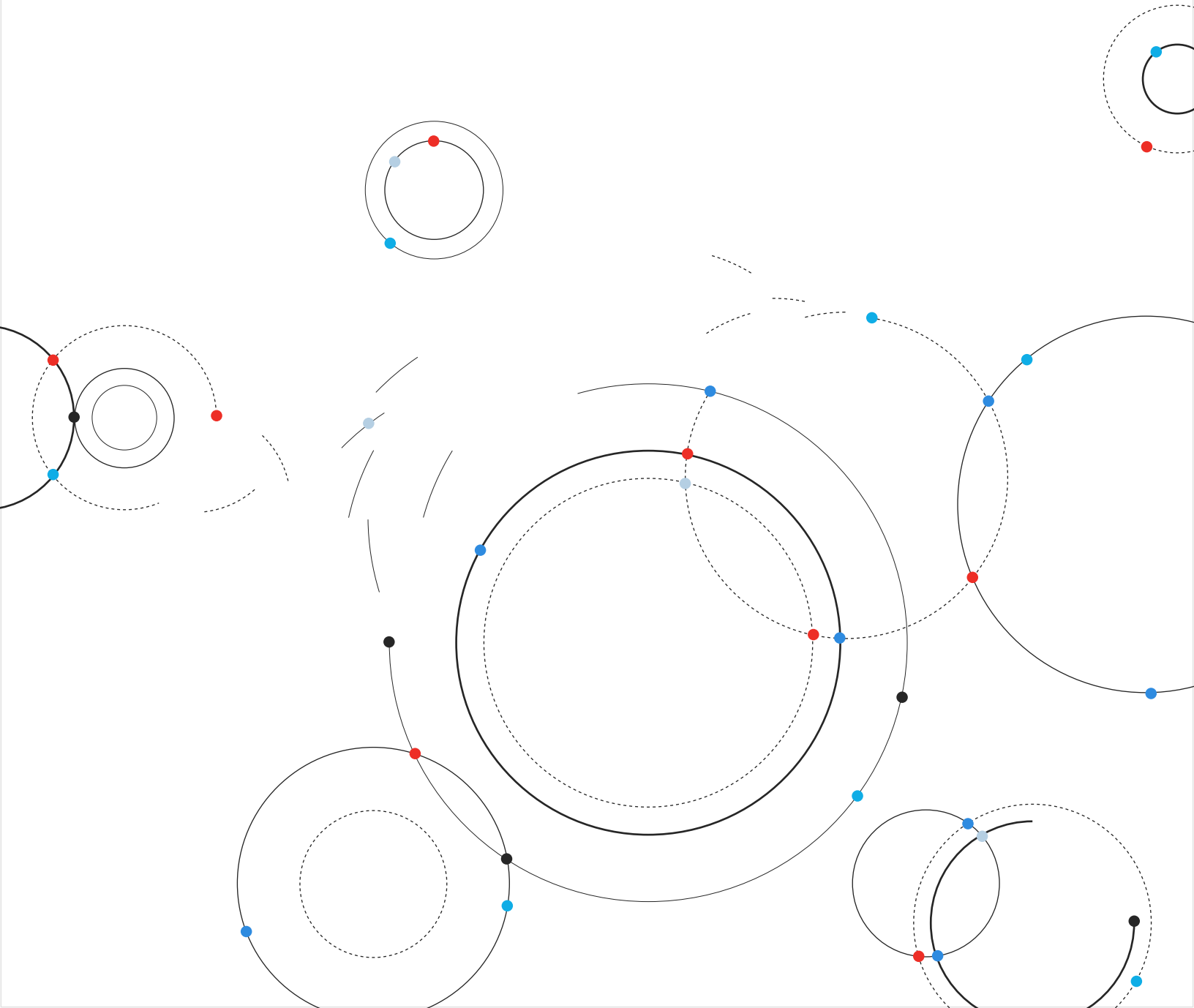
Qualys Threat Research Unit

修復における理論の限界

リスク管理の未来は自律化にある。



序文

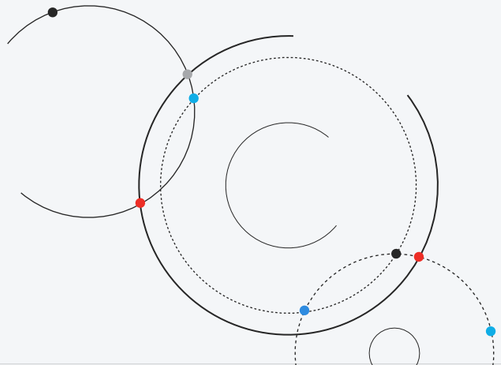
脅威の状況は根本的に変化しており、多くの組織が依存している防御策は、今後待ち受ける脅威に対応できるようには設計されていません。顧客と面談し、彼らが直面している課題を直接聞く中で、私が目にする脅威は、より静かで構造的なものです。 具体的には、チームが管理できる範囲を超えて拡大した攻撃対象領域、ポリシー策定のペースを上回るIDの乱立、そして依然として手動実行に依存した是正ワークフローなどが挙げられます。 企業のリスクを決定づけるのは、ニュースの見出しを飾るようなランサムウェアの亜種や高度なゼロデイ攻撃ではなく、こうした要素なのです。
攻撃者がますますマシンの速度で活動する時代において、人間の速度での対応に依存するアーキテクチャには、構造的なリスクが伴います。

本レポートのデータは、4年間にわたり1万組織に及ぶ10億件以上のCISA KEV修復記録を通じて、この実態を裏付けています。平均的な「悪用までの時間（Time-to-Exploit）」はマイナス1日へと短縮しており、攻撃者はパッチがリリースされる前に脆弱性を悪用しています。重大な脆弱性の件数は6.5倍に急増したにもかかわらず、7日目および30日目に未修正のまま残っている割合は悪化しています。完全な悪用タイムラインを追跡した52件の注目すべき悪用済み脆弱性のうち、 88%は悪用されるよりも遅れて修復されました。その半数は、公開前に悪用されていました。 従来の「パッチ競争」、すなわち「平均修復時間（Mean Time to Remediate）」を短縮すれば攻撃者を追い越せるという考え方は、数学的な限界に直面しています。 一方、公開されたすべてのCVEのうち、確認済みで悪用され、リモートから攻撃可能なリスクは1%未満に過ぎません。
組織は、実際に悪用可能な脆弱性が残っているにもかかわらず、理論上のリスクに対して修復リソースを浪費しています。

その使命は明確です。 自律的な攻撃に対抗するには、自律的な防御を確立しなければなりません。 そのためには、事後対応的な人的トリアージから脱却し、組み込み型インテリジェンス、実際の悪用可能性の確定的な確認、自律的な修復を単一の運用ループに統合した「**リスクオペレーションセンター（ROC）**」へと、アーキテクチャの根本的な転換が必要です。 その目的は、人間の判断を排除することではなく、それを高次なものへと昇華させ、実務担当者が戦術的な行動を実行する役割から、自律システムを導くポリシーの管理へと役割を移行させることにあります。

新たな運用環境へようこそ。

Sumedh Thakar
President and CEO
Qualys



はじめに

本レポートのデータを読む前に、それが測定対象としている攻撃者について理解しておくと役立ちます。

重要なのは攻撃者のタイムラインだけであり、そのタイムラインは予測可能です。 敵対者は革新を行わず、効果のある手法を繰り返します。脅威アクターが複雑な製品の脆弱性を悪用し始めると、1つのCVEで止まることはありません。彼らは、防御側が対応しきれない状態になるまで、そのソフトウェアファミリー全体を体系的に悪用し続けます。本レポートの修復データはこれを反映しています。 未解決の脆弱性のロングテールには、同じ製品クラスが繰り返し登場しますが、それはそれらが未知であるからではなく、運用モデルが迅速にそれらを解消できないためです。

最も侵入しやすい経路は、エンドポイントからエッジへと移行し、さらにそこから、企業が暗黙のうちに信頼を寄せているエンタープライズソフトウェアの深部へと広がっています。 高度な権限を持ち、システムに深く組み込まれており、セキュリティチームが管理しているケースも稀なこれらのシステムは、攻撃者にとって単一のエクスプロイトで最大の成果を得られる対象となっています。 是正措置に関するデータが、その理由を明らかにしています。 これらは、「手作業の負担 (Manual Tax)」が最も大きく、脆弱性が露呈する期間が最も長く、本レポートが指摘する確認のギャップが最も深刻な資産クラスだからです。

その結果は予測可能なものです。 本報告書で記録された対策の不備は、ランサムウェア被害の発生と直接的な関連があります。 しかし、ランサムウェアはあくまで症状に過ぎません。 真の原因は、攻撃者に攻撃の機会を与えた、蓄積され、未解決のまま放置された脆弱性——本報告書で「リスクマス (Risk Mass) 」として測定されているものです。

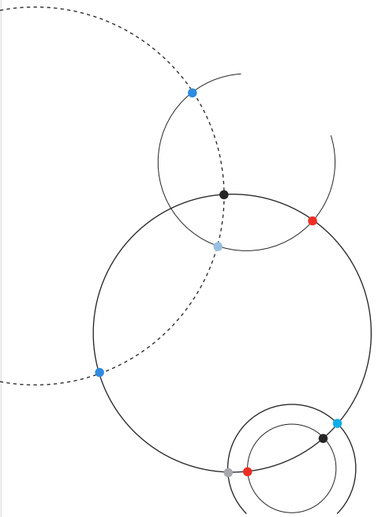
サイバーセキュリティの各世代は、プラットフォームの変革に対応して登場してきました。新しい技術が新たなリスクを生み出し、防御側はそれに適応してきました。 そのサイクルは直線的で、対処可能なものでした。 しかし、今まさに起こりつつあるのは、単なるプラットフォームの変革ではありません。 敵そのものが自律化しつつあるのは、これが初めてのことです。

今や、攻撃側の主体は、人間が関与するいかなる運用よりも迅速に、脆弱性を発見し、悪用し、攻撃を実行できるようになっています。 防御側も同様の変革を遂げなければなりません。そして本レポートでは、その変革が遅れるごとに生じるコストを算出しています。

以下に、それを裏付けるデータを示します。

Saeed Abbasi
Head of Threat Research Unit
Qualys

目次



Qualys脅威調査ユニット

エグゼクティブ・サマリー

2025年9月に公開されたGoogle Threat Intelligence Group（GTIG）による「2024 Time-to-Exploit Trends」の分析によると、平均エクスプロイト化までの時間（TTE）はマイナス1日にまで短縮された。

攻撃者は、パッチがリリースされる前、あるいは脆弱性が公表されたその瞬間に、脆弱性を悪用してシステムを侵害している。

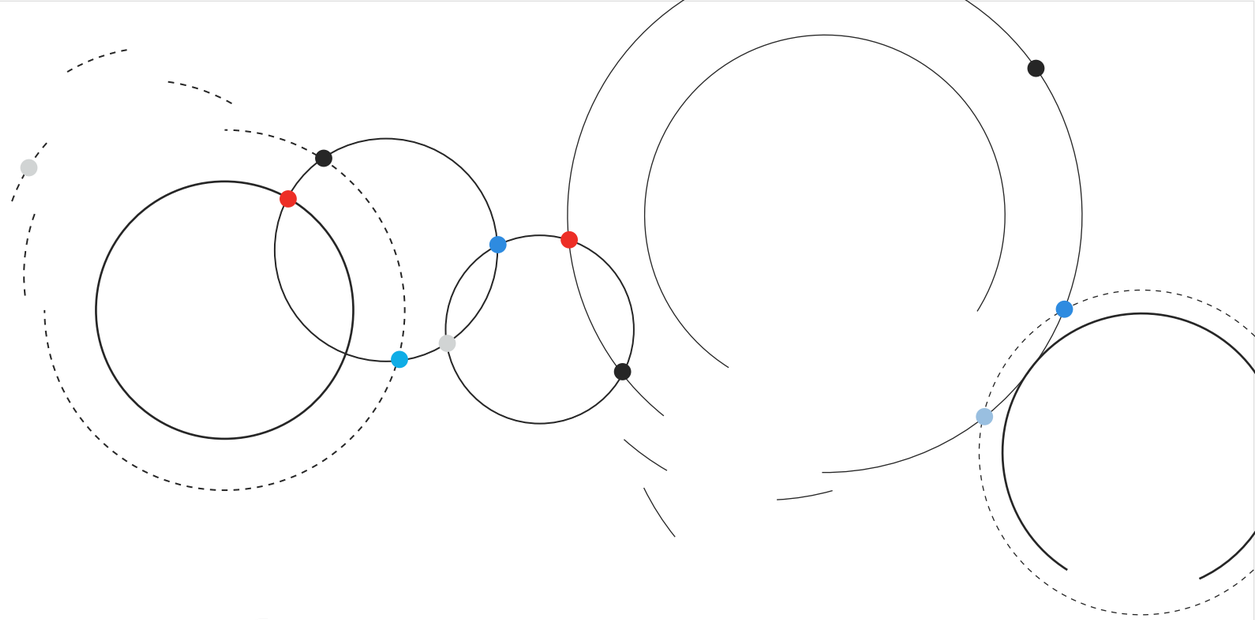
これは、脆弱性対策の運用モデルにおける根本的な崩壊を意味している。

この10年間、業界は「パッチ競争」という前提の下で動いてきました。つまり、MTTR（平均修復時間）さえ短縮できれば、敵に先んじることができるという考えです。「数ヶ月」かかる解決策では、「数分」の問題を解決することはできません。

本レポートでは、1万社以上の組織における10億件を超えるCISA KEV修復記録（2022年～2025年）を分析し、拡大するギャップを数値化しています。 KEVの脆弱性件数が6.5倍に増加した一方で、7日目になっても未解決のままの重大な脆弱性の割合が増加していることを示しています。これは、手動による修復には限界があることを証明するものです。 本レポートでは、MTTRを補完する指標として「平均エクスポージャー期間（AWE）」と「リスクマス」を導入します。 これらは、対応速度だけでなく、大規模な環境における累積的な露出度も捉える指標です。

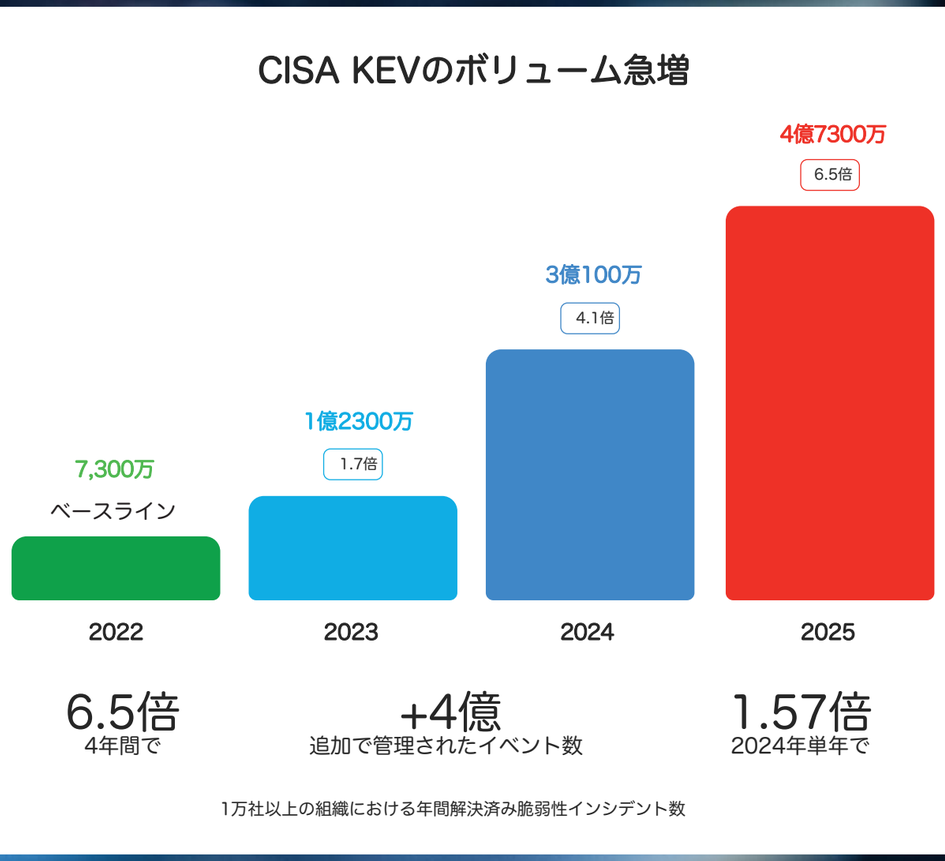
調査結果はさらに踏み込んだ内容を示しています。 悪用可能性が極めて高いと評価された脆弱性であっても、確認テストの結果、是正措置を考慮すると、実際に検証されたリスクをもたらすのはごく一部に過ぎないことが判明しました。 つまり、組織はすでに軽減済みの脅威に対して是正措置を講じている一方で、真に悪用可能な脆弱性は依然として残っているのです。

攻撃の速度が加速する中――敵対勢力がAIを活用し、偵察、攻撃手段の構築、攻撃の実行を機械並みの速度で自動化する傾向が強まるにつれ――人間の介入は単に遅くなるだけでなく、第一の防衛ラインとして構造的に不適合なものとなりつつあります。 進むべき道は明らかです。 それは、リスクオペレーションセンター（ROC）アプローチによるエンドツーエンドの運用化された是正措置――検知から検証、そして対応に至るまでの全サイクルを自動化することです。 リスクへの「モグラたたき」的な対応は、スケールしません。 脅威環境が依然として許容する唯一の対応策は、反復可能でマシンスピードでの運用化です。



1 人間による修復の限界

手動による修復作業は、もはや存在しない世界のために考案されたものでした。 それは、脆弱性の数が直線的に増加し、エクスプロイトのタイムラインが数週間単位で測定され、十分な人員を擁するチームであれば、優先順位付け、パッチ適用という手順を踏んで安全を確保できると合理的に期待できた世界です。 その世界は、7,300万件目から4億7,300万件目の修復作業の間のどこかで、静かに幕を閉じました。



脆弱性に関する対応が完了した件数は、脆弱性件数の増加と組織全体の対応範囲拡大の両方によって、4年間で6.5倍に増加し、2022年の約7,300万件から2025年には4億7,300万件に達した。

人間の限界

2022年から2025年にかけて、1万社以上の組織における10億件を超えるCISA KEV脆弱性修復記録を分析しました。 このデータセットは、これまで実施された企業における脆弱性の修復行動に関する縦断的研究の中でも最大規模のものです。 各記録は、単一のアセット上で検出された単一の脆弱性事例を表しており、検出から修復完了までの経過を追跡したものです。

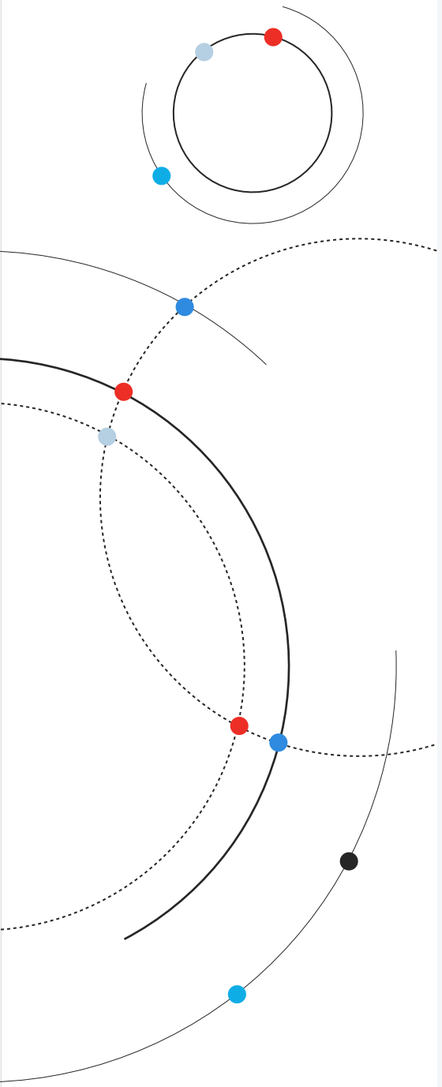
この分析からは、人員の増強、プロセスの成熟度、あるいは経営陣の緊急性といった要素をいくら高めても克服できない構造的な限界が明らかになりました。

解決済みの脆弱性インシデントの件数は、脆弱性の総数が増加したことに加え、対象となる組織の範囲が拡大したことも相まって、4年間で6.5倍に増加しました。 具体的には、2022年の約7,300万件から2025年には4億7,300万件へと増加しています。

その増加分を考慮しても、7日目に未修正のまま残っているCISA KEVにおける重大な脆弱性の割合は改善されませんでした。 むしろ悪化し、2022年の56%から2025年には63%へと上昇しました。

これが人的リソースの限界です。 各チームはより懸命に働き、絶対数としてはより多くのチケットを処理しましたが、新たに発生するリスクのペースが、是正措置のペースを上回ってしまいました。

未処理案件は減るどころか、さらに積み重なっていったのです。 悪用可能なリスクが6.5倍に増加したからといって、人員を6.5倍に増やして対応することは不可能です。 仮にそれができたとしても、データによればそれだけでは不十分であることが示されています。
制約となっているのは「努力」ではありません。 それは、運用モデルそのものなのです。



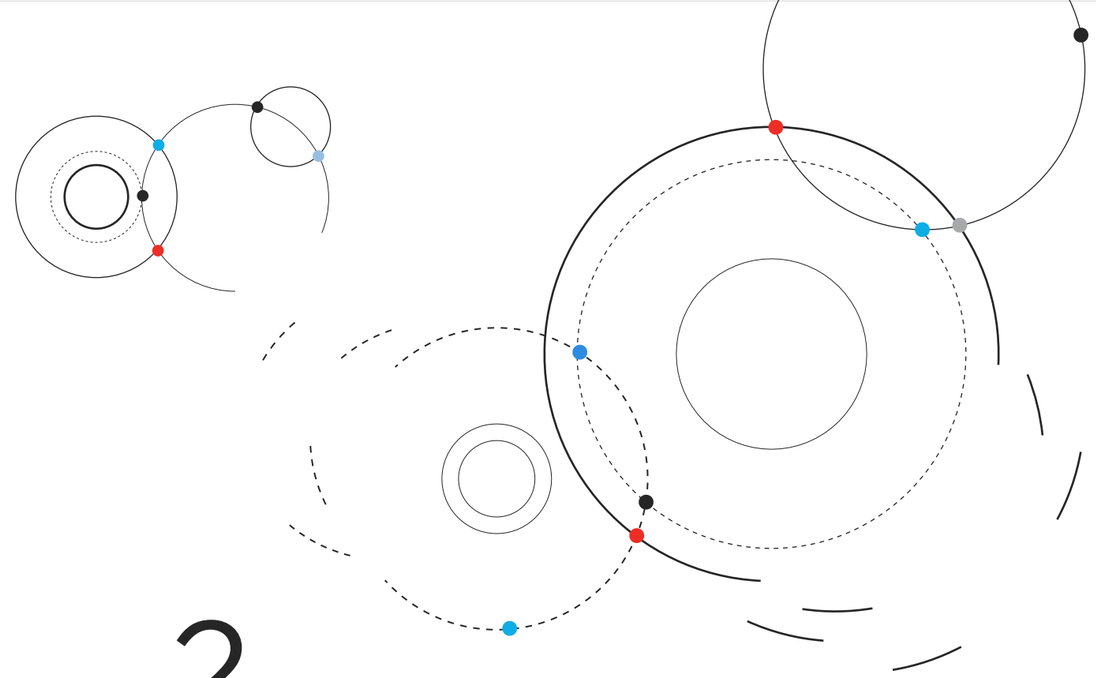
インテリジェンスの重要性

修復スケジュールの破綻には、あまり議論されていないものの、同様に緊急性を要する二次的な影響が伴います。 それは、運用上の修復判断を行うために脅威インテリジェンスをどのように活用すべきかという在り方を根本的に変えるということです。

戦略的な脅威インテリジェンス（攻撃者の属性分析、TTPマッピング、攻撃者の動機、攻撃キャンペーンの追跡など）は、セキュリティプログラムにとって依然として不可欠です。 これは防御アーキテクチャの策定、投資優先順位の決定、脅威ハンティングの指針となり、自動化システムでは再現できない状況理解を提供します。

変化したのは運用レイヤー、つまりインテリジェンスを特定の資産に対する具体的な是正措置へと転換しなければならない段階です。是正措置が人間主導のプロセスであった時代には、戦術的インテリジェンスは人間による伝達経路を経由することが許容されていました。つまり、アナリストがレポートを読み、その関連性を解釈し、ワークフローへと回すという流れです。 このモデルは、洞察から行動に至るまでに時間的余裕があることを前提としていました。しかし、「Time-to-Exploit（悪用までの時間）」が「-1日」となった現在、運用上の是正措置の決定において、その前提はもはや成り立ちません。

この戦術的レイヤーにおいては、インテリジェンスは、是正措置の決定が行われるプラットフォームに直接組み込まれる必要があります。 インテリジェンスは、環境固有のコンテキストを伴って提供されなければなりません。 単に「このCVEが実環境で悪用されている」というだけでなく、「このCVEが悪用されており、貴社の環境にも存在し、現在の対策ではこれを軽減できず、取るべき措置はこれである」という形で提供される必要があります。情報は、機械が解析できるほど構造化されており、自律的な意思決定を促すほど具体的でなければなりません。 戦略的インテリジェンスはプログラムの方向性を示し、機械の速度で提供される運用インテリジェンスは具体的なアクションを導きます。 両者とも不可欠です。しかし、特に修復パイプラインにおいては、人間の速度でのルーティングではもはや十分とは言えません。



2
修復における理論の崩壊

MTTR（平均修復時間）が、業界における標準的な修復指標としての地位を確立しているのは、それなりの理由があります。 この指標は、現実的かつ運用上重要な要素、すなわち脆弱性が修復プロセスに入った後、セキュリティチームやITチームがどれほど迅速に対応するかを測定するものです。

運用効率を測る指標として、MTTRは依然として有用であり、チームの対応が速くなっているか、SLAが遵守されているか、そしてプロセスの改善が効果を上げているかを示してくれるからです。

MTTRが測定するようには設計されていないのが、ビジネスリスクへのエクスポージャーです。MTTRは、最初のチケットが作成される前に何が起きたか、修復作業が行われている間、環境がどれだけの期間リスクにさらされていたか、あるいは平均値を算出している間にパッチが適用されずに残っていたすべての資産が被った複合的なリスクを捉えることはできません。MTTRは対応の速さを測定するものであり、リスクへの曝露期間を測定するものではありません。 エクスプロイトのタイムラインがゼロに近づき、さらにはゼロを下回るにつれて、この区別は運用上極めて重要になります。 それは、MTTRが誤った指標だからではなく、取締役会や経営陣がますます回答を求めているリスクに関する問いに対して、MTTRが不完全な指標であるからです。

平均エクスポージャー期間（AWE）

AWEは、MTTRが見落としている点、すなわち脆弱性が悪用可能になってから環境全体で修復が完了するまでの全期間を捉えます。 これは、最後のスプリントだけでなく、レース全体を測定するものだと考えてください。 攻撃者が1日目に侵入し、パッチ適用が21日目に完了した場合、AWEは21日となります。 もしMTTRが「8日」と示していたとしたら、それは最も迅速な対応と最も遅い対応を平均化したものであり、資産の3分の1が数週間後も依然として危険にさらされていたという事実を覆い隠す単一の数値を生み出していたことになります。

業界が是正措置の効果を定量化する方法における構造的な盲点を解消するため、Qualysの社長兼CEOであるSumedh Thakar氏は「平均エクスポージャー期間（AWE）」を考案しました。 MTTRが運用上のスピード（チームがチケットをどれだけ速く解決するか）を測定するのに対し、AWEは全資産群にわたる戦略的なリスク露出を測定します。

この区別は単なる学問的な議論ではありません。エクスプロイトのタイムラインがゼロデイの閾値を超えて短縮されるにつれ、「いかに迅速に対応したか」と「どれだけの期間、脆弱性にさらされていたか」との間のギャップは、プロセスを評価する指標とリスクを反映する指標との違いとなります。 AWEはこのギャップを埋めるものであり、悪用可能状態から修復完了に至るまでの全期間を捕捉します。

全体にわたる戦略的なリスクを測定し、平均化によって本質的に隠蔽されがちな「ロングテール」のリスクを可視化するものです。

GTIGが実環境で悪用された112件の脆弱性を分析した2024年の調査によると、「悪用までの平均時間（Average Time-to-Exploit）」はマイナス1日へと急激に短縮したことが判明しました。 つまり、現在、積極的に悪用されていることが確認された脆弱性については、平均して、パッチが提供される前に武器化が行われているということです。

防御側の時計は、異なる物語を語っています。2025年のCISA KEV重要脆弱性に対する当社のサバイバルカーブ分析によると、開示時点で、脆弱な資産の85%は未修正のままです。 1週間後には63%です。平均的な修復完了時期である約21日時点では、3つの資産のうち1つ、つまり33%が依然として無防備な状態です。そして90日後には、攻撃対象領域の12%近くが依然として残存しています。

注目すべきは、KEV導入前に15%の脆弱性を修復していた組織は、単なる事後対応的な修正の段階をすでに脱しているという点です。 これらの組織は、TruRiskなどのスコアリングシステムによるリスクベースの優先順位付けや、高度な修復機能を活用し、実際に悪用されていることが確認される前に、悪用される可能性の高い脆弱性に対処しています。 これらは、脆弱性修復のタイムラインを短縮することが可能であることを示す好例です。 もっとも、こうした組織は少数派に過ぎません。

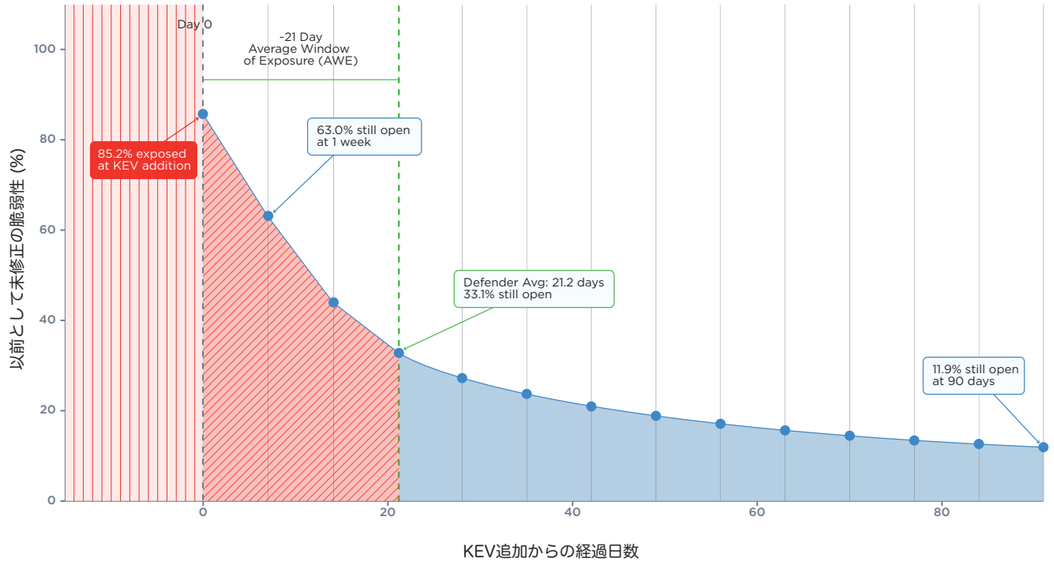
侵害の期間

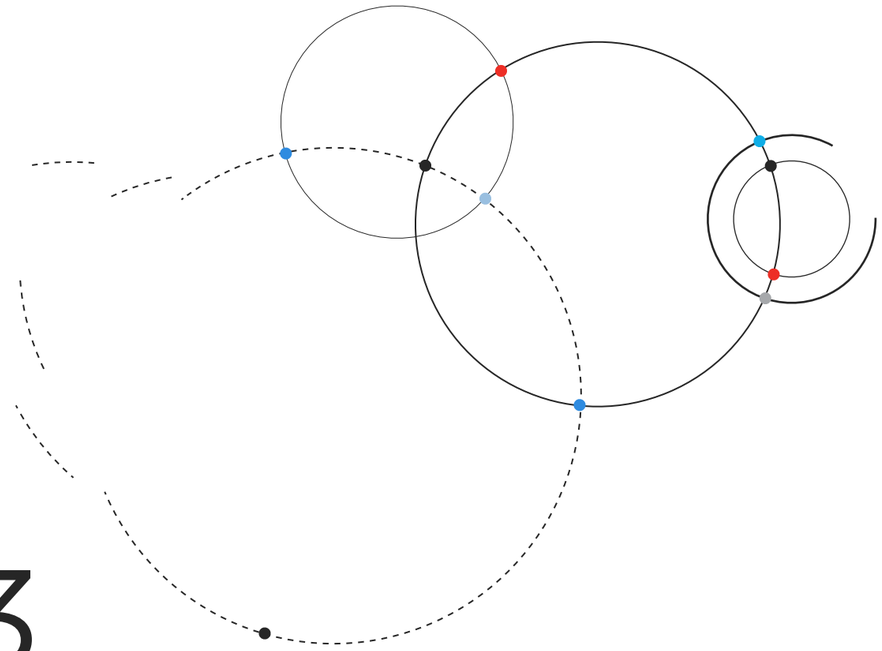
生存曲線の下にある網掛け部分は、単なる抽象的な概念ではありません。 これは、修復作業が完了しない日ごとに組織が被る累積的なリスク、つまり本レポート第4章で詳しく解説する「リスクマス (Risk Mass)」を表しています。この曲線上のすべての点は、潜在的なリスクを示しています。 最初の低下が急であればあるほど、初期対応の自動化は効果的であることを示しています。 曲線の裾野が長ければ長いほど、ダッシュボードでは把握できない累積リスクが大きくなります。

防御側は「Day 0」から修復作業を開始します。しかし、重大なゼロデイ脆弱性の大部分において、攻撃者はすでにそこに潜んでいます。 この2つのスタートラインの間のギャップ、そして修復プロセスの終盤における緩やかな減衰こそが、セキュリティ侵害が発生する場所です。手動による加速では、いかなる手段を用いてもこのギャップを埋めることはできません。自動化され、運用化された是正措置のみが、結果を変化させるのに十分な速さでこの曲線を圧縮できるのです。

侵害の期間：平均エクスポージャー期間（AWE）

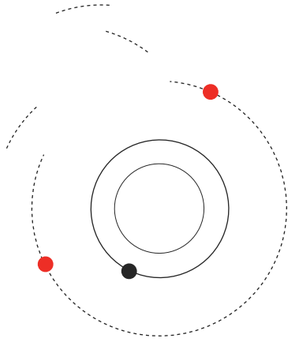
攻撃側の攻撃速度と防御側の是正速度 - セキュリティ侵害が発生するギャップ





3 「物理的ギャップ」攻撃側の速度 vs. 防御側の速度

前のセクションでは、平均的な企業が重大な脆弱性を21日間放置している一方で、攻撃者は1日未満で悪用していることが明らかになりました。本セクションでは、当社の脅威インテリジェンス（複数の商用および独自情報源によって裏付けられたもの）が、最初の悪用日が確認された完全な悪用タイムラインを維持している、52件の個別のCISA KEV脆弱性について、この不均衡がどのようなものかを検証します。この対象群は、無作為抽出ではなくインテリジェンスの完全性に基づいて定義されているため、より広範な研究の注目を集めた、注目度の高い脆弱性に偏っている可能性がある。その点を考慮しても、この格差は集計統計が示唆するよりも深刻である。 これらの脆弱性の半数は、公開前に悪用されていた。残りの脆弱性についても、防御側は依然として対抗措置の大部分で敗北を喫している。



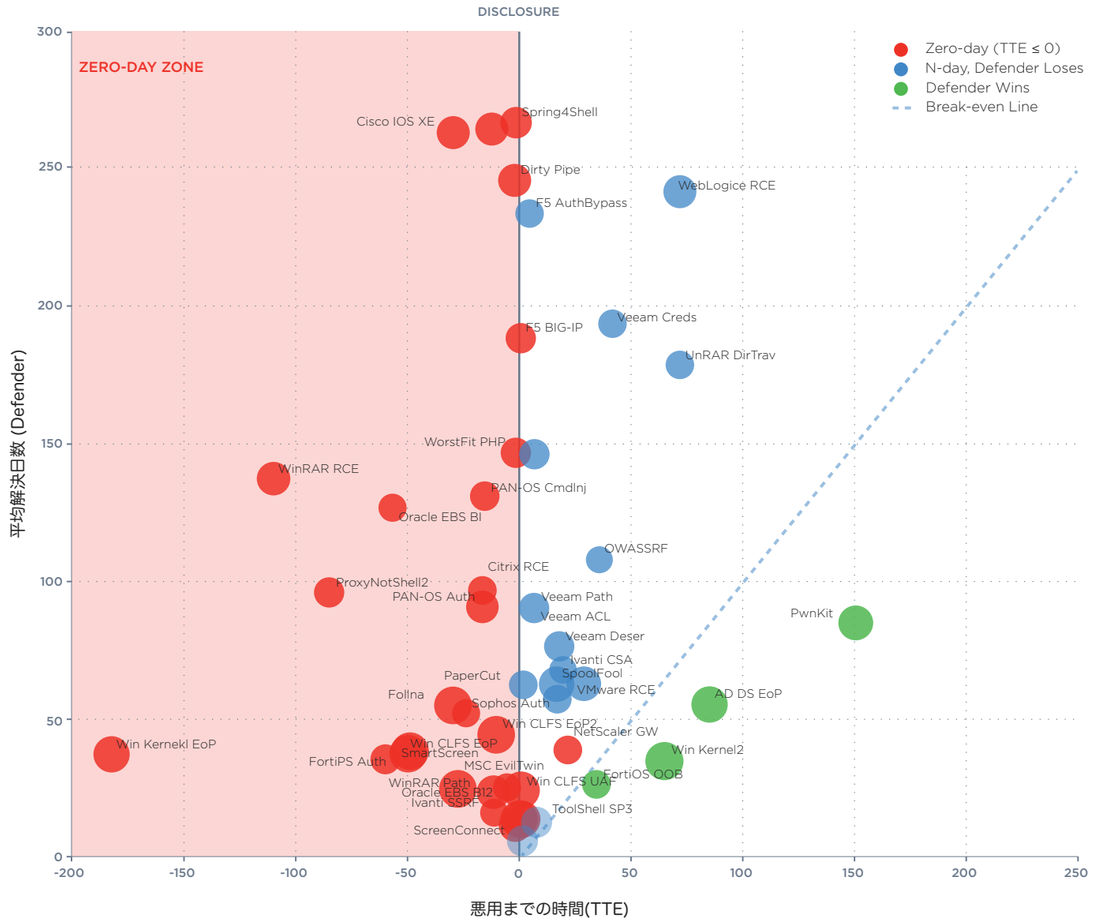
理論のギャップを読み解く

この散布図は、52件の脆弱性を2つの軸上にプロットしたものです。横軸はTTE（Time-to-Exploitation）を示しており、脆弱性が公開されてから最初の悪用が確認されるまでの日数を表しています。

縦軸は、組織が脆弱性を修正するのに要した平均日数を示しています。 対角線上のブレークイーブンラインは均衡点を表しています。脆弱性がこのライン上に位置する場合、防御側のパッチ適用速度と攻撃側の悪用速度が完全に一致したことを意味します。 ラインより上なら攻撃側の勝利、下なら防御側の勝利となります。

その結果は極めて厳しいものです。 このデータセットに含まれる脆弱性の88%が損益分岐点を上回っています。
つまり、過去4年間に発見された最も深刻で、実際に悪用されている脆弱性の大部分について、平均的な組織がパッチを適用する速度は、攻撃者が悪用する速度よりも遅かったということです。 バブルの大きさは、数百万件に及ぶ脆弱なインスタンス全体におけるリスクの規模を反映しています。 これらはKEVカタログ内の孤立した例外ではありません。 企業のリスクを定義する「武器化された脅威」というカテゴリーにおいて、この「逆転した物理法則」こそが常態なのです。

物理的ギャップ：攻撃者の速度 vs. 防御側の速度



ゼロデイ・ゾーン

52件の脆弱性のうち26件（ちょうど半数）はTTEが負の値となっており、これはCVEが公開される前に悪用が行われていたことを意味しています。

さらに3件は、公開当日に悪用されました。修正プログラムの基盤となる「Day 0」というスタートラインは、こうした重大な脅威の大部分にとって、競争の始まりを表すものではありません。 それは、防御側がすでに後手に回っていることに気づく時点を表しているのです。

公開前の悪用事例の規模は大きく異なります。 Win Kernel EoP（CVE-2024-21338）は、公開の182日前に悪用されました。 WinRAR RCE（CVE-2023-38831）は、110日前に武器化されました。 ProxyNotShell (CVE-2022-41040) および関連する脆弱性は、アドバイザリの公開より85日前に悪用されました。 FortiOS Auth (CVE-2024-55591) は、公開の60日前に武器化されました。Follina (CVE-2022-30190) は、公開の1ヶ月前に悪用されました。 その他 — SmartScreen、Oracle EBS、Win CLFS EoP、MSC EvilTwin、Sophos Auth、Citrix RCE、PAN-OS CmdInj、PAN-OS Auth、ActiveMQ、Cisco IOS XE — はすべて、防御側がその存在を公に知る数日から数週間前に悪用されていました。

ゼロデイ・ゾーンが特に深刻な被害をもたらす理由は、単に攻撃者が先行しているからだけではありません。 パッチが公開された後に何が起こるかが問題なのです。 Cisco IOS XEはDay 0の30日前に悪用され、平均的な修復期間は263日を要しました。

ActiveMQのRCEは15日早く悪用され、平均的な修復完了まで459日でした。　Spring4Shellは公開の2日前に悪用され、平均的な修復完了まで266日を要しました。　攻撃者の優位性は数日または数週間単位で測定されましたが、防御側の対応は数ヶ月または数年単位で測定されました。

Qualys脅威調査ユニット

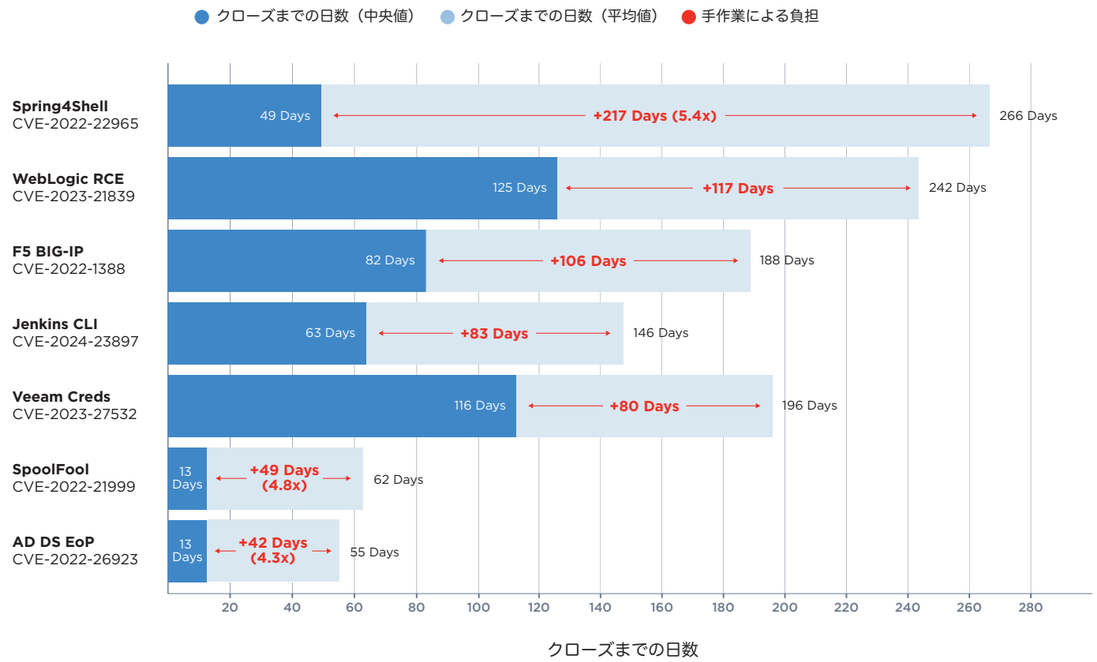
手作業の負担

是正措置にかかる時間の中央値と平均値の差からは、データセット全体にわたり一貫した傾向が見て取れます。私たちはこれを「手作業の負担（Manual Tax）」と呼んでいます。 これは、手作業によるプロセスでは迅速に対応しきれない、資産のロングテール部分によって生じるコストです。

「手作業の負担」は固定値ではなく、倍率として表されます。 Spring4Shellの場合、平均値は中央値の5.4倍です。 SpoolFoolの場合は4.8倍、AD DSの権限昇格については4.3倍です。 分布の下位半分——忘れ去られたサーバー、リモート接続のノートPC、シャドーIT、次のスプリントに先送りされた資産——は、組織内で最もパフォーマンスの高いチームに比べて4〜5倍の時間を要します。 チケットの上位50%はダッシュボード上では妥当に見えるペースで解決されますが、残りのテール部分によって、実際のリスクへの曝露期間が3〜9ヶ月も引き延ばされてしまいます。

一部の脆弱性については、中央値ですら遅すぎです。 Cisco IOS XE（TTE：-30日、中央値：232日）、ActiveMQ RCE（TTE：-15日、中央値：530日）、F5 AuthBypass（TTE：4日、中央値：231日）などがある。 これらのケースでは、開示の数週間あるいは数ヶ月前に悪用されていた脆弱性を修復するのに、上位50%の組織でさえ7ヶ月から17ヶ月を要しました。

手作業の負担：クローズまでの日数（中央値）と（平均）の比較



インフラの格差

手作業の負担は均等に分散されていません。 52件の脆弱性を資産の種類別に分類すると、3つの異なる是正の現実が浮かび上がります。 それぞれに異なる運用アプローチが求められます。

エンドポイントおよびクライアント側の資産は、最も迅速にパッチが適用されます。 脆弱性1件あたり1,200万件を超えるイベントが発生する場合でも、修復完了までの期間の中央値は常に14日未満に収まっています。

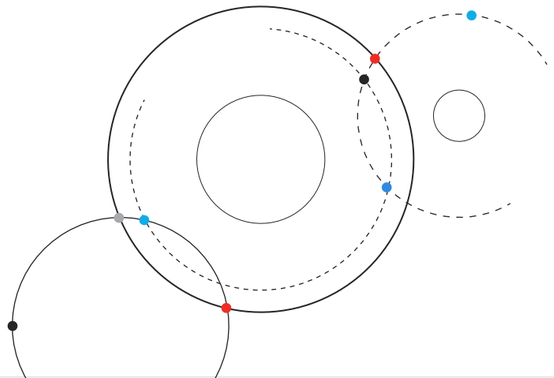
これらの資産には自動化されたパッチ適用インフラが整備されており、確実に機能しています。 エンドポイント運用における優先課題は、このスピードの優位性を、公開前の検知および緩和機能によってさらに拡大することです。 そうすることで、公開前に悪用される脆弱性の増加に対しても、同様の効率で対処できるようになります。

エッジおよび境界デバイス（ファイアウォール、VPN、ゲートウェイなど）は、脆弱性1件あたりの戦略的リスクが最も高いです。 これらはインターネットに面しており、内部ネットワークへの直接アクセスを提供しており、このデータセットの大部分は公開前に悪用されていました。こうした資産については、包括的かつ継続的に更新される資産インベントリが基盤となります。

組織は、見えないものを保護することはできません。その基盤の上に、悪用からパッチの提供までの期間におけるリスクを低減するためには、補完的な制御策と緩和策の層が不可欠です。

インフラストラクチャおよび基幹システム（ミドルウェア、アプリケーションサーバー、バックアップインフラ、ネットワーク機器）は、修復において最も困難な課題となっています。 インフラストラクチャの脆弱性に対する修復完了までの期間の中央値は、常に数ヶ月に及んでいます。 具体的には、Cisco IOS XEが232日、F5 AuthBypassが231日、WebLogic RCEが125日、Veeam Credsが116日です。これに対し、エンドポイントの修復期間の中央値は常に14日未満に収まっています。 この差は構造的なものであり、変更ウィンドウ、ダウンタイムの制約、手動による更新プロセスによって引き起こされています。 ここに「ロングテール」が存在し、手動作業による負担が最も重くのしかかっています。

3つのカテゴリーすべてを統合した単一の是正指標を報告すると、リスクポスチャーにおける重要な違いが見えにくくなる可能性があります。 エンドポイントの速度、境界の可視性、インフラストラクチャの深度という各軸において、自社がどの位置にあるかを把握することが、平均値ではなく実際のリスクに対処する是正戦略を策定するための第一歩となります。



Qualys脅威調査ユニット

ギャップを埋める:
緩和策を修復レイヤーとして活用する

パッチ適用サイクルが数週間から数ヶ月単位となるインフラストラクチャ環境においては、パッチ適用だけではセキュリティ上の脆弱性が露呈する期間を完全に解消することはできません。 パッチは依然として決定的な修復手段ですが、こうした資産のタイムラインを考えると、チームはパッチが 変更承認やメンテナンスウィンドウを経る間にリスクを低減するため、ネットワークレベルの封じ込め、仮想パッチによるホストの隔離、トラフィックの遮断、および代償的制御といった追加の対応層を導入する必要があります。 AWEが数時間で測定され、パッチサイクルが数ヶ月単位である場合、その間のギャップを能動的な緩和策で埋める必要があります。

無駄になった先行優位性

ゼロデイ攻撃による損失は、ある意味では技術的な失敗と言えるでしょう。 パッチが存在しなかったからです。 しかし、データからは、より大きなコストがかかり、しかも予防可能だったはずの失敗パターンを明らかにしています。 それは、防御側が十分な警告を受けていたにもかかわらず、結局は敗北してしまった「nデイ」の脆弱性です。

WebLogicのRCE（CVE-2023-21839）は、公開から71日後に初めて悪用されました。 組織が対策を完了するまでには平均242日を要しました。 この2か月の先行期間は、架空の攻撃者によって無駄にされたのではなく、実在する攻撃者によって活用されてしまったのです。 中国を拠点とする暗号通貨マイニング脅威アクター「Water Sigbin」（「8220 Gang」としても追跡されている）は、この脆弱性を悪用し、PowerShellベースのローダーを展開してXMRig暗号通貨マイニングマルウェアを大規模に配布しました。

この同じ脆弱性は、ロシアのランサムウェア・アズ・ア・サービス（RaaS）エコシステム内で活動する金銭目的のアクター「Prophet Spider」によっても悪用されました。 国家主体の動機と犯罪的な動機を持つ2つの異なる脅威アクターが、いずれもパッチが2ヶ月以上前から公開されていた脆弱性を悪用したのです。

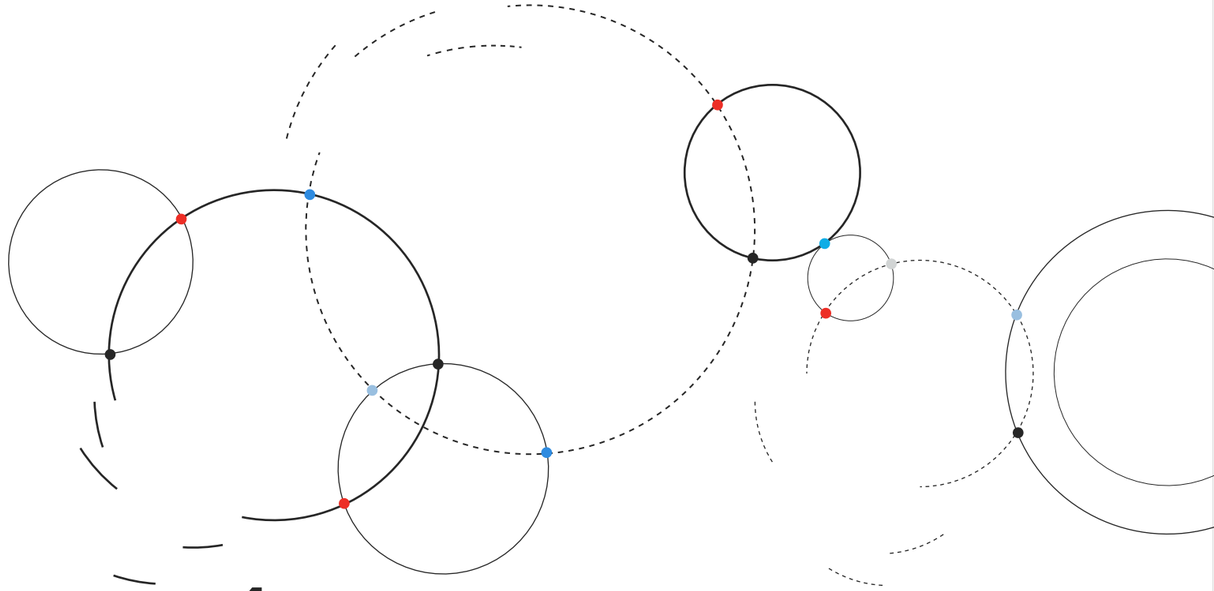
UnRARのディレクトリトラバーサル（CVE-2022-30333）は、発見から70日目に初めて悪用され、防御側が修復を完了するまで平均178日を要しました。 この脆弱性は、2022年半ばに登場し、Cl0p、BlackCat/ALPHV、Ryuk を含む複数のランサムウェア・アズ・ア・サービス（RaaS）グループと活動上のつながりを持つ金銭目的の脅威アクター「ShadowSyndicate」や、侵入チェーンの一環としてこの脆弱性を悪用したランサムウェアグループ「MalasLocker」が注目しました。

繰り返しになりますが、これらは国家レベルの資源を必要とするような高度なゼロデイ攻撃キャンペーンではありません。 パッチが存在する既知の脆弱性を悪用し、修復プロセスが未完了の組織を標的とした、機会主義的な攻撃者によるものです。

こうした見逃された好機こそが、運用改善において最も高いROIが見込める対象です。 なぜなら、パッチは存在し、攻撃者は特定され、攻撃の手口も記録されていたにもかかわらず、迅速に修復を適用する仕組みだけが欠けていたといえます。 これはインテリジェンスの失敗ではなく、運用面での失敗であるといえます。

「観測」から「排除」へ

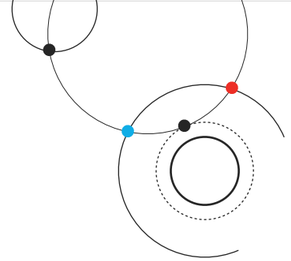
このセクションのデータは、脆弱性を観測することと、それを排除することは別物であることを証明しています。 リスクオペレーションセンター（ROC）のアプローチは、そのギャップを埋めるものです。 つまり、CVE件数の受動的な監視から、 運用化されたリスク排除へと移行するのです。 具体的には、資産のコンテキストを統合し、ビジネス用語でリスクの程度を定量化し、修復と緩和策を機械並みのスピードで調整します。
攻撃者と防御者の力関係が不均衡であるため、手動のプロセスではこうした対峙の大部分で敗北することが確実である以上、検知から対応に至るまでの全サイクルを自動化することこそが、唯一の実効性のある対応策となります。



4
リスクマス：脆弱性数のカウントからリスクの測定へ

多くの組織が是正措置の成果を測定するために依存している指標には、共通の欠点があります。 それは、単に事象の数を数えているだけだということです。 従来の是正措置の指標は、脆弱性が修正されたかどうか、そしてどのくらいの速さで修正されたかという2つの点を的確に捉えています。 しかし、脆弱性が未修正のままであった間に組織が被った累積的なリスクは捉えられていません。 1日で修正されたCVEも、6ヶ月かけて修正されたCVEも、どちらも「修正済み」として記録されます。 しかし、後者の場合、組織は180倍もの悪用されるリスクを抱えていたことになります。 これは、水位を測定するのではなく、豪雨の回数を数えて洪水被害を測定するようなものです。 回数は何かが起こったことを示しますが、累積的な影響については何も教えてくれません。

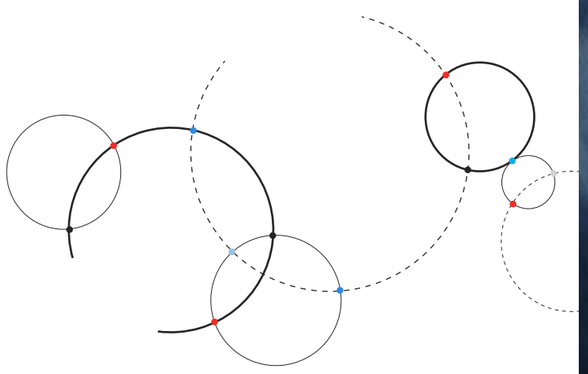
深刻度スコアは、脆弱性の危険性を表します。 リスク・マスは、その危険がどのくらいの期間、どの程度の範囲に及んだかを表します。



我々は、「リスクマス（Risk Mass）」という用語を採用します。 これは、疫学や信頼性工学において長年確立されてきた累積曝露指標に倣ったものであり、CVE件数やMTTR（平均修復時間）がいずれも無視している「時間」という次元を、脆弱性管理に取り入れるものです。 その計算式は単純明快で、脆弱な資産の数に、それぞれの資産が曝露状態にある日数を乗じるだけです。

その結果は「エクスポージャー・デー（暴露日数）」として表され、攻撃者が環境を悪用できた総期間を捉える単一の値となります。 数学的には、リスク・マスは「修復曲線下の面積」に相当します。これは生存分析でよく知られた概念であり、ここでは脆弱性の暴露測定という特定の問題に適用されています。 運用面では、組織が対策を講じなかった日々の累積コストに他なりません。

400の資産に影響を与える脆弱性が1日で修正された場合、400日分の暴露日数となります。 同じ脆弱性が100日間放置された場合、40,000日分の暴露日数となります。CVEのカウントではこれらを同じ事象として扱いますが、リスクマスではこれらが根本的に異なるリスク状況であることが明らかになります。



Qualys脅威調査ユニット

Follina (CVE-2022-30190): 33,000 日分のエクスポージャー分析

リスクマスが実際にどのように機能するかを示すため、過去4年間で最も重大な脆弱性の1つにこの手法を適用しました。

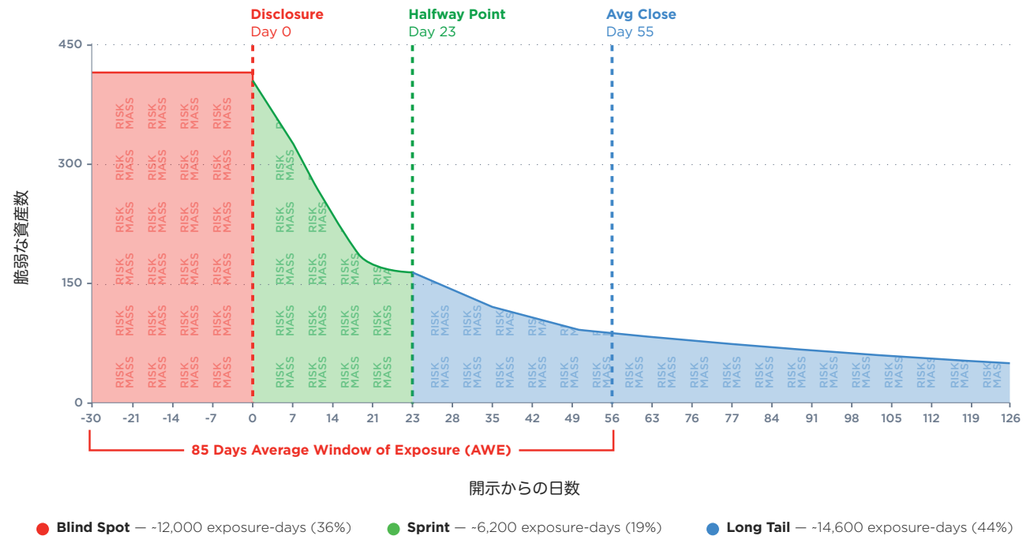
Follinaは、Microsoftサポート診断ツールに存在するリモートコード実行の脆弱性で、マクロを必要とせず、特別に細工されたWord文書を介して悪用できます。 Follinaの脅威アクターの活動時期は、そのリスクの拡大段階と一致しています。 ブラインドスポット段階では、中国関連のアクターが標的型攻撃を用いてこの脆弱性を悪用し、TA413は情報公開の数週間前にチベットの組織に対してこの脆弱性を仕掛けました。

スプリント段階では、ロシア軍情報機関（APT28、Sandworm）が500以上のウクライナの標的に対してこの脆弱性を悪用し、UAC-0098はウクライナのインフラにCobalt Strikeを配信しました。 ロングテール段階では、Qakbot関連組織、AsyncRAT、Rozenaといった汎用攻撃者がこの脆弱性を採用し、ランサムウェアグループ（Cl0p、LockBit 3.0、Bl00dy、Buhti）がアクティブな攻撃キャンペーンに組み込みました。 各段階で、異なるレベルの攻撃者がこの脆弱性を悪用しました。 末端に残された資産は、最も広範囲かつ予測不可能な脅威に直面していました。

Follina (CVE-2022-30190)・平均的な組織

リスクマス: 単一のCVEから生じる約33,000日間のエクスポージャーリスク

脆弱な資産数：約400件 x エクスポージャー期間



攻撃者の関心の幅広さは、決して偶然のものではありません。 それは、悪用されやすく、検知が難しく、そして以下のデータが示すように、修正に時間がかかるという脆弱性を反映しています。

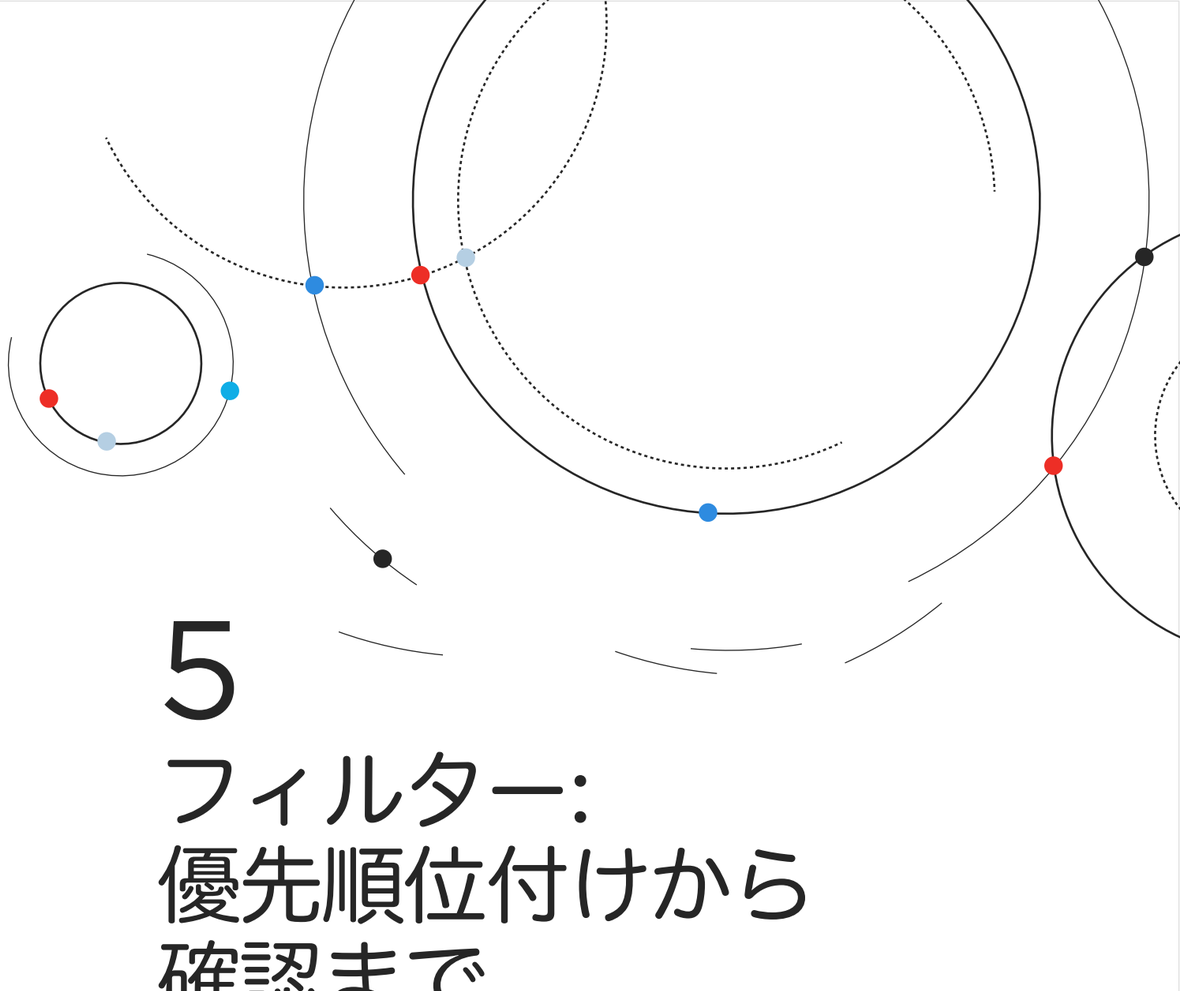
Follinaは、当社のデータセットにおいて6,000を超える組織に影響を及ぼしました。 1組織あたり平均約400の脆弱性のある資産が存在し、それぞれが外部にさらされたエンドポイントを表しています。 「リスクマス（Risk Mass）」という概念がどのように運用上の測定指標へと変換されるかを説明するため、Follinaのエクスポージャーのライフサイクルを3つの異なる段階に分け、追跡します。 各段階は、修復プロセスにおける異なる失敗モードを表しています。

ブラインドスポット (公開30日前〜公開当日): 約12,000日間のエクスポージャー期間。 Follinaは公開の30日前に攻撃ツールとして悪用され始めていました。 この期間中、400件の資産すべてが脆弱な状態にあり、パッチは存在せず、修正チケットを作成することもできませんでした。防御側はその存在すら認識していませんでしたが、国家レベルの攻撃者はすでにこの脆弱性を悪用していました。 この段階はリスクマスの総量の36%を占めており、もはや些細な割合ではなく、最大の単一の失敗要因となっています。 チケットが作成されるまでの1ヶ月間、純粋で回避不可能なエクスポージャーリスクにさらされていたのです。

スプリント（0日目から23日目）：約6,200日間のエクスポージャー期間。 開示時に修復が開始されました。 初期対応は積極的な対応が行われたものの、7日目までに資産の約79%がパッチ未適用のままでした。 14日目には57%に減少しました。 23日目の折り返し地点でも、組織の攻撃対象領域の42%が依然として露出していました。 このフェーズは総リスクマスの19%を占め、修復作業が最も多く、曲線が最も急激に低下する期間を表しています。 ダッシュボード上では、このフェーズは進捗しているように見えます。

ロングテール（23日目から364日目以降）：約14,600日間の脆弱性エクスポージャー期間。 組織の中央値がパッチ適用を完了した後も、約170の資産が未修正のままでした。平均的なパッチ適用完了日である55日目には、約90の資産が脆弱性を抱えたまま残っていました。91日目には65、1年後には15のアセットが、公開前から国家主体の攻撃者が悪用していたCVEに対して依然として脆弱な状態でした。

リスクマスは、2つの異なる失敗モードを明らかにします。ブラインドスポット（開示前の30日間の暴露）は、リスクマス全体の約36%を占めます。 ロングテール（中央値の組織がパッチ適用を完了した後の数ヶ月間の残存暴露）は約44%を占めます。 これらを合わせると、累積暴露の80%になります。 スプリント（経営ダッシュボードやコンプライアンスレポートに表示されるフェーズ）は、20%未満を占めます。 ダッシュボードはスプリントを測定しますが、リスクマスはスプリントで見逃されたすべてを測定します。



5 フィルター: 優先順位付けから確認まで

前述のセクションでは、攻撃者が脆弱性を悪用する速度と、組織が脆弱性にさらされる期間について説明しました。 本セクションでは、修復プロセスの次の段階について取り上げます。 組織が重要な脆弱性の優先順位付けに成功した後、どのようにして最終的な確定的確認レイヤーを追加し、機械速度で安全に自律的な修復をトリガーできるかについて考察します。

優先順位付けの成果

業界が成し遂げてきたことを認識することが重要です。 過去10年間で、脆弱性管理はCVSSの深刻度のみに基づく無差別なパッチ適用から、脅威アクターの活動、資産の状況、ビジネス上の重要度を考慮した、高度なリスク情報に基づく優先順位付けへと進化しました。 TruRiskのような高度なリスクスコアリングシステムは、過去最高の導入率を達成しています。

今日の組織は、この分野の歴史上いかなる時期よりも、何が重要であるかを明確に把握しています。

これは紛れもない成果であり、必要不可欠な基盤であり続けます。 本セクションの内容は、優先順位付けそのものに異を唱えるものではありません。 データが示唆しているのは、たとえ適切に実施されたとしても、優先順位付けだけでは、何が危険かを把握することと、特定の環境において実際に何が悪用可能であるかを確認することの間に、重大なギャップが生じるということです。

このギャップを埋めることが、この分野の次の進化であり、これまでの手法に取って代わるものではありません。

1%未満という現実

そのギャップがなぜ重要なのかを理解するには、脆弱性開示に関する単純な数字を考えてみよう。

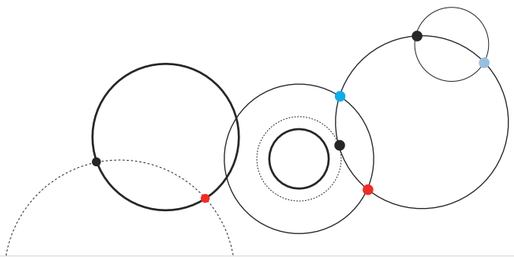
2025年には、業界で48,172件の新たな脆弱性が公表されました。 そのうち、当社の脅威インテリジェンスによると、リモートから悪用可能で、実際に悪用され、動作する概念実証コードによって裏付けられている脆弱性はわずか357件（0.74%）でした。 この1%未満という割合は、公表された脆弱性の総数がほぼ倍増したにもかかわらず、驚くほど一貫しています。

これは、残りの99%が無関係だという意味ではありません。 コンプライアンス、多層防御、将来的な悪用リスクはすべて継続的な注意を払う必要がありますが、これは対応のスピードが存亡に関わるレベルを定義するものです。

ここで脅威インテリジェンスとリスクベースの優先順位付けが不可欠な役割を果たします。 つまり、数万件に及ぶCVE（共通脆弱性識別子）を、実際に悪用されるリスクを表すごく一部に絞り込むのです。 この層をまだ導入していない組織にとって、48,172件の脆弱性を修復するか、357件に絞るかの違いは、業務麻痺と防御可能なプログラムの実現との違いに等しいのです。

この傾向はさらに広範な規模でも当てはまります。 2026年2月現在、CISAの既知の悪用された脆弱性（KEV）カタログは、業界全体で優先順位付けの基準として広く採用され、コンプライアンスのベンチマークとしてますます義務付けられていますが、これまでに公開された315,354件のCVEのうち、1,517件が登録されています。 これは全体の0.48%に相当し、これまでに公開された脆弱性の約200件に1件が、実際に悪用されていることが確認され、CISAによってカタログ化されています。
TruRiskスコアリング、CISA KEVアライメント、あるいは類似のフレームワークのいずれを用いても、結論は一貫しています。 緊急の対応が必要な運用環境は、公開された脆弱性総数のほんの一部に過ぎません。 もはや課題は、その一部を特定することではなく、その中のどのエントリが実際に自社の環境で悪用可能であるかを確認し、対応期限が切れる前にその確認に基づいて行動することです。

しかし、この削減後、つまり組織が最も危険な1%未満の対象に焦点を絞り込むことに成功したとしても、2つ目のフィルタリングの問題が残ります。



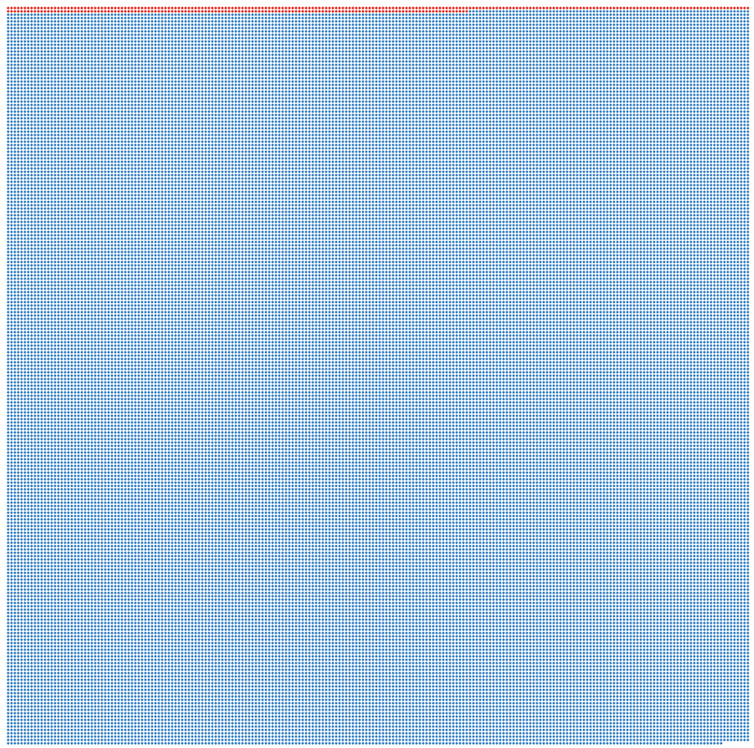
「1%未満」という現実: 2025年、業界では**48,172件**の新たな脆弱性を公表しました。そのうち、当社の脅威インテリジェンスによると、**357件**（わずか**0.74%**）のみが、リモートから悪用可能であり、実環境で積極的に攻撃に利用されており、動作する概念実証（PoC）コードによって裏付けられていました。この**「1%未満」**という現実は、公表された脆弱性の総数がほぼ倍増したにもかかわらず、驚くほど一貫しています。

1%未満という現実

針を見つける: 2025年の48,172件のうち、悪用可能な脆弱性は357件

各点は2025年に開示された1件のCVEを表しています ● **赤ドット =** 遠隔操作が可能、実際に悪用されており、概念実証（PoC）が確認されている

48,172個のドットのうち357個 = 0.74%



前年比

2022
25,043 開示
131 武器化 0.52%

2023
28,816 開示
185 武器化 0.64%

2024
39,964 開示
218 武器化 0.55%

2025
48,172 開示
357 武器化 0.74%

過去全て
315,354
total CVEs

CISA KEV カタログ
1,517
現在悪用されている
(0.48%)

要点
優先順位付によって絞り込む。
検証によって本物を見極める。

確認のギャップ

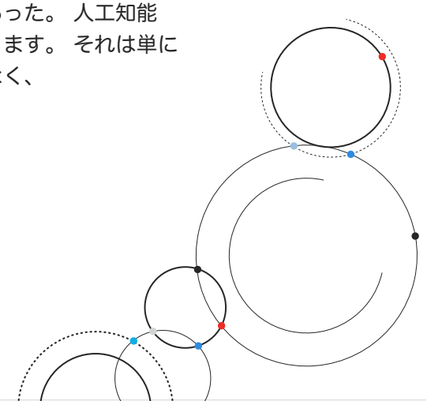
リスクベースの優先順位付け（TruRisk、CISA KEVアライメント、または類似のフレームワークによるもの）は、組織にとって理論的に最も脅威となる脆弱性を正しく特定します。 これはまさにその設計目的であり、前述の1%未満のフィルタリングがその有効性を証明しています。 しかし、優先順位付けでは答えられない別の疑問があります。 それは、特定の組織が導入している補完的な制御策を考慮した場合、この優先度の高い脆弱性は実際に現時点で悪用可能なのか、という点です。

その質問への答えは、環境レベルでのみ導き出せます。 クリティカルと正しく評価された脆弱性は、実際には、Webアプリケーションファイアウォールによるエクスプロイト経路のブロック、非アクティブ構成でのサービス実行、ネットワークセグメンテーションによる資産の攻撃者アクセス可能なインフラストラクチャからの隔離、または実行時にペイロードをインターセプトするエンドポイント検出ルールによって軽減される可能性があります。 これらの対策は脆弱性の深刻度を下げるものではなく、状況に応じた悪用可能性を低減するものです。

脆弱性は確かに存在し、優先順位付けも適切です。 しかし、この特定の環境におけるリスクは、スコアだけでは表せないほど低いのです。

我々は、この残存するギャップを「環境調整済み悪用可能性」と呼んでいます。 これは、理論的に危険なものと、既存の制御策の下で悪用可能であることが確認されたものとの差です。 自動修復をトリガーする前の最終ステップは、実際の悪用可能性を状況に応じて確認することです。 これにより、機械並みの速度での対応が、理論上のリスクではなく、検証済みのリスクに対して向けられるようになります。

サイバーセキュリティは歴史的に技術革新の派生として進化してきました。 メインフレームからモバイル、クラウドに至るまで、新しいプラットフォームが登場するたびに、それに対応するセキュリティ上の必須事項が生じ、それは後から考えると予測可能であった。 人工知能は、そのパターンを打ち破ります。 それは単に防御すべき新たな表面ではなく、



脅威の状況そのものの根本的な再構築であり、攻撃者はツールに支援された人間のオペレーターから、機械の速度で脆弱性を特定、武器化、悪用できる自律型エージェントへと移行しておりその影響は深刻です。 エクスプロイトのタイムラインは数週間から数時間に短縮され、パッチが適用される前に悪用可能なエクスプロイトが流通する状態、すなわち実務者が現在「-1日」と呼ぶ状況が到来しています。 にもかかわらず、多くの企業のセキュリティ運用は依然として、手動による「ヒューマン・イン・ザ・ループ」型のワークフローに固執しています。つまり、悪用可能なリスクと統計的なノイズを区別できないスキャナーから報告される数千件ものの理論上の脆弱性をトリアージし、チームは根拠のないパッチ適用を巡る議論に陥り、修復サイクルは人間の速度でしか動かない一方で、攻撃者はますますその速度を超越しています。

この非対称性こそが、現代における中心的な課題を決定づけています。 防御側がAI主導の攻撃のスピードと自律性に追いつくまで、その差は拡大し続けるでしょう。 こうした状況において、エージェント型AIオーケストレーションは、漸進的な改善ではなく、運用上の必須事項として浮上します。 Qualys Enterprise TruRisk Managementのエージェント型AIオーケストレーションレイヤーであるAgent Valは、この変化を体現しています。 TruConfirmを通じて本番環境における実際の脆弱性を自律的に検証し、どの攻撃経路が開いており、どの経路が既存の制御によって無効化されているかを確認し、対象を絞った緩和策をトリガーし、結果を再検証することで、リスク低減のクローズドループな証明を提供します。 もはや、より高速なスキャンやより広範囲なカバレッジが求められるのではなく、防御サイクルから人間の処理速度によるボトルネックを完全に排除し、情報漏洩から悪用までの猶予期間が完全に失われる前に、仮説に基づく優先順位付けを、証拠に基づき機械によって検証されたリスク管理に置き換えることが求められています。

確率からより高い確信へ

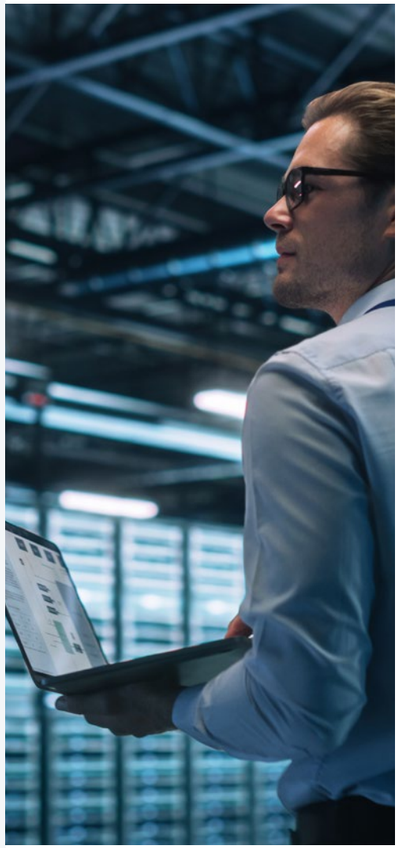
確認ギャップを埋めるには、バージョンベースの検出からエクスプロイトベースの検証へと移行する必要があります。 つまり、*「このソフトウェアは脆弱か？」*という問いを、*「この脆弱性は、今この環境で実際に悪用できるか？」*という問いに置き換える必要があるのです。

Qualys TruConfirmは、まさにこのような機能を提供します。 TruConfirmは、ソフトウェアのバージョンをアドバイザリデータベースと照合するのではなく、攻撃者が実際に使用する実行パスをテストする、安全性を最優先としたエクスプロイトベースの検証エンジンとして機能します。 本製品は、最先端のマルチモーダル検証技術を採用し、各脆弱性の性質とエクスプロイト特性に基づいて動的に調整することで、運用を中断することなく、ターゲットの運用環境において完全なエクスプロイトチェーンが成功するかどうかを判断します。 エクスプロイト可能と確認された脆弱性は、決定的な証拠とともにエスカレーションされます。つまり、エクスプロイトチェーンが実行された場合、その発見結果は確定的なものとなります。

運用上の影響は明白です。 上記で説明したマルチモーダル検出（既存の脆弱性を特定するための従来型のバージョンベースの評価に続き、実際に悪用可能な脆弱性を検証するTruConfirm）と組み合わせることで、組織は確認済みの修復対象リストを、パッシブスキャンのみの場合に比べて大幅に削減できます。ゴーストリスクの修復から解放されたリソースは、検証済みで実証済みの脆弱性に完全に振り向けることができます。 優先順位の引き下げは、現状の保護が確認されたことを示すものであり、永久的な排除ではないことに注意することが重要です。
補償的な制御は、即時の悪用可能性を低減しますが、根本的な脆弱性を排除するものではなく、制御環境の変化によって、以前に軽減されたリスクが再び顕在化する可能性もあります。

この階層型アプローチの運用上の価値は、本レポートで詳述されている修復の物理的側面から見ると明らかになります。 TruRiskは、48,000件の脆弱性を、実際に悪用可能なリスクを表す1%未満の脆弱性に絞り込みます。 この階層がなければ、運用可能な修復は開始点すらありません。 TruConfirmは、最終的に選定された重要な脆弱性群が安全にアクションを発動するために必要な決定論的な証明を提供します。 優先順位付けによって、何に注意を払うべきかが分かり、確認によって、何にアクションを起こすべきかが分かります。これら2つが一体となって、運用可能な修復に必要な完全なパイプラインを形成します。

Qualys脅威調査ユニット



6
運用化か、それとも失敗か

本報告書に示された証拠: 6.5倍のボリューム増加、TTE（悪用時間）が-1日、累積リスクの大部分を吸収する修復期間の長期化は、一つの結論を示唆している。 問題はスピードではありません。問題なのは運用モデルそのものです。

リスクオペレーションセンター（ROC）

これらの調査結果に対する対応は、漸進的なものではなく、アーキテクチャ全体の変革です。 脆弱性を発見し、スコアリングし、チケットを発行し、修復キューを通して手動でルーティングするスキャン・レポートモデルは、脆弱性の検出量が少なく、エクスプロイト処理期間が長く、人的遅延が許容されていた時代向けに設計されていました。しかし、その時代は終わりました。 それに代わるものが、私たちがリスクオペレーションセンター（ROC）と呼ぶものです。これは、修復ライフサイクル全体をマシンスピードで実行する、再現性のあるエンドツーエンドの運用パイプラインです。

ROCとは、ダッシュボードでも、チーム名でも、ガバナンスレイヤーでもありません。 それは、継続的かつ自動化されたチェーンとして機能する必要のある3つの主要な機能に基づいて構築された運用アーキテクチャです。 Qualys Enterprise TruRisk Managementは、これら3つの機能すべてを単一のプラットフォーム内で運用可能にします。

第一に、組み込み型インテリジェンスです。 第1節で述べたインテリジェンスの必要性は、ここで具体的な運用上の表現となります。

ROC（リスク管理センター）では、脅威インテリジェンスは消費される成果物として提供されるのではなく、修復パイプラインに直接投入される機械可読な意思決定ロジックとして提供されます。 脆弱性が開示されると、システムはアナリストによる評価を待つことなく、組織の資産インベントリとCVE（共通脆弱性識別子）を照合し、影響を受ける資産が内部向けか外部向けかを評価し、脅威アクターの活動と組織の業界との関連性を相互参照し、実際の悪用事例をチェックし、既存の補完的制御を評価し、類似の脆弱性クラスに対する過去の修復事例を検討します。 そして、数日ではなく数秒で、対応が必要かどうか、またその優先順位を決定します。

2つ目は、アクティブ確認です。 これは、ゴーストリスク問題を排除するノイズフィルターの役割を果たします。 ROC（リスク評価コンポーネント）は、マルチモーダル検証を適用します。まず、バージョンベースの検出や構成評価といった従来の手法を用いて「何が存在するかを特定」し、続いて「Safety-First」のエクスプロイトベース検証エンジンであるTruConfirmによるアクティブ確認を行い、組織が導入している制御策を考慮した上で「実際に悪用可能な箇所」を検証します。 その結果、ターゲットリストは大幅に絞り込まれます。 理論的に重大な脆弱性を何千件も修復するのではなく、チームと自動化システムは、確認・検証済みの脆弱性のみに焦点を当てることができます。

3つ目は自律的な行動です。 確認されたリスクに対しては、修復対応は脅威に見合った時間スケールに短縮する必要がありますが、自動化の度合いは組織の運用成熟度とリスク許容度を反映するべきです。

自動パッチ適用インフラストラクチャが確立されているエンドポイントでは、組織は過去の成功データに基づいたポリシー主導型の展開へと移行できます。 これは、過去のパッチ適用サイクル、ロールバック率、環境固有の結果から得られるパターンを活用し、時間の経過とともに自動化された意思決定に対する信頼性を高めるものです。 パッチ適用サイクルが変更ウィンドウやダウンタイム要件によって制約されるインフラストラクチャ資産については、システムは、最終的な修復が承認プロセスを経て完了するまでの間、リスクを軽減する代替制御（仮想パッチ、ネットワークレベルの封じ込めルール、ホストの分離など）を推奨し、承認されている場合は展開できます。

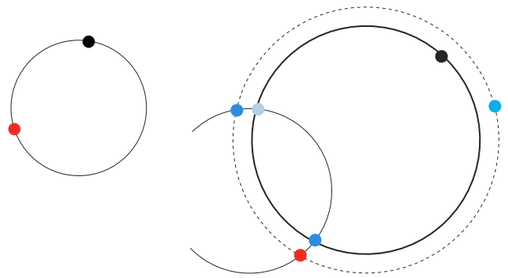
また、パッチ適用が目標期間内に行えない場合、これらの補完的な制御策は暫定的な措置ではなく、主要な防御線となり、最終的な修復策が適用されるまで継続的な緩和策を提供します。 目標は、人間の監視を完全に排除することではありません。 人間がすべてのアクションを実行するのではなく、アクションの実行時期と方法を決定するポリシーを管理することに焦点を当てることです。 これは、手動によるトリアージでは対応できない方法で、処理量に応じて拡張可能なモデルです。

「リスクのモグラたたき」の終焉

新たな重大なCVE（共通脆弱性識別子）が発生するたびに、それを個別の緊急事態として扱い、チームを招集し、チケットをエスカレートさせ、修復に向けて全力疾走するという本能的な行動は理解できます。しかし、それは持続不可能です。 脆弱性の数が6.5倍に増加し、エクスプロイトのタイムラインがマイナスに転じ、手動による修復作業が累積リスクの3分の2を占める状況では、事後対応型のモデルは拡張性に欠けます。 あらゆるスプリントがトリアージとなり、トリアージを行うたびに、より多くの問題が残されます。そして、その問題はさらに深刻化していくのです。

今後の進むべき道は、個々の脆弱性への対応を迅速化することではありません。 重要なのは、インテリジェンスの取り込みから確認、そして自動化されたアクションに至るまで、あらゆる段階で人間の介入を必要とせず、大規模かつ一貫して実行される、反復可能な運用プロセスを構築することです。 私たちのデータセットに含まれる組織の中で、既に物理的ギャップを克服している組織は、セキュリティチームの規模が大きいから成功しているわけではありません。 彼らが勝っているのは、エンドツーエンドの修復ライフサイクルを運用化し、重要なプロセスから人間の遅延を排除しているからこそ成功しているのです。

攻撃のスピードは今後も加速し続けるでしょう。 攻撃までの時間はプラスに転じることはなく、脆弱性の数は横ばいになることもありません。 防御側が制御できる唯一の変数は、修復対応のスピードと一貫性です。 そして、このレポートのデータは、10億件の記録と4年間の証拠に基づき、現在の脅威環境が要求する時間スケールにその対応を短縮する唯一の方法は、それを完全に運用化することであることを示しています。



Qualys

Qualys Threat Research Unit

www.qualys.com/tru

Qualysについて

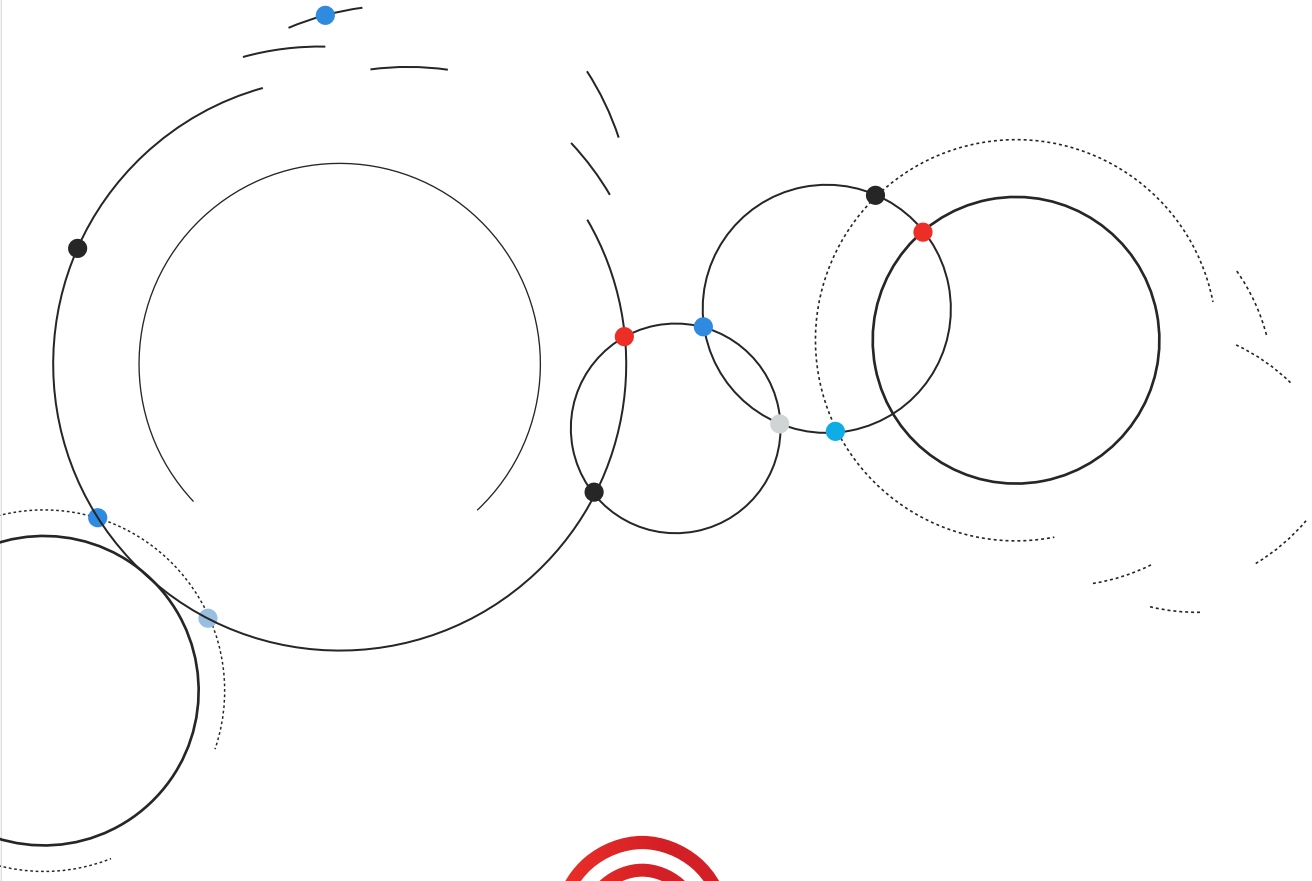
Qualys, Inc. (NASDAQ: QLYS) は、Forbes Global 100 および Fortune 100 の大部分を含む、世界中に10,000 社以上のサブスクリプション顧客を持つ、革新的なクラウドベースのセキュリティ、コンプライアンス、および IT ソリューションのパイオニアおよび大手プロバイダーです。 Qualys は、組織のセキュリティとコンプライアンスの合理化と自動化を支援し、ソリューションを単一のプラットフォームに統合することで、機敏性の向上、ビジネス成果の向上、大幅なコスト削減を実現します。詳細については、qualys.comをご覧ください。

Qualys 脅威研究ユニット（TRU）について

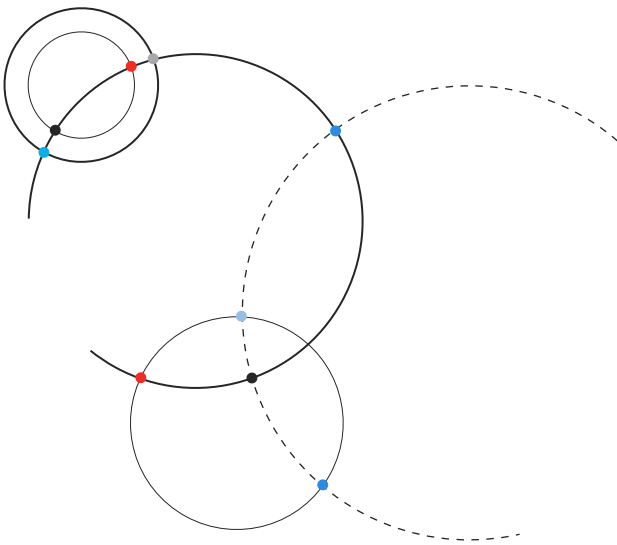
Threat Research Unit（TRU）は、Qualysの研究部門です。 TRUチームは、脆弱性、コンプライアンス、マルウェア、脅威アクターの研究に注力し、Qualys Enterprise TruRisk™プラットフォーム向けに世界最高水準のセキュリティインテリジェンス、検出データ、ガイダンスを提供することを目指しています。

新しいテクノロジーは、世界中の人々の生活と経済に革命をもたらしています。

サイバー脅威も同様のペースで増加しており、あらゆる場所で人々の生活を向上させるサービスへのアクセスを脅かしています。 TRUの研究と知見を活用することで、IT、セキュリティ、コンプライアンスに関わるお客様や関係者の皆様を支援し、混乱を引き起こし信頼を損なう悪意のあるアクターからデジタル世界を守り、保護することができます。 私たちはQualys脅威リサーチユニットです。私たちの盾は、お客様の盾です。



Qualys Threat Research Unit



Qualys.