



TED × PenTera 共同webinar

東京エレクトロン デバイス株式会社

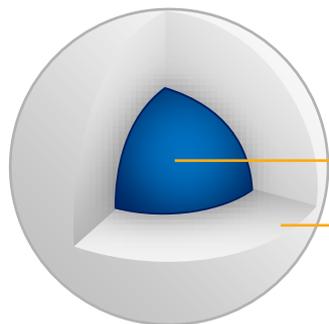




攻撃対象となる環境全体の
セキュリティを確かなものに

ミッション

Assure security readiness across
your complete attack surface



Internal Core Network

External Attack Surface

- 設立 2015年 ユニコーン企業
- 従業員数 >330人
- 導入実績
 - 56カ国
 - >800社



TOTAL ATTACK SURFACE COVERAGE

One platform for all your
security validation
operations

TED×PenTera 攻撃者から見た効果的な対策シリーズ

7月	ランサムウェア対策
9月	継続的な脅威エクスポージャーマネージメントとその実装
11月	脆弱性とASM（Attack Surface Management）による対策
12月	2023年のKey learning、2024に向けて

セキュリティ人材なら知っている 今話題の用語CTEM (継続的な脅威エクスポージャーマネージメント) とその実装

2023年9月

柴崎 恵美
Sales Engineer Japan

組織のサイバーセキュリティや脆弱性管理に自信がありますか？



継続的な脅威エクスポージャーマネージメント

Continuous Threat Exposure Management (CTEM)

エクスポージャーマネージメント

組織がITリスクやサイバー攻撃にさらされている程度を計測し、改善していくプロセス

エクスポージャー(露出) = 組織サイバー攻撃にさらされているリスク
マネージメント = 管理

アタックサーフェス

攻撃者がアクセスできる
対象や範囲

脆弱性

OSやアプリケーションの
脆弱性

漏洩したクレデンシャル

過去に漏洩した
ユーザーID/パスワード情報

継続的な脅威エクスポージャー管理

Continuous Threat Exposure Management (CTEM)

継続的なエクスポージャー管理をもとに優先順位付けしてセキュリティ投資を行う組織は、2026年までに侵害に苦しむ可能性が3分の1に減少すると予想されます。

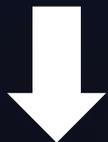
By 2026, organizations that **prioritize** their security investments based on a **continuous exposure** management program will be 3x less likely to suffer a breach

組織の視点と攻撃者視点

組織側の視点



転換が必要



攻撃者側の視点

見えるものの違い

組織が把握していること



攻撃者から見えること

優先順位付けの違い

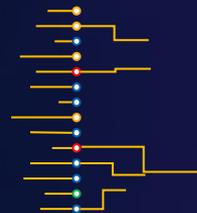
CVSSIにもとづき
対処を優先順位付け



攻撃のできるものを攻撃対象

検証方法の違い

脆弱性を確認



影響や攻撃の成果を確認

Validation(検証)とは

攻撃者の視点から色々な攻撃手法を用いてテストを行い、サイバー攻撃を受ける危険性があるのかを検証すること

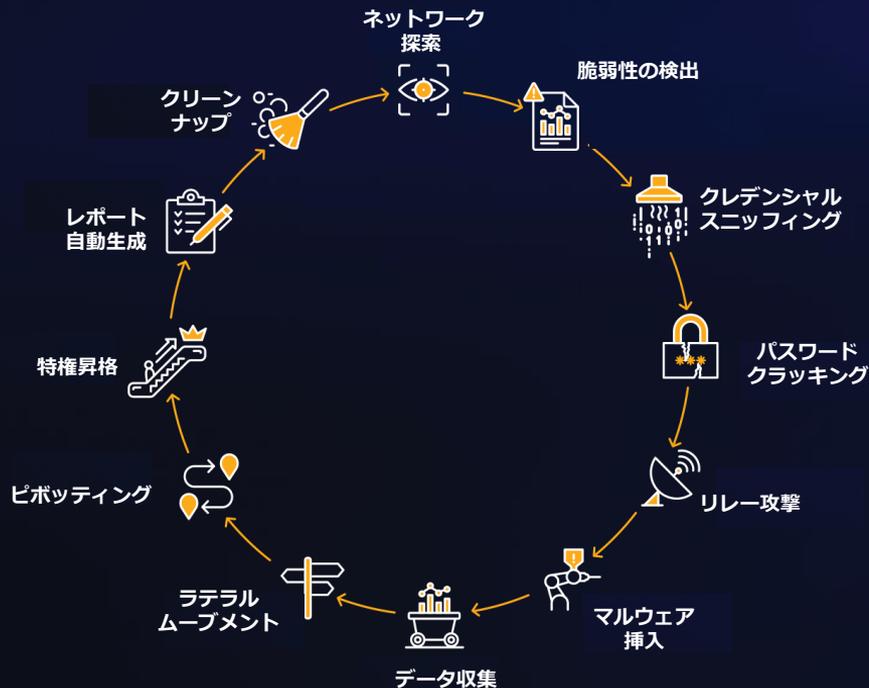
VALIDATION

- | | | |
|-------------|---|------------------------|
| 脆弱性の発見 | → | 脆弱性をついた攻撃が可能か |
| クレデンシャルの奪取 | → | そのクレデンシャルを使ってログイン可能か |
| 疑わしいファイルの有無 | → | マルウェアが実行できC2C通信が確立できるか |

VALIDATION



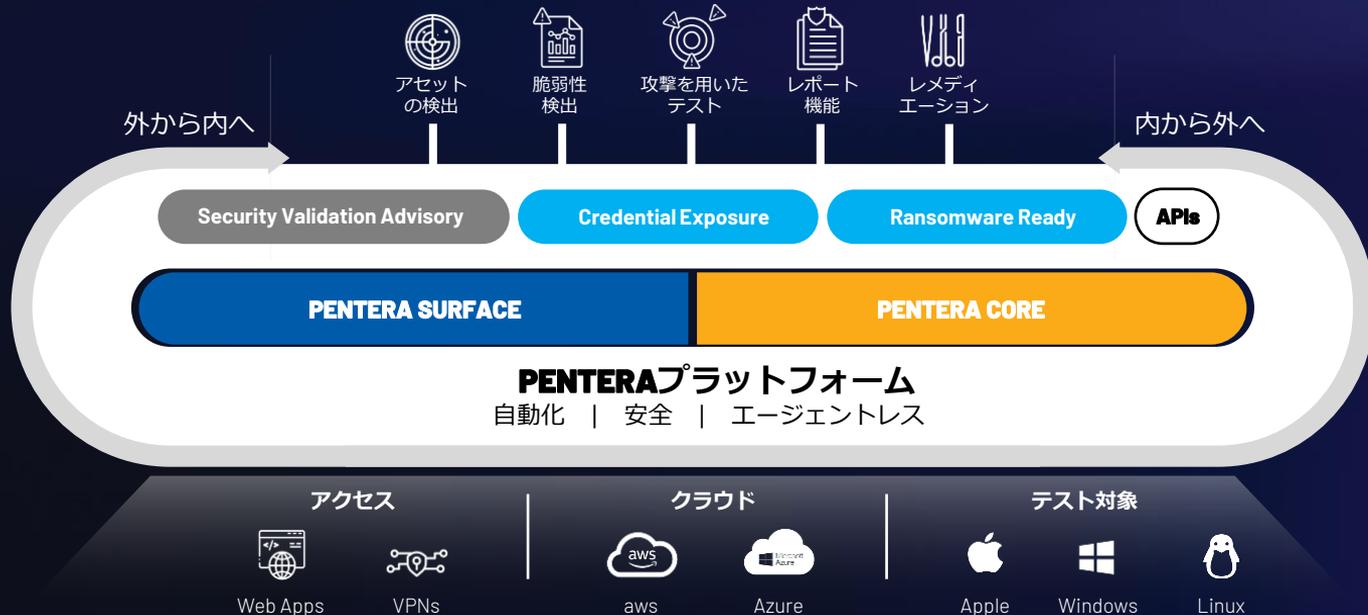
Penteraのご紹介



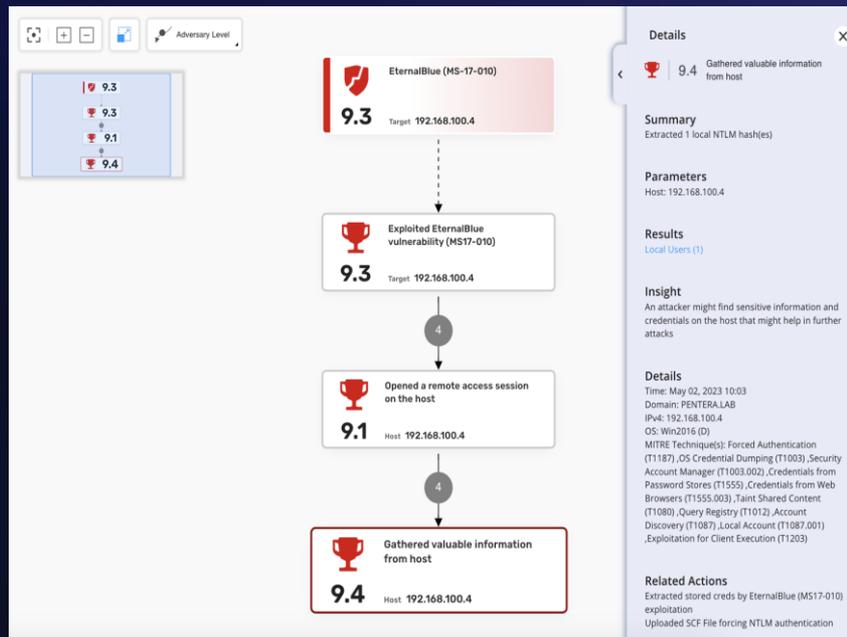
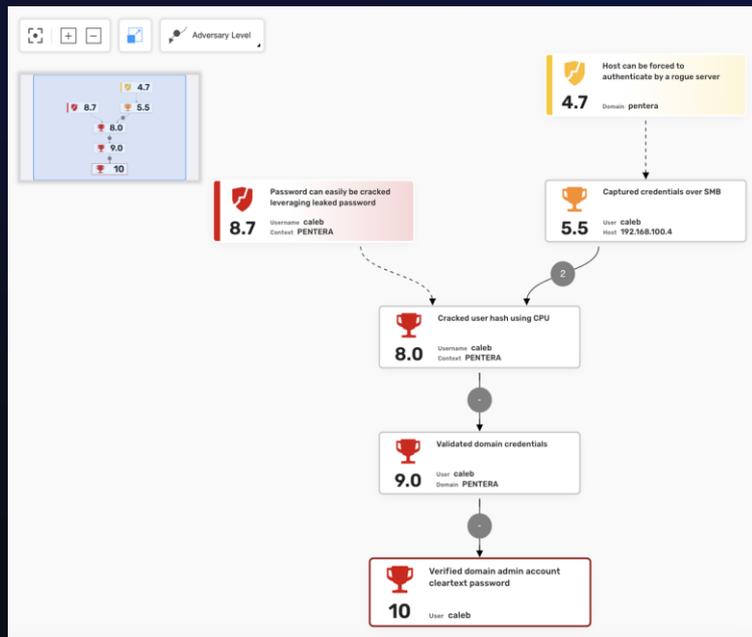
ASV Automated Security Validation

自動化
実際の攻撃と同様のテスト
エージェント不要
安全

Penteraのプラットフォームの構成



テスト結果例



自動レポート生成



PENTERA Apr. 16, 2021 Detailed Report

MITRE ATT&CK map

Credential Access	Discovery	Lateral Movement	Collection	Command and Control
Network Sniffing Mitigation: 1/1000	Account Authentication Mitigation: 1/1000	Network Sniffing Mitigation: 1/1000	Security Account Manager: 1/1000	Network Sniffing Mitigation: 1/1000
Account Authentication Mitigation: 1/1000	Network Sniffing Mitigation: 1/1000	Security Account Manager: 1/1000	Network Sniffing Mitigation: 1/1000	Web Application Admin Shell: 1/1000
Credential Sniffing Mitigation: 1/1000	Security Account Manager: 1/1000	Account Authentication Mitigation: 1/1000	Establishment of Remote Services: 1/1000	Network Sniffing Mitigation: 1/1000
Security Account Manager: 1/1000	Credential Sniffing Mitigation: 1/1000	Account Authentication Mitigation: 1/1000	Account Authentication Mitigation: 1/1000	Account Authentication Mitigation: 1/1000
Passport Sniffing: 1/1000	Pass in the Wilds: 1/1000	Account Authentication Mitigation: 1/1000	Account Authentication Mitigation: 1/1000	Account Authentication Mitigation: 1/1000
Pass in the Wilds: 1/1000	Account Authentication Mitigation: 1/1000	Account Authentication Mitigation: 1/1000	Account Authentication Mitigation: 1/1000	Account Authentication Mitigation: 1/1000

PENTERA Apr. 16, 2021 Detailed Report

88 Vulnerabilities

Pentera identified a total of 88 vulnerabilities across 60 assets. Severity breakdown: Critical (14), High (2), Medium (15), Low (57).

- 4.2 The host is vulnerable to ZeroLogon**
An attacker can change a vulnerability record when an attacker establishes a vulnerable RemoteApp session (affected connections to domain controllers).
CVE: CVE-2020-1472 (WHITEHORN-SAN), CVE: CVE-2020-1472 (WHITEHORN-SAN)
- 5.6 The host is vulnerable to BlueKeep (CVE-2019-0708)**
An attacker might look for vulnerable operating systems in the organizational network. By exploiting this vulnerability, the attacker can gain a high-privilege shell.
CVE: CVE-2019-0708 (WHITEHORN-SAN)
- 6.3 The host is vulnerable to BlueKeep (CVE-2019-0708)**
An attacker might look for vulnerable operating systems in the organizational network. By exploiting this vulnerability, the attacker can gain a high-privilege shell.
CVE: CVE-2019-0708 (WHITEHORN-SAN)
- 7.2 Using easy to guess passwords (L)**
Factors such as the password only a list of commonly used passwords. Successful in obtaining the password using common password manipulation rules.
CVE: CVE-2019-0708 (WHITEHORN-SAN)
- 9.2 Sensitive information can be sniffed due to network misconfiguration**
In cases where the DNS server fails to name resolution queries, the LLNMR, NBNS, and mDNS services are exposed to remote hosts.
CVE: CVE-2019-0708 (WHITEHORN-SAN)

PENTERA Apr. 16, 2021 Detailed Report

Cyber Resilience Score

A+

Name	Detailed Report
Description	Security Validation
Type	Penetration Testing (Black Box)
Time & Duration	Apr 08 2021 10:24 - Apr 09 2021
Included IP Range(s)	102.103.80.0/24
Action Approval Score	20/24 - 83%

Resilience Score Card

- Critical Assets** (Score: 10/10) Critical
- Credentials and Account Takerover** (Score: 1/1) Low
- Sniffing** (Score: 1/1) High
- AWEDR Bypass** (Score: 1/1) Medium

72 Total Action Approvals | **1,550** Total Assets

PENTERA Apr. 16, 2021 Detailed Report

Name Resolution Protocols (LLNMR/NBNS/mDNS)

MITRE

Insight

Insight: In cases where the DNS server fails to name resolution queries, the LLNMR, NBNS, and mDNS services are exposed to remote hosts. In cases where the DNS server fails to name resolution queries, the LLNMR, NBNS, and mDNS services are exposed to remote hosts. In cases where the DNS server fails to name resolution queries, the LLNMR, NBNS, and mDNS services are exposed to remote hosts.

Impact

Impact: In cases where the DNS server fails to name resolution queries, the LLNMR, NBNS, and mDNS services are exposed to remote hosts. In cases where the DNS server fails to name resolution queries, the LLNMR, NBNS, and mDNS services are exposed to remote hosts. In cases where the DNS server fails to name resolution queries, the LLNMR, NBNS, and mDNS services are exposed to remote hosts.

Recommendations

Recommendations: In cases where the DNS server fails to name resolution queries, the LLNMR, NBNS, and mDNS services are exposed to remote hosts. In cases where the DNS server fails to name resolution queries, the LLNMR, NBNS, and mDNS services are exposed to remote hosts. In cases where the DNS server fails to name resolution queries, the LLNMR, NBNS, and mDNS services are exposed to remote hosts.

Penteraによる継続的なエクスポージャーマネージメント



まとめ

- CTEM（継続的な脅威エクスポージャーマネージメント）は、**継続的に優先順位付け**することで、効率的に実施できます。
- 優先順位付けは、攻撃者の視点から行うことが重要です。
- Penteraのご利用により、攻撃者の視点からリスク検証を行い、セキュリティ対策の優先順位付けと継続的なCTEMが可能です。



Thank You