Mist セキュリティ

WIDS･WIPS

ジュニパーネットワークス株式会社
2021年11月 Ver 1.0

WIDS·WIPS

Q: Mist AP はワイヤレス脅威をどのように検出しますか?

1

3つの無線

- すべての無線はインライン型・または専用のセンサーとして動作し続けます

2

セキュリティコンテキストとしての位置情報

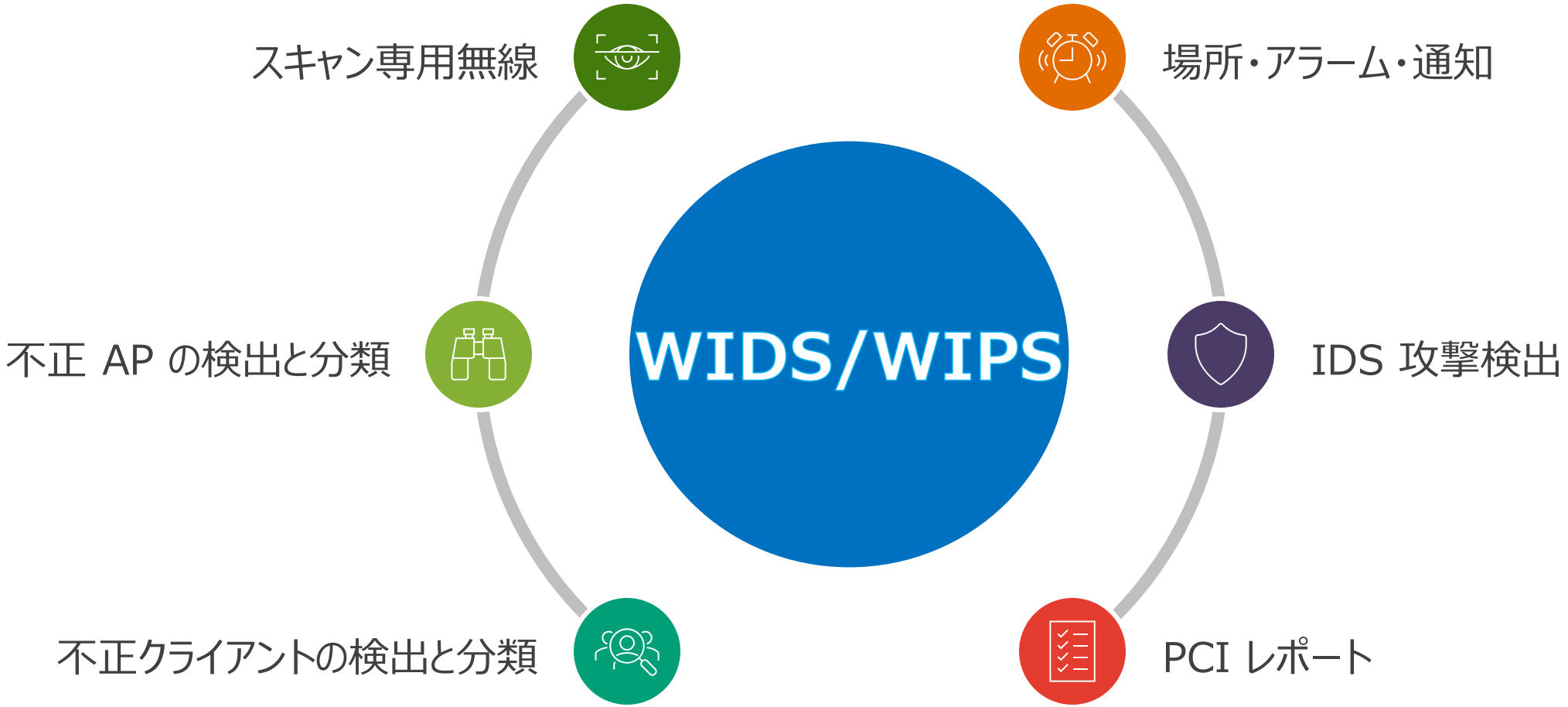
- セキュリティの観点からお使いいただける位置情報を提供します

3

IoTポート

- アナログ IoT デバイス用に組み込まれた IoT ポートを有しています

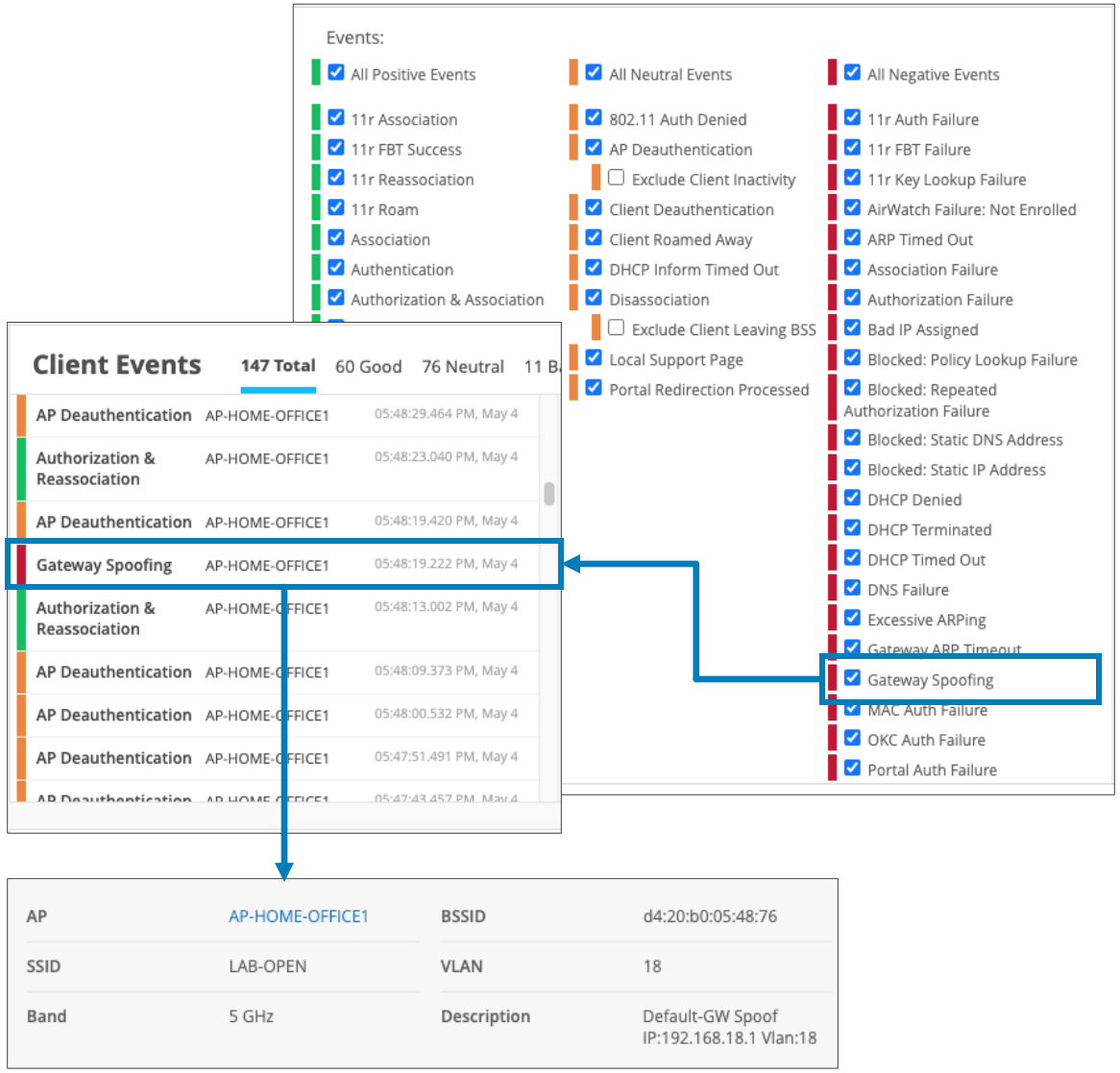
WIDS・WIPS
Q: どのレベルのワイヤレスセキュリティを提供できますか?



WIDS・WIPS
Q: ARP および DHCP アタックを検出できますか?

ARP アタック
- AP はデフォルト・ゲートウェイ・スプーフィング攻撃を検出し、クライアントのイベントとして表示することができます

DHCP アタック
- ワイヤレスクライアントから発信されるすべての DHCP オファーおよび DHCP ACK パケットをデフォルトでブロックします



WIDS･WIPS
Q: 不正APを検出できますか？

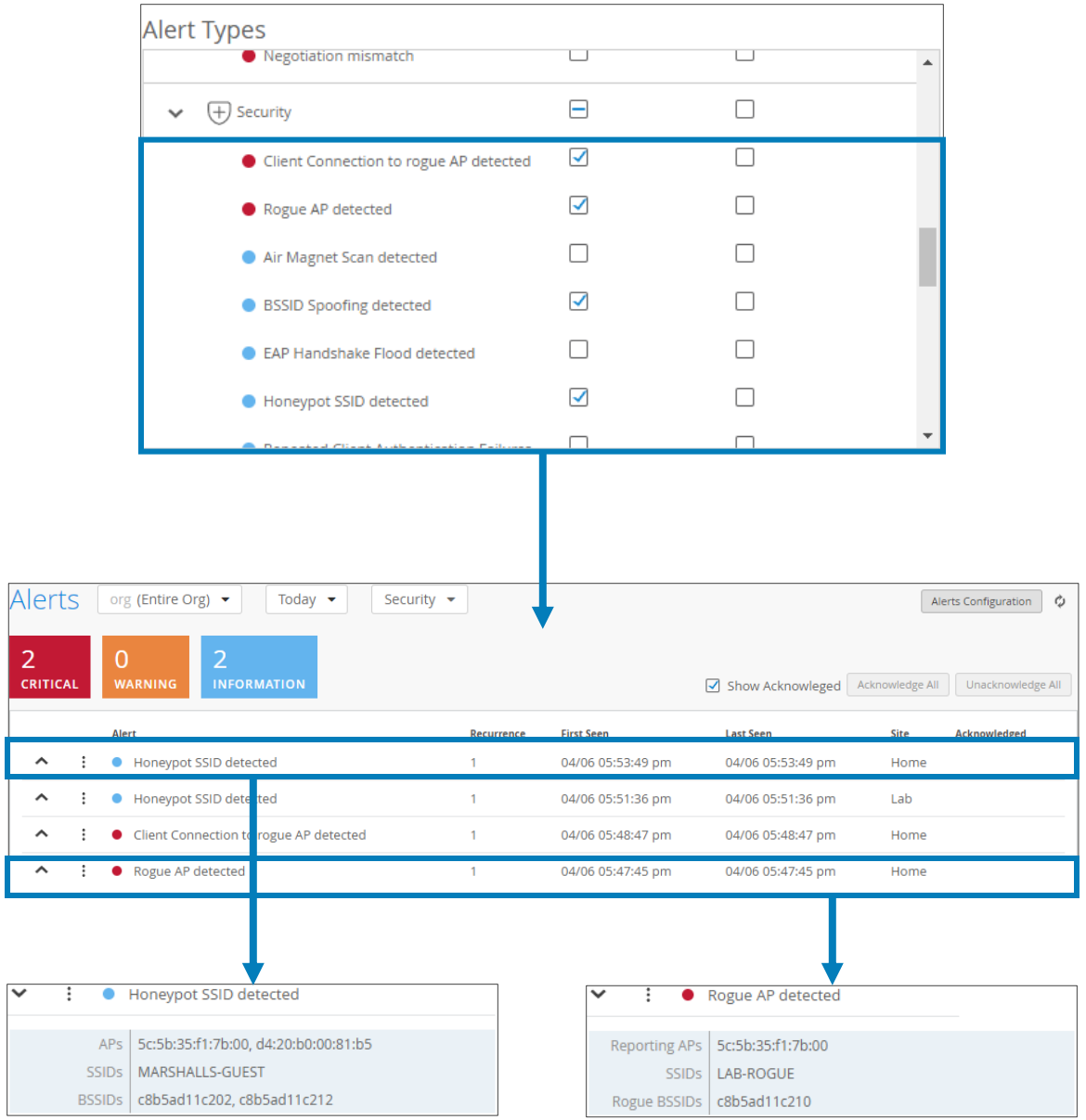
正確な検出、分類、アラート通知が可能です

ローグ AP
- Organization に未登録で、同じ有線ネットワークに接続されているAP

ローグ クライアント
- ローグ AP に接続されたクライアント

ハニーポット AP
- SSID をアドバタイズする未承認の AP

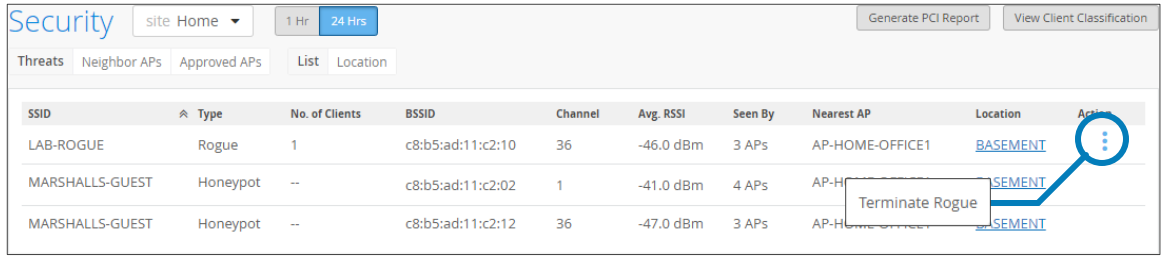
BSSID スプーフィング
- 有効な AP であるかのように振る舞う不正な AP

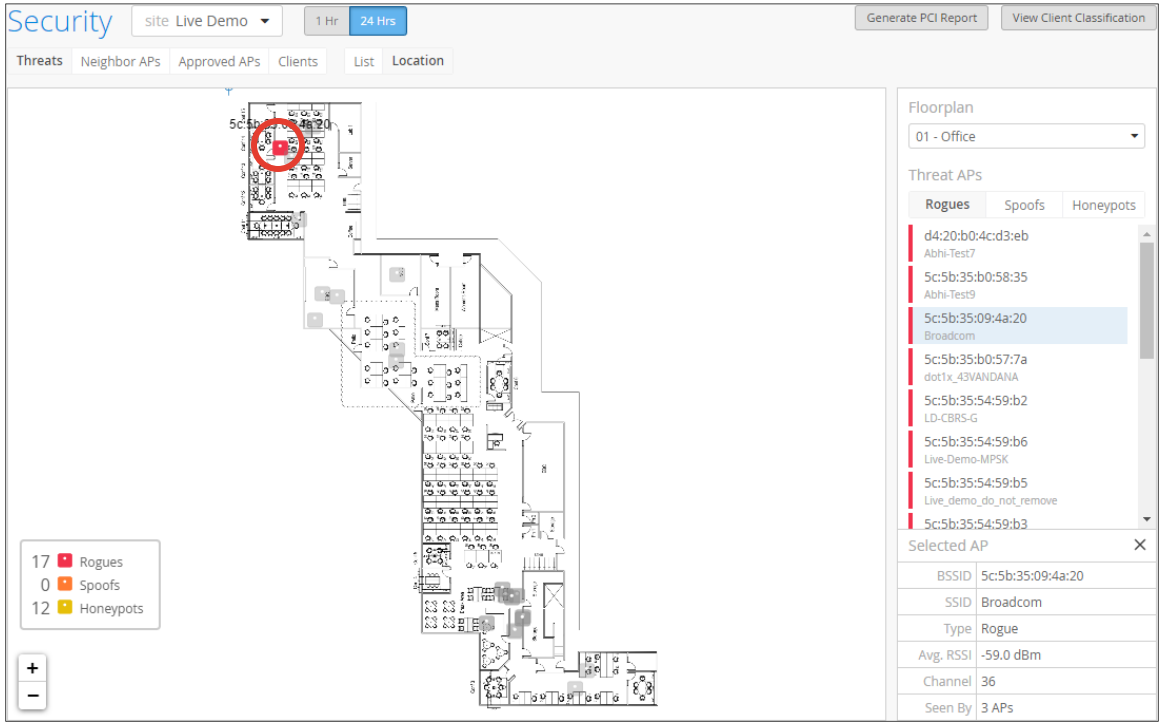


WIDS·WIPS
Q: ローグ AP を切断できますか?

ローグ AP の切断
- ローグ AP として分類された AP を手動で切断します

未承認 AP の場所特定
- 物理的な修復のためにフロアプラン上に未承認 AP の場所を表示します

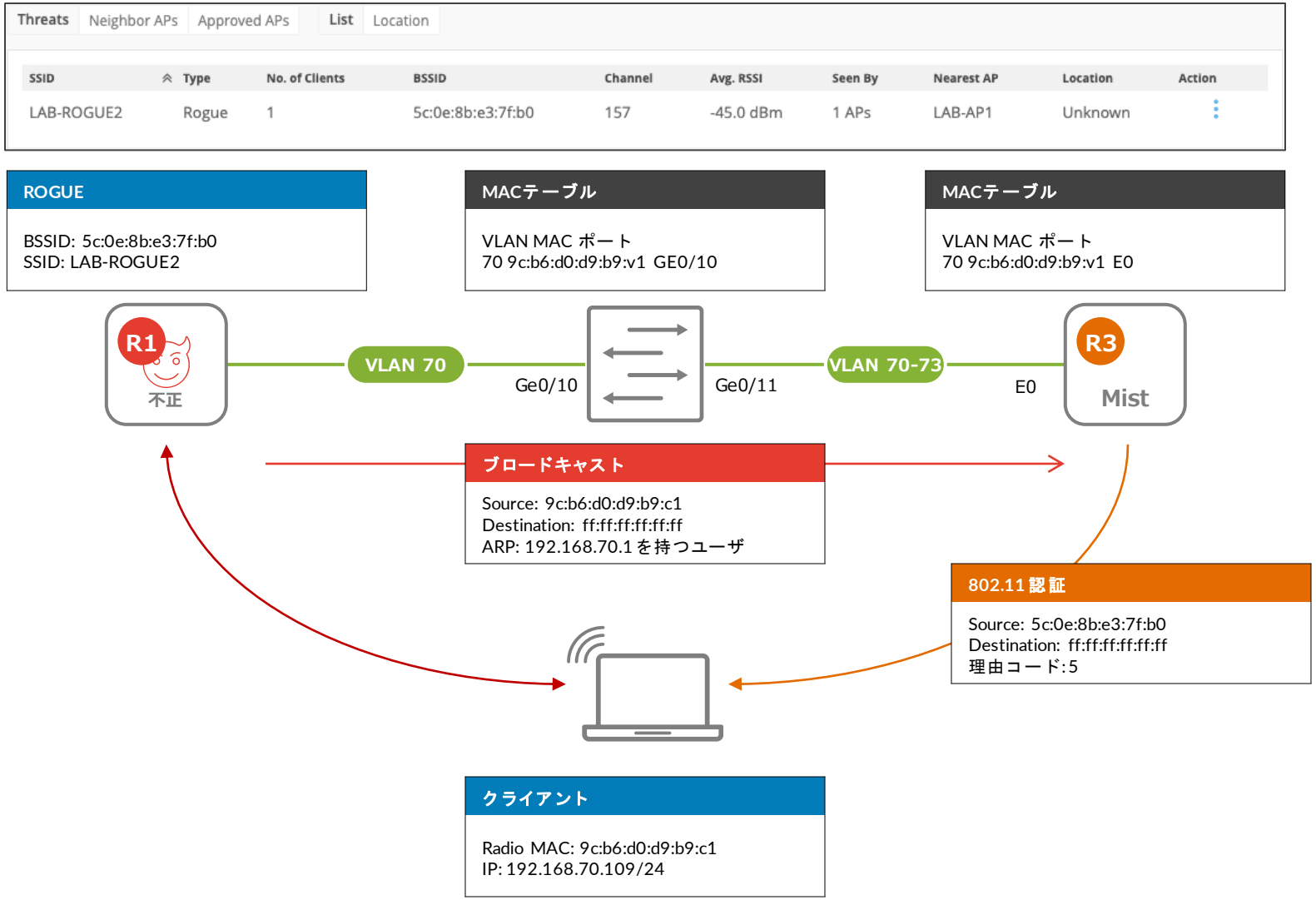




WIDS･WIPS
Q: 不正検知と封じ込めはどのように実行されますか?

特定
- Mist AP は、ブロードキャスト･マルチキャストフレームを学習することで、イーサネットポート上の不正なクライアント MAC アドレスを特定します

切断処理
- センサー専用無線経由で802.11 de-authenticationフレーム (コード 5) をブロードキャストで送信します



WIDS･WIPS
Q: どのような脅威を検出できますか？

ローグ AP 検出に加え、
20 以上の IDS シグネチャをサポートしています

- インフラストラクチャへの脅威
- EAP 攻撃
- フラッディング攻撃
- Man-in-the-Middle 攻撃

脅威

- 不正APへのクライアント接続の検出
- 不正AP検出
- エアーマグネットスキャン検出
- BSSID スプーフィングの検出
- EAP ハンドシェイクフラッド検出
- ハニーポットSSID 検出
- クライアント認証の繰り返し失敗
- Active Watched Station 検出
- アドホックネットワーク検出
- Disassociation Attack 検出
- EAP ディクショナリ攻撃の検出
- EAP Failure インジェクション 検出
- EAP スプーフィング成功検出
- EAPOL-Logoff 攻撃検出
- ESSIDジャック検出
- 過剰なクライアントの検出
- 過剰EAPOL-Start 検出
- 偽AP フラッディング検出
- Monkey Jack 検出
- Out of Sequence 検出
- Replay インジェクション検出 - KRACK Attack
- SSID インジェクション検出
- セキュリティポリシー違反
- TKIP ICV 攻撃
- ベンダーIE 欠落
- ゼロSSIDアソシエーションリクエストの検出

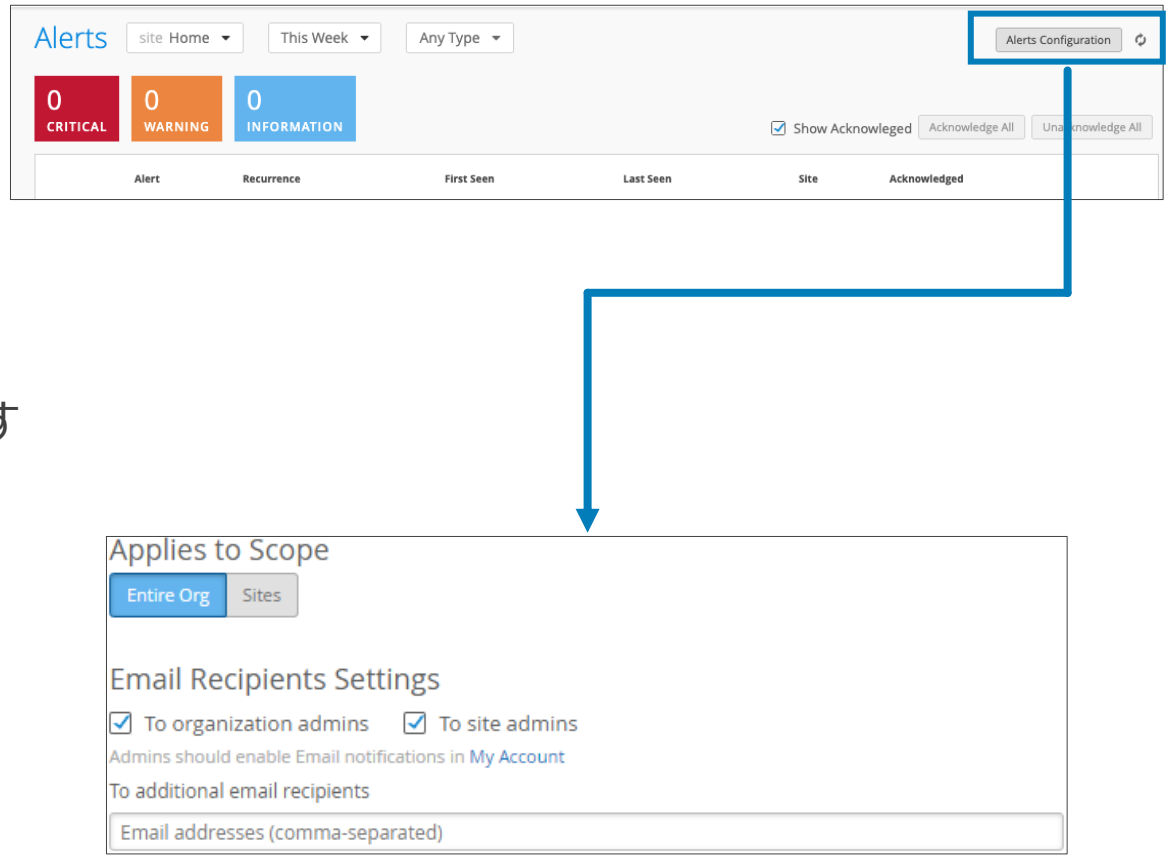
WIDS・WIPS
Q: 脅威が検出された場合、セキュリティチームに通知できますか?

Organization 全体またはサイトごとにアラートを設定可能です

- 各アラートごとにダッシュボードへの表示
  およびEメール通知が可能です

- メールの宛先を柔軟に設定可能です
  (組織管理者、サイト管理者、特定のアドレス)

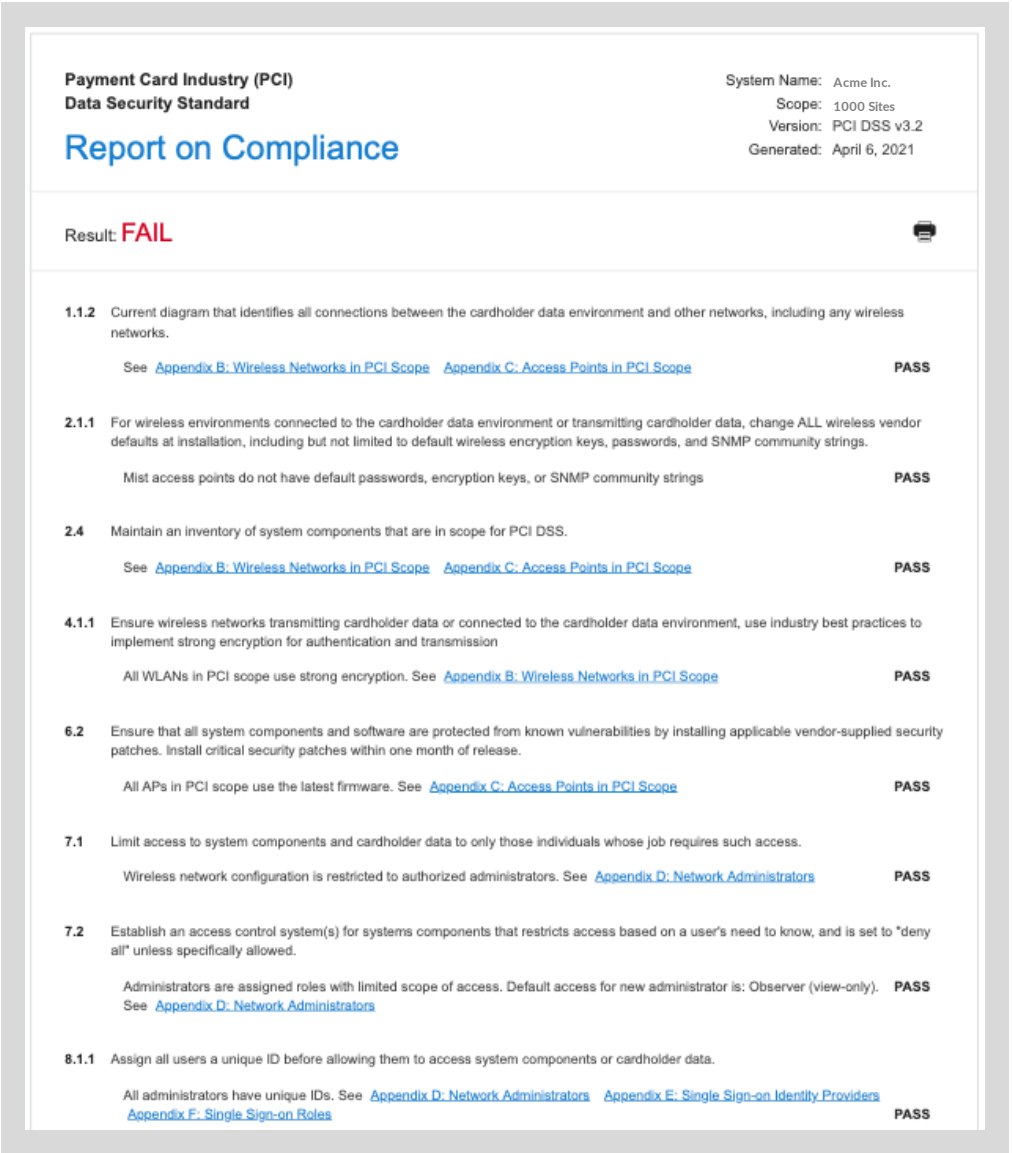
リアルタイムイベントストリーミング用の Webhook を使用して、
サードパーティアプリケーションにアラートを転送することもできます



WIDS・WIPS
Q: PCI レポートを生成できますか?

PCIスキャンレポートを柔軟なスコープで作成可能です

- Organization、Site、Siteグループを自由に選択可能
- カード所有者データを送信する SSID は
  特定の WLAN またはすべての WLAN を選択可能
- カード所有者データの転送には1つ以上の VLAN ID を使用
- 明確なフォーマットで、合格・不合格・理由を表示する
  読みやすいレポートを生成



Payment Card Industry (PCI)
Data Security Standard

System Name: Acme Inc.
Scope: 1000 Sites
Version: PCI DSS v3.2
Generated: April 6, 2021

Report on Compliance

Result: FAIL

1.1.2 Current diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.

See Appendix B: Wireless Networks in PCI Scope Appendix C: Access Points in PCI Scope **PASS**

2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

Mist access points do not have default passwords, encryption keys, or SNMP community strings **PASS**

2.4 Maintain an inventory of system components that are in scope for PCI DSS.

See Appendix B: Wireless Networks in PCI Scope Appendix C: Access Points in PCI Scope **PASS**

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission

All WLANs in PCI scope use strong encryption. See Appendix B: Wireless Networks in PCI Scope **PASS**

6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

All APs in PCI scope use the latest firmware. See Appendix C: Access Points in PCI Scope **PASS**

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

Wireless network configuration is restricted to authorized administrators. See Appendix D: Network Administrators **PASS**

7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

Administrators are assigned roles with limited scope of access. Default access for new administrator is: Observer (view-only). See Appendix D: Network Administrators **PASS**

8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.

All administrators have unique IDs. See Appendix D: Network Administrators Appendix E: Single Sign-on Identity Providers Appendix F: Single Sign-on Roles **PASS**


Thank you
JUNIPER
driven by Mist AI