ではローカルでの認証権限攻撃などについての攻撃手法を研究している。
    - https://i.blackhat.com/USA-22/Wednesday/US-22-Forshaw-Taking-Kerberos-To-The-Next-Level.pdf
    - https://www.youtube.com/watch?v=GM1PxZPiLMk

BlackHat USA 2022概要

トレンド１：Active Directory + AzureADへの攻撃

- エンタープライズ環境では、認証＋認可の管理をActive Directory OR Azure ADで実施している。
- そのため、多くの攻撃テクニック（権限昇格・Lateral Movement）は、AD/AADの仕様を悪用しているため、研究が盛んにおこなわれている。

- 例）Azure ADに対する攻撃
  - Active Directory（オンプレ版）とは似て非なる仕組みだが、考え方は応用できる。
  - 攻撃例）Pass-The-PRT・Pass The Certificate・Token Abuse
  - https://github.com/rootsecdev/Azure-Red-Team

- *AAD Joined Machines - The New Lateral Movement*
  - オンプレミス環境でLateral Movement（横断的侵害）を行う手法の一つとして、NTLMやKerberos認証を悪用した攻撃（例：Pass-The-Hash）が存在するが、AAD環境では利用できない。
  - その一方、Kerberos PKU2UやNegoExを悪用することにより、同様のアプローチをつかってAAD上の端末でLateral Movementをすることが可能（NegoEx Relay）
    - https://i.blackhat.com/USA-22/Wednesday/US-22-Rubin-AAD-Joined-Machines-New-Lateral-Movement.pdf
    - https://github.com/morRubin/NegoExRelay

BlackHat USA 2022概要

トレンド１：Active Directory + AzureADへの攻撃

- エンタープライズ環境では、認証＋認可の管理をActive Directory OR Azure ADで実施している。
- そのため、多くの攻撃テクニック（権限昇格・Lateral Movement）は、AD/AADの仕様を悪用しているため、研究が盛んにおこなわれている。

- 脆弱なAD環境を作るなら：
  - Vulnerable AD：
    - https://github.com/WazeHell/vulnerable-AD
  - Detection Lab：
    - https://github.com/clong/DetectionLab
    - https://jpn.nec.com/cybersecurity/blog/210416/index.html
  - TryHackMe & HackTheBoxなどを使うのも一つ！

BlackHat USA 2022概要

トレンド１：Active Directory + AzureADへの攻撃

- エンタープライズ環境では、認証＋認可の管理をActive Directory OR Azure ADで実施している。
- そのため、多くの攻撃テクニック（権限昇格・Lateral Movement）は、AD/AADの仕様を悪用しているため、研究が盛んにおこなわれている。

- ADを継続的モニタリングするツールを利用し、ADのヘルスチェックを行うことが重要！
  - ツールの具体例として以下の通り（評価は各自でお願いします）
    - 例）Attivo Network社 AD Assessor https://www.attivonetworks.com/product/adassessor/
    - 例）SpectorOps社 Bloodhound Enterprise https://bloodhoundenterprise.io/
    - 例）Tenable社 Tenable.ad https://www.tenable.com/products/tenable-ad
    - 例）PingCastle https://www.pingcastle.com/
    - 例）CrowdStrike社 Falcon ITP/ITD https://www.crowdstrike.jp/products/identity-protection/

- 参考）*ITDR：ID Threat Detection & Response*
  - Gartner社「2022年のセキュリティ／リスク・マネジメントのトップ・トレンド」として挙げている。
  - 侵害の多くは、IDの悪用が起点となるため、IDの利用を検知・対応するサービスが少しづつ登場している。
  - 脅威ハンティングの観点でも、IDに注目する重要性はより高くなる（と思う）。

BlackHat USA 2022概要

トレンド２：コア技術への攻撃

- *IAM The One Who Knocks*
  - 企業において、マルチテナント/マルチテナント環境を使うことが一般的であるが、当該環境では最小権限のアクセスを強制することが難しくなり、各クラウド環境に固有の新しいルールと権限が必要となる。その攻撃手法について整理した講演
    - https://i.blackhat.com/USA-22/Wednesday/US-22-Gofman-IAM-The-One-Who-Knocks.pdf

- *Kubernetes Privilege Escalation: Container Escape == Cluster Admin?*
  - Kubernetesの利用が普及に伴い、クラスターを侵害するという最終的な目標を持った専用のマルウェアが登場しており、ポッドを悪用して権限昇格をする新しい手法を公開
  - https://i.blackhat.com/USA-22/Thursday/US-22-Avrahami-Kubernetes-Privilege-Escalation-Container-Escape-Cluster-Admin.pdf

- *Let's Dance in the Cache - Destabilizing Hash Table on Microsoft IIS*
  - Orange Tsai氏（@orange_8361）IISのハッシュテーブルに対する攻撃に関する最新手法
    - https://i.blackhat.com/USA-22/Wednesday/US-22-Tsai-Lets-Dance-in-the-Cache-Destabilizing-Hash-Table-on-Microsoft-IIS.pdf

BlackHat USA 2022概要

その他：

- *Smishmash - Text Based 2fa Spoofing Using OSINT, Phishing Techniques and a Burner Phone*
  - 公開されている情報源からデータを収集し、2 要素認証システムで使用されている可能性が最も高い電話番号を、漏洩した他の電子メールおよびログイン資格情報に関連付ける方法
    - https://i.blackhat.com/USA-22/Wednesday/US-22-Olofsson-Smishsmash.pdf

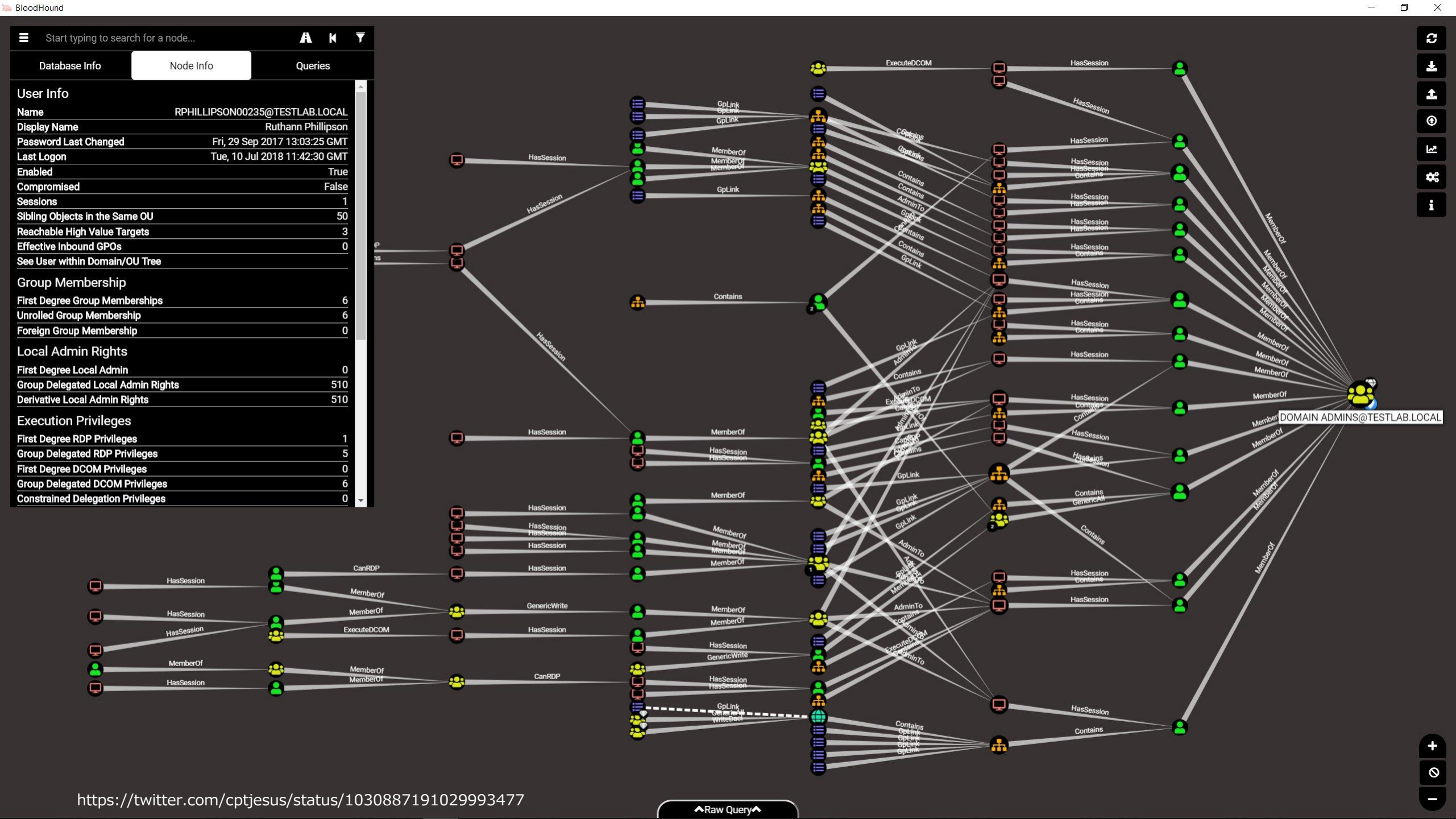
- *The Open Threat Hunting Framework*
  - 脅威ハンティング（SecureWorks社の定義）
    - **既存のセキュリティ対策を回避する現在/過去の脅威を能動的・再帰的に調査**し、その情報を利用して**サイバーレジリエンスを向上**させること（=プロアクティブなアプローチ）
  - フレームワークは様々存在するが、新しい手法の提唱されている
    - 例：TaHiTIモデル（Targeted Hunting integrating Threat Intelligence）
  - 文書を読んだ限り、体系的にまとまっている。
    - https://www.blackhat.com/us-22/briefings/schedule/#the-open-threat-hunting-framework-enabling-organizations-to-build-operationalize-and-scale-threat-hunting-26702

3. 注目すべきセキュリティトレンド

トレンド: 脆弱性管理 / Attack Path Management

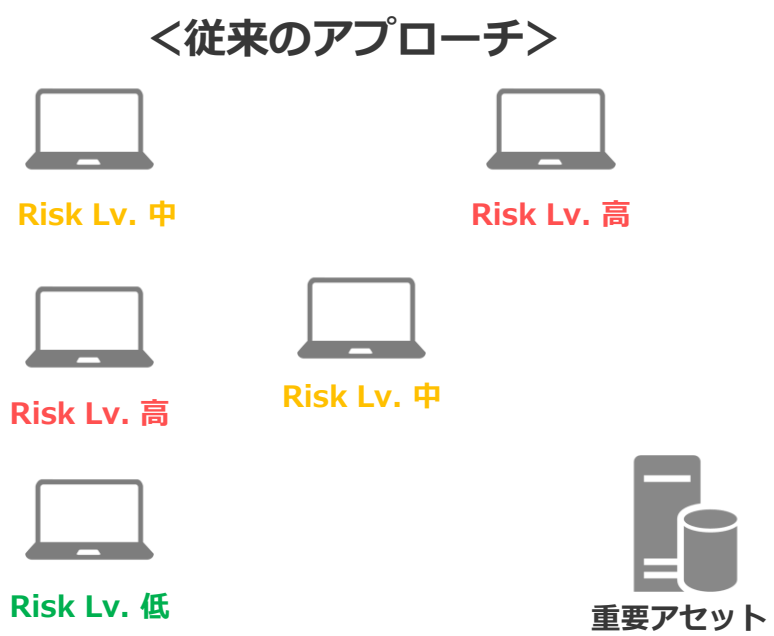
- 注目すべきキーワード：Attack Path Management

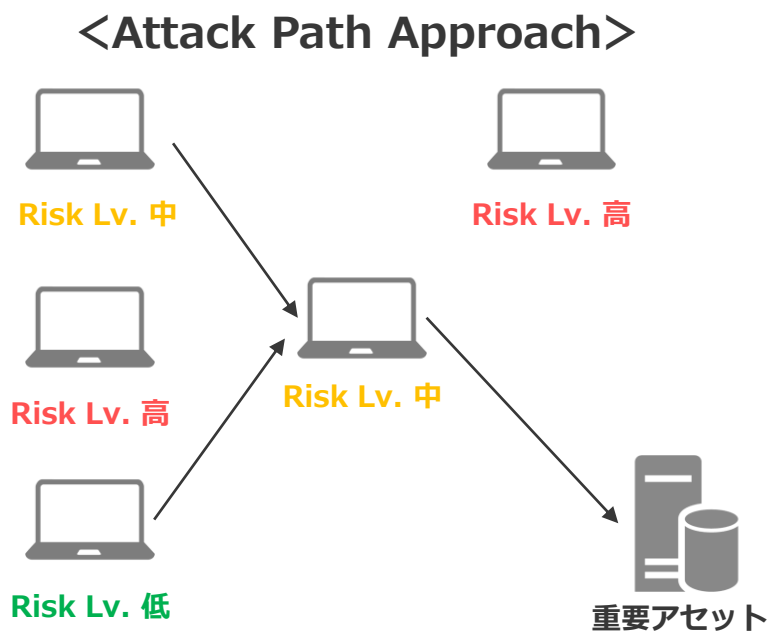
- Attack Pathとは？
  - 攻撃者がシステムの弱点を悪用するためにたどるパスを視覚的に表したもの。関連するリスクとセキュリティのコンテキスト全体を調べて、潜在的な弱点を見つけて対処することに重点を置く。

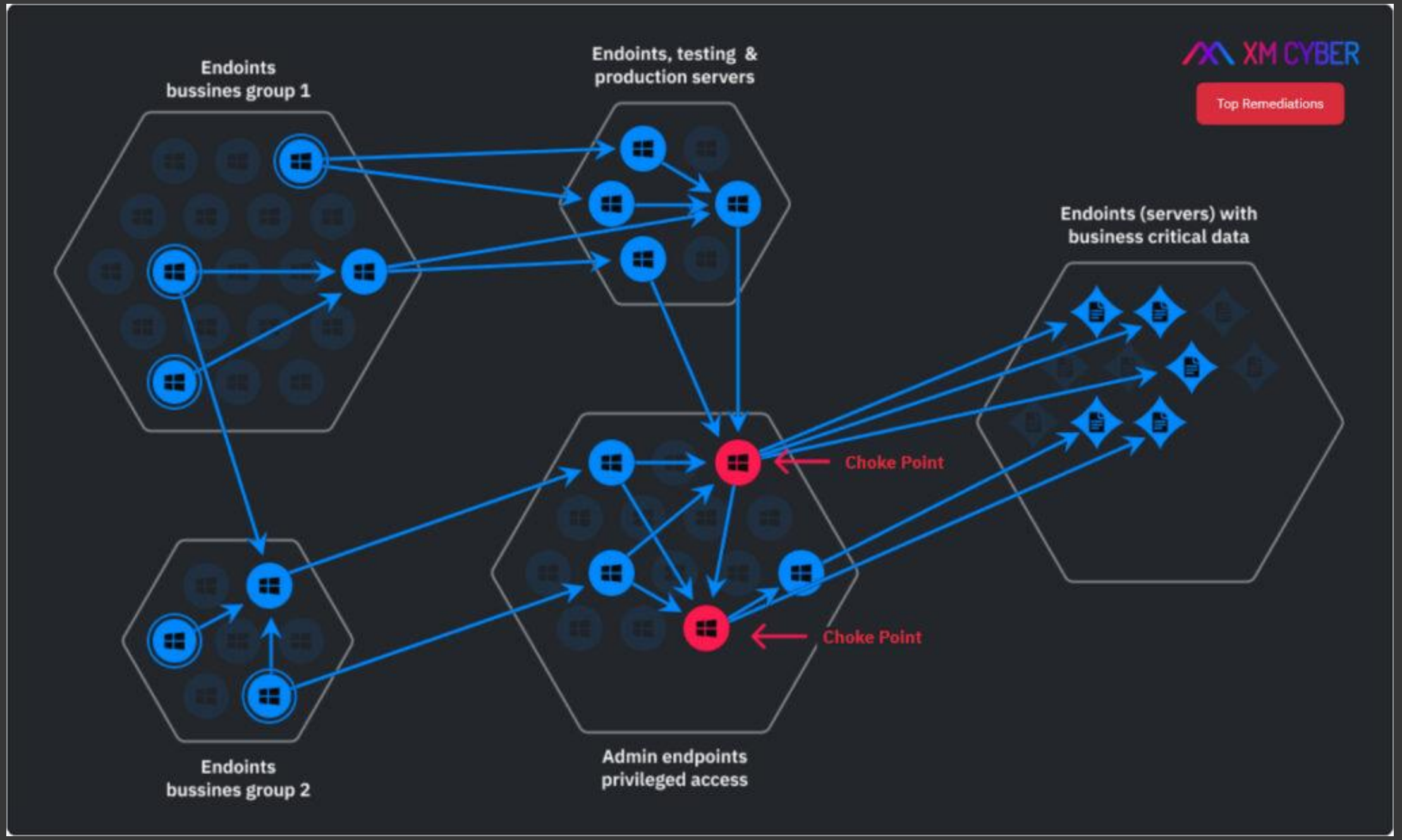

BloodHound
Start typing to search for a node...
Database Info
Node Info
Queries
User Info
Name RPHILLIPSON00235@TESTLAB.LOCAL
Display Name Ruthann Phillipson
Password Last Changed Fri, 29 Sep 2017 13:03:25 GMT
Last Logon Tue, 10 Jul 2018 11:42:30 GMT
Enabled True
Compromised False
Sessions 1
Sibling Objects in the Same OU 50
Reachable High Value Targets 3
Effective Inbound GPOs 0
See User within Domain/OU Tree
Group Membership
First Degree Group Memberships 6
Unrolled Group Membership 6
Foreign Group Membership 0
Local Admin Rights
First Degree Local Admin 0
Group Delegated Local Admin Rights 510
Derivative Local Admin Rights 510
Execution Privileges
First Degree RDP Privileges 1
Group Delegated RDP Privileges 5
First Degree DCOM Privileges 0
Group Delegated DCOM Privileges 6
Constrained Delegation Privileges 0
DOMAIN ADMINS@TESTLAB.LOCAL
https://twitter.com/cptjesus/status/1030887191029993477
Raw Query

トレンド: 脆弱性管理 / Attack Path Management

- Attack Pathをどう活用するのか？
  - 大前提：
    - 組織において、脆弱性管理・ペネトレーションテスト（TLPT）の結果を全て修正することは難しい。
    - そのため、組織は優先度をつけて対応を行う（例：CVSSスコア、アセットの重要性、ベンダーの推奨）
    - 但し、TLPT（Threat-Led Penetration Test）などでは、テストに使われた端末の対策のみならず、他に同様の問題がないか、伏在調査を行わないといけない。
  - Attack Pathを可視化することにより、優先度をつけることが可能となる（**Choke Point**を押させる）







https://www.xmcyber.com/blog/reinforce-aws-security-with-continuous-and-automated-mitigation-of-hybrid-cyber-risk/

トレンド：XDR +XSPM

- EDR・NDRなどに加え、IDに注目した脅威検知、Dataに注目したDetection & Responseサービスが少しづつ登場している。
  - **ITDR (ID Threat Detection and Response)**
  - **DDR（Data Detection & Response）**

- CSPM（Cloud Security Posture Management）に続き、様々な観点に注目したセキュリティ態勢管理（XSPM）も登場し始めている。
  - **DSPM（Data Security Posture Management）**
  - **SSPM（SaaS Security Posture Management）**

4. まとめ

まとめ

- **技術トレンド：**
  - AD + Azure ADへの攻撃は引き続き研究が進められている
  - Kubernetesやクラウド基盤に対する攻撃などもトレンド
    - 但し、比較的すぐ対処されるので、発表時には修正されていることも多々ある

- **製品トレンド：**
  - （セキュリティ態勢の）可視化系製品：
    - ASM（Attack Surface Management）
    - Attack Surface Management
    - XSPM (X Security Posture Management)

  - （人材不足を補う）自動化製品：
    - XDR（eXtended Detection & Response）
    - SOAR（Security Orchestration and Automation Response）

実務系カンファレンスへの参加しよう！

- 実務系カンファレンスに参加するメリット：
  - セキュリティのトレンド・最新動向がわかる。
  - 講演だけでなく、製品動向からもどのようなセキュリティサービス・トレンドに注目が集まっているかが把握できる。
  - Undergroundセッションがそのうち復活するかも！

  - 総合系：
    - RSA Conference
    - Black Hat & DEFCON
    - Bsides

  - 特定領域系：
    - https://ringzer0.training/
    - https://www.offensivecon.org/

Thank You!