ivanti

敵対者から同盟者へ

セキュリティチームをIT部門と連携させる5つの方法

共通の使命、異なるアプローチ

セキュリティチームとIT チームの目標は、どちらも組織を円滑に運営することですが、セキュリティチームは悪影響を避けるために、IT チームは全体的なアウトプットを改善するために、それぞれ異なる方向からこの任務に取り組んでいます。

組織の義務: セキュリティか IT か

セキュリティがオペレーションの中断を防ぐ

つまり、セキュリティスペシャリストは、継続的な戦術的実施と戦略的かつ予防的な脅威分析と是正措置のさまざまな実施を通じて、内部または外部の脅威によるサイバー攻撃で予期せぬ混乱が発生するリスクを継続的に最小化します。

ITは業務上のアウトプットを円滑化する

つまり、ITスペシャリストは、シームレスなバックグラウンドテクノロジーの導入やメンテナンスを通じてエンドユーザーの生産性を向上させ、他のスペシャリストの成果や成果物を脅かすハードウェアやソフトウェアの問題を解決します。

しかし、両部門が協力すれば、より効果的に目的を達成することができます。

IT部門がセキュリティチームを支援し、セキュリティ部門がITパートナーからリクエストを受ける前に、予防的な戦略とプロセスが用意されていれば、プロセスは効果的に機能します。

しかし、セキュリティポリシーの成功を支援したいと考えるIT部門の積極的な友人を獲得し、社内の優先事項のためにセキュリティ目標を犠牲にしようとする消極的な敵をうっかり作らないような方法で、セキュリティチームの目標やプロジェクト案を提示するにはどうすればよいのでしょうか。

ivanti

セキュリティとITの連携による利点トップ3

より速く、より優れた結果

ITチームは、パッチを要求するセキュリティチームを信頼していれば、時間とリソースを要するアップデートやパッチを実施する可能性が高くなります。

リソースを共有することで、IT支出全体を削減

チームが互いに信頼し合えば、同じツールを使って異なる目標を達成することができます。共有リソースは、コストセンターの組織的な間接費を削減します。

現実的で持続可能なセキュリティ対策

セキュリティは、セキュリティプロトコルを実装するITに依存しています。もし、その要求があまりにも困難であったり、IT 部門に多大な時間を割いたりするものであれば、IT 部門はそのような規制やプロトコルを維持することができないかもしれません。

このeBookでは、以下の内容を説明します。

01 **IT管理者とエンドユーザー双方のステークホルダーに対して、セキュリティ計画、変更、要求** の背後にある「理由」を実装前に説明します。

02 **セキュリティポリシーがIT部門の予算、スケジュール、リソース配分に与える影響を軽減します。**

03 セキュリティを柔軟にする余裕のある場合には妥協します。
(セキュリティを " No " の部署にしない!)

04 **可能な限り共通の言語、ダッシュボード、測定基準を用いて、**
共通の目標を策定し、実施します。

05 **事務的な支援であれ、技術的な専門知識であれ、リソースの共有であれ、その他であれ、プロアクティブにサポートします。**

結局のところ、満ち潮はすべての船を持ち上げ、セキュリティチームもIT部門も、生産的で安全な職場という同じ最終目標を共有しているのです。

ivanti

01

理由を説明する：

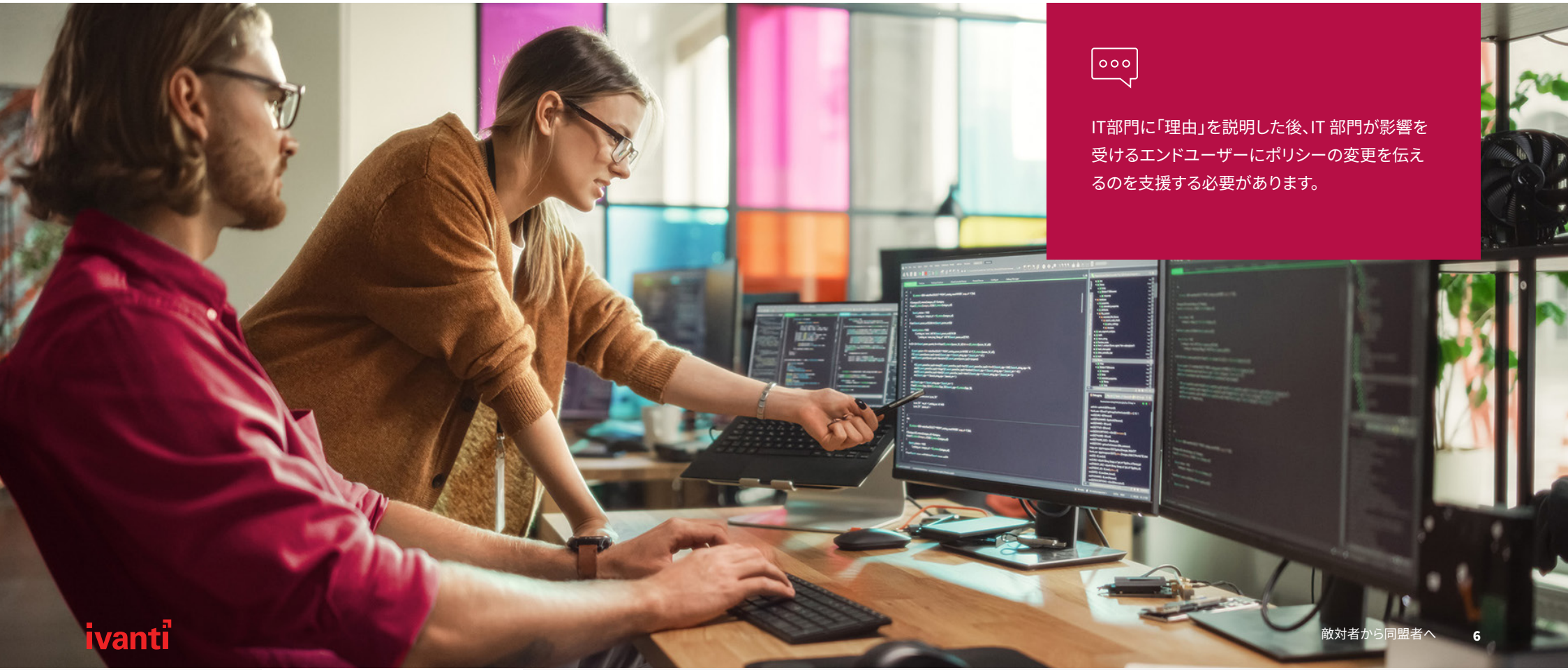
命令口調を避け、セキュリティ計画、変更、要求の背後にある説明を提供します。

ivanti

「理由」を忘れない

セキュリティからの説明のない指示は、すぐに IT 部門の反感を買ってしまいます。時間や帯域幅の制約のために、なぜその変更が要求されるのかを説明したり、IT パートナーがどのようにその変更を実施できるかを検討したりする間もなく、セキュリティ要求が出されることがあります。

たとえば、セキュリティチームがリムーバブルメモリデバイスを使用不可にすると決めた場合、ポリシーの実施には、その根拠を IT部門に伝えることから始める必要があるでしょう。IT チームに対して、特定の種類のデバイスを使用不可にすることで、サイバー保険の支払いが少なくなり、内部および外部の脅威によるデータの損失を防ぎ、組織のリスクエクスポージャを減らせると説明することもできるでしょう。



IT部門に「理由」を説明した後、IT 部門が影響を受けるエンドユーザーにポリシーの変更を伝えるのを支援する必要があります。

この共同コミュニケーションには、以下を盛り込む必要があります。

業界の専門用語を使わず、何が影響するのかを明確に説明。たとえば、デバイス使用禁止ポリシーの社内文書では、「リムーバブルメモリデバイス」ではなく、「ジャンプドライブ」、「USBドライブ」、「ファイルを持つことができ、ケーブルでコンピューターに接続できるもの」といった用語を使用します。

- この場合、ケーブルで接続されたコンピューターのマウス、キーボード、スピーカー、その他の周辺機器である。たとえば、デバイス使用禁止ポリシーの社内文書では、「リムーバブルメモリデバイス」ではなく、「ジャンプドライブ」、「USB ドライブ」、「ファイルを持つことができ、ケーブルでコンピューターに接続できるもの」といった用語を使用します。

変更の1日か2日以上前に明確なタイムラインを提示し、ユーザーに代替手段を見つける時間を与え、重要な営業プレゼンテーションの前に誤ってノートパソコンからUSBドライブをロックアウトしないようにします。

義務化の例外を定義し、その例外を申請するための、できれば手間のかからないプロセスを定義することで、ユーザーが「独自の状況」のために回避策を実行するのを阻止します。

予想される頻度の高い質問、一般的なトラブルシューティング、予期せぬエッジケースに対応するため、主要な担当者または拠点を特定します。

このコミュニケーションがなければ、ITチームはセキュリティプロトコルが導入されたときに苦情やチケットであふれかえり、その不満や怒りをセキュリティにぶつけてしまうかもしれません。

02

影響を軽減する:

導入前に、セキュリティポリシーがIT予算、スケジュール、リソースに与える影響を検討します。

ivanti

ITへの影響の予測と緩和

ITチームが他にどのような要求に直面しているかを把握します。あなたが要求した時点で、彼らはもっと大きなプロジェクトに対処しているかもしれないし、タスクを完了するために必要な人材がいないかもしれません。

その代わりに、このセキュリティチームが哀れな IT 部門に対して行ったこととは異なり、ITの同盟者がセキュリティポリシー、リクエスト、パッチを簡単に実行できるようなツールやシステムを探しましょう。

現実世界への影響

大学のセキュリティがIT部門に24時間の臨時パスワードのために面談調査を強制

ある大学のセキュリティチームは、キャンパス内の全学生を対象に、端末を置き忘れたり紛失したりしがちな端末を含む全学生を対象に、端末に紐づいた二段階認証を導入することを決定したことがあります。

学生が大学のネットワークやリソースにアクセスするために、一時的に新しいパスワードを要求する必要がある場合、セキュリティチームは以下を要求しました。

1. 対面またはZoom電話会議による本人確認。
2. ミーティングでは、申請者は公的な身分証明書を見せながら、複数のセキュリティに関する質問に答えました。
3. そして、チームは一時的な資格証明書を発行することができましたが、それは24 時間しか有効ではありませんでした。
4. もし学生がその時間内に古いデバイスを見つけられなかった場合、あるいは単に新しいデバイスを入手できなかった場合、すべてのプロセスをやり直さなければならなかったのです。

もしセキュリティチームが、負担の大きいポリシーを導入する前にIT部門に相談していれば、より合理的な解決策は、次の方法でネットワークを分割することだったと気づいたはずです。

- より簡単な認証で、限定的な学生ネットワークを導入する。
- より機密性の高い従業員ネットワークのために、完全な面談と回復プロセスを維持する。

(結局のところ、完全に成長した大人の従業員は、若い大学生よりも自分のデバイスを追跡する意欲と精神的能力が高いのが普通です。)

このような分割されたネットワークシステムは、ITのニーズに敏感でありながら、大学のパーティーで頻繁に紛失するにもかかわらず、学生の個人所有のデバイスを保護することができるでしょう。

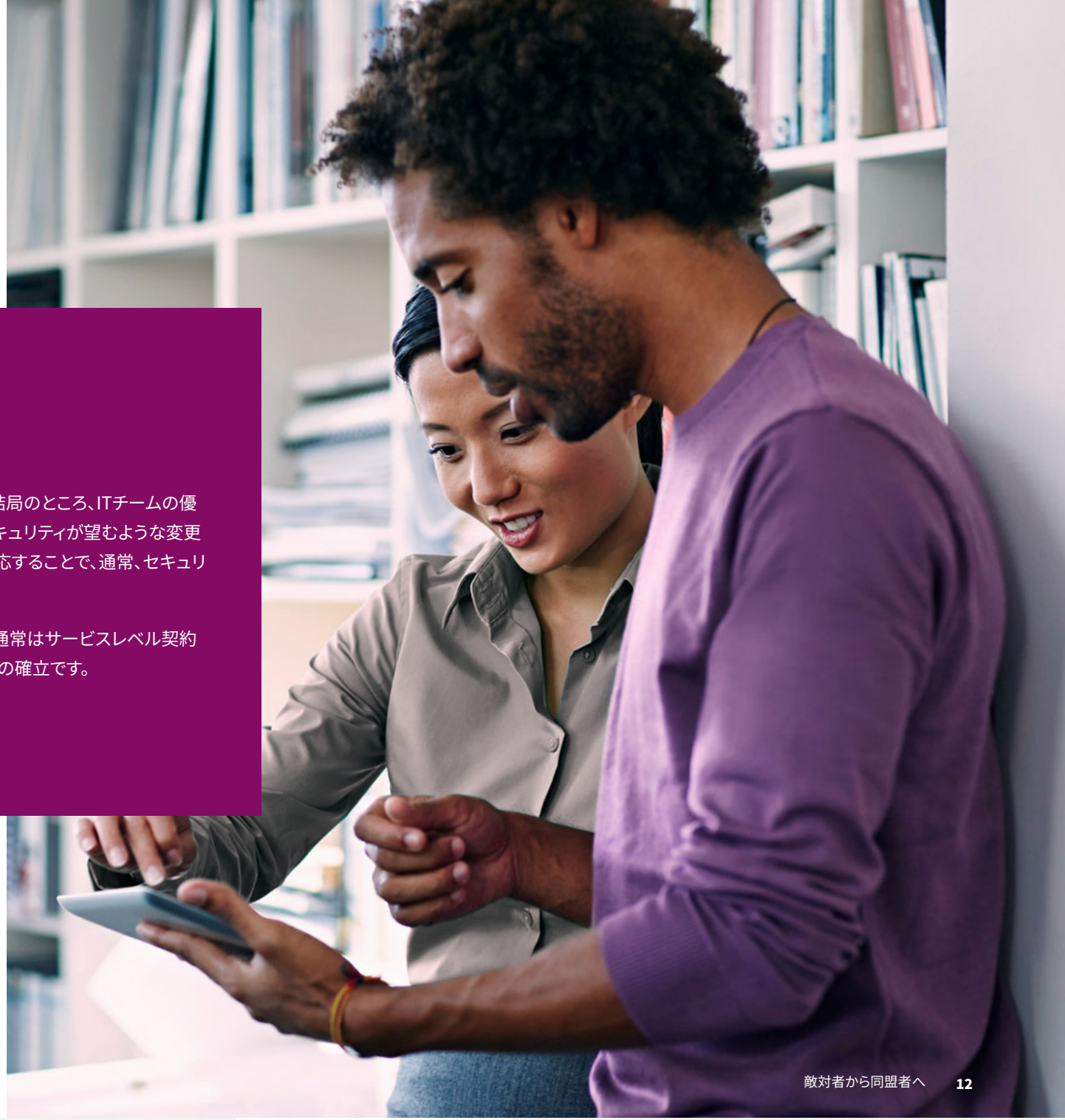
03

妥協する：

できる範囲で柔軟に対応し、「No 部門」にならないようにしましょう。

ivanti

妥協のテクニック



他部門と仕事をするときは、妥協することも想定しておきましょう。結局のところ、ITチームの優先事項は業務を円滑に進めることです。パッチをリリースしたり、セキュリティが望むような変更をすぐに行えるような時間的余裕はないかもしれません。柔軟に対応することで、通常、セキュリティとITは共存の道を見つけることができます。

このような柔軟性を積極的に求めることができる方法のひとつが、通常はサービスレベル契約（SLA）を通じて文書化される、相互に合意したサービス期限と契約の確立です。

このSLAでは、各ステップにおけるコラボレーションの期待値とタイムフレームを定義し、いつ、誰が、何をするのかを全員が把握できるようにします。

すべての定義。 あなたの組織が「悪用された脆弱性」と考えるような基本的なことであっても、予想以上の基本的なことが必要になるでしょう。

共同部門プロセスの各段階に必要な仕様と技術スタックの展開。.

- これらのプロセスには、パッチのロールアウトから新しいポリシーの導入まで、あらゆるものが含まれます。

優先順位付けの基準。 セキュリティにとっての緊急事態と、IT 部門にとっての緊急事態を明確にします。

- カスタム内部尺度、ルーブリック、その他の内部評価方法は、プロセスのこの部分を標準化するのに役立ちます。SLA 作成プロセスの一環として、IT チームと一緒に作成します。

相互プロジェクト中のコミュニケーション頻度。 たとえば、次のようなプロセスに関する質問を考えてみましょう。

- Patch Tuesdayの具体的なパッチ展開について、IT 部門がセキュリティ部門から連絡を受けるのはいつになるのでしょうか。
- セキュリティ担当者は、IT部門から問題やパッチのロールアウト成功の確認について、いつ連絡があると予想できますか。
- どの時点で、(どちらの側からの) オープンリクエストも、返答がないことを理由にクローズできるのでしょうか。どのような場合に上層部をチェーンに加えるべきでしょうか。

「標準的な」タイムラインと成果物の期待値 を、プロジェクトの種類ごとに、各チームから提示します。また、標準的な手順に対する例外も明示的にリストアップし、説明します。

各部門から指名された窓口または特定の役職

- その責任には、SLA の方針や手続きに関する混乱を解決することや、部門をまたがる担当者と SLA を毎年見直し、更新することも含まれます。

04

IT部門と共通の目標を策定し、実施します。

ivanti

共有目標の設定

前にも述べたように、セキュリティとITはアプローチが異なるものの、組織、ユーザー、そしてすべてのプロセスを可能な限り円滑に動かすという点では、同じような使命を担っています。

したがって、時間をかけて IT リーダーと共有目標を設定し、KPI（主要業績評価指標）、ダッシュボード、その他の共有測定値を作成し、日々の戦術的な共有目標を強化する価値があります。

たとえば、パッチのロールアウトを考えてみましょう。(このeBookではよくある例ですが、それには理由があります。)

ITチームもセキュリティチームも、組織のテクノロジーが円滑に動くことを望んでいます。つまり、理由は違えど、どちらの部門もワークフローを中断させるパッチは望んでいません。

IT部門は、アプリのユーティリティや接続性を壊すような不適切なパッチの実装によって発生するすべてのヘルプデスクチケットに対処することは避けたいと考えています。

セキュリティはエンドユーザーを困らせたくないし、（より安全な）パッチが適用された企業アプリが、それまで確立されていたワークフローを積極的に妨害するようなことがあれば、業務を行うためにリスクの高い回避策やシャドーITの実装を求めるような方向に向けたくはありません。

共有された目標を施行するということは、問題回避するということ

ITチームの解決策として、パッチをまったく適用しないこともあります。特に、パッチが基幹業務フローを破壊しないことをセキュリティが保証できない場合です。また、セキュリティチームは、IT 部門からの反発に直面して、パッチの適用を見送ることを選択するかもしれません。

しかし、IT部門もセキュリティ部門も、情報漏えいに対処することは避けたいと考えています。情報漏えいは、デバイスやアプリケーションがアクティブなエクスプロイトに対して定期的にアップデートされていない場合によく起こります。

サイバー攻撃を撃退するのは明らかにセキュリティの責任と負担ですが、セキュリティ侵害の際には ITチームも被害を受けます。

結局のところ、セキュリティチームがバックアップの安全とネットワークからの侵入者の排除を保証している間でも、技術システムをできるだけ早く復旧させなければならないのは IT 部門なのです。

パッチが適用されていないシステムが原因で攻撃が発生した場合、IT部門は何を優先リストから除外するのでしょうか。

そして、両チームが望んでいるのは、組織のプロセスが中断されるのを何としても避けることである、という基本的な理解を共有した上で、セキュリティと ITの両チームにとって有効な強固なパッチ適用戦略を考えることは、両チームにとって最善の利益となります。

05

支援を提供する:

自社の管理リソース、技術的専門知識、
その他のツールを積極的に共有します。

ivanti

互恵関係がより良い協力関係を生む

IT部門に何かを求めるのであれば（たとえば、現在のIT技術スタック、ポリシー、プロセスを借用して自社のセキュリティユースケースに適応させるなど）、見返りを与える必要があります。

多くの場合、共有ツールや企業に対する財政的責任を分担することも含まれますが（各チームが共有ツールに拠出する予算は、各チームが個別にリソースを確保するのにかかる費用よりも少額になります）、この支援にはさまざまな形があります。

最終的には、ツールやリソースを共有することで、セキュリティチームとITチームは全体的なコストを削減し、コラボレーションを向上させることができます。

共有されたツール、ダッシュボード、レポートは、両チームがお互いを理解するためのコンテキストを作り出します。互いの世界を覗く窓は、共感と信頼を築きます。

IT部門の価値観と優先順位を知ることは、セキュリティチームが、IT パートナーにとって実用的であり、かつ IT パートナーに配慮した方法で、さまざまなプロジェクトの賛同を得るのに役立ちます。

もちろん、無理のない範囲内で、セキュリティが手を差し伸べてくれるなら、その賛同はさらに早く得られるでしょう。

ivanti

セキュリティが予算を超えてITを支援する3つのクリエイティブな方法

管理負荷	ITチームのメンバーも含め、多くの人が仕事のペーパーワークの部分を困難だと感じています。それで相手部署があなたのことを良く思ってくれるなら、できる限りその負担を引き受けることを申し出ましょう。 たとえば、IT チームが新しいセキュリティポリシーがチケットキューに影響を与えると予測した場合、新しいポリシーに関連するすべてのチケットやユーザーからの問い合わせに回答するセキュリティスペシャリストを任命します。 また、受理された元の提案書から、技術者以外の読者向けに新しい方針を「翻訳」し、それを社内のコミュニケーションチームに渡して、社内のステークホルダーと共有することもできます。
技術的専門知識	新しいプロセスやポリシーを提案しても、自分では簡単に思えても、IT担当者は混乱してしまうかもしれません。 IT担当者に対して、戦術的な実装に関するトレーニングセッションの開催を提案します。あるいは、時間があれば、IT部門に代わって設定を行うこともできます。(メンテナンスにあたるIT担当者が、関連するトラブルシューティング資料を簡単に見つけられるようにします。) その見返りとして、IT管理者にセキュリティのトレーニングを依頼し、たとえ彼らがIT部門からセキュリティ部門に異動してきたとしても、組織内でどのようにITが運用されているかを、IT 部門が基本的に理解できるようにします。
共有リソース	セキュリティがITの技術的能力の活用をどのように要請するかについては、別のガイドで説明します。(詳細は「セキュリティのシフトレフト」を参照してください。) ただし、特に、自社のチーム向けに用意している専門的な開発資料やトレーニング資料へのアクセスなど、セキュリティに特化した特定のツールをIT部門で利用できない理由はありません。 そうすることで、IT部門がセキュリティの任務と立場を理解するようになり、今後の要請を迅速に処理できるようになります。

現実世界への影響

部門横断的な「群がる」帯域外セキュリティリスク

セキュリティチームもITチームも、毎月リリースされる「Patch Tuesday」を中心に、テスト、試験運用、ロールアウトのスケジュールを立て、実装に関する問題に計画的に対処することがよくあります。

しかし、いくつかのパッチは「帯域外」に落ち、2 つの理由で皆を慌てさせます。

1. **帯域外のパッチや修正リリースは通常、アクティブなエクスプロイトであり、**すぐに実行する必要があります。
2. **チームは他の重要なタスク** の優先順位を下げ、新たに解放されたリスク、つまり緊急事態が解決される間も問題を引き起こし続けるタスクの優先順位を上げなければなりません。

このような緊急事態に「総動員」で対応するのではなく、成熟した組織は「群れる」方法を開発しました。

- セキュリティやITなど複数の部門にまたがる専門家からなる**帯域外専門対応チーム**を任命します。
- 帯域外のパッチがリリースされると、**これらのチームは**緊急のパッチや修正に「群がり」、完全に修正に集中します。
- その一方で、親部門は**定期的に予定された**タスクやプロジェクトを継続します。

帯域外のパッチが落ちる前にこのような部門横断チームを結成することで、組織は避けられない緊急事態に迅速に対処しながら、軌道を維持することができます。

「それは文化の転換であり、群れるメンタリティです。

「(帯域外リスクに対処する際) 私たちは、誰が悪いかを探そうとはしていません。このような場合、ほとんどの場合、脆弱性は組織の誰の責任でもありません。

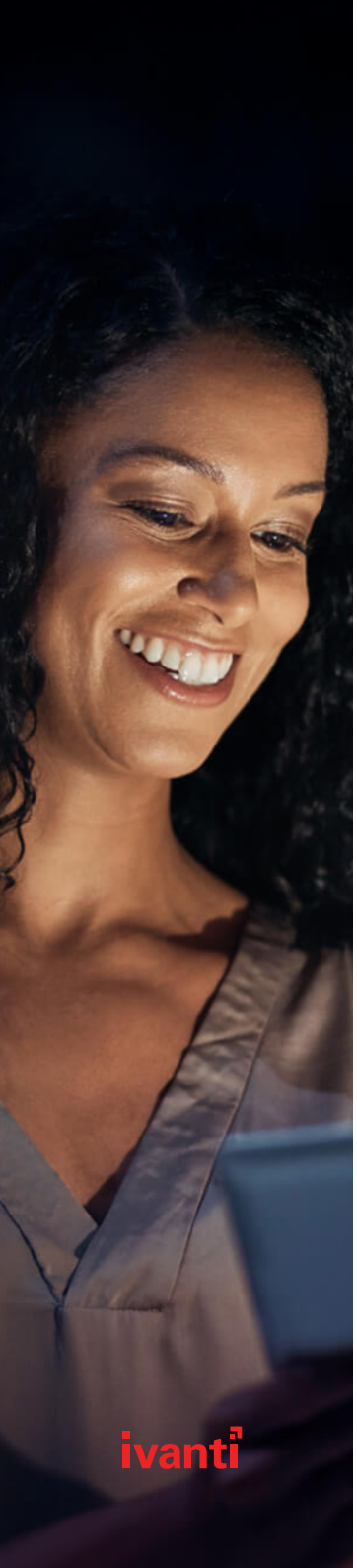
「その代わり、群れるような状況では、誰が解決に向かうのがベストなのかを見極めるだけでいいと理解されています。

「その人物を特定したことで、組織内の他の全員が、もし大群が発生している間にその人物をサポートすることになった場合、その (修復が) 新たな優先事項であることを知ることになります。

「他の優先事項は、それが解決するまで優先順位が下がります。

「私が見てきた中で、より群がるメンタリティを採用している組織は、より健全なレベルの対応で、最終的に脆弱性が解決されるまでのレスポンスも通常より迅速です。」

- Chris Goettl
Ivantiエンドポイントセキュリティ製品管理担当副社長



参考文献

- Australian Cyber Security Centre. (30 June 2017). “Essential 8 Maturity Model”: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- Bowermaster, P. (February 2023). “Shift Left to Risk-Based Proactive Security Management.” CIO’s The Future of Work Summit.
- Center for Internet Security. (2021). “Critical Security Controls Version 8”: https://www.cisecurity.org/controls/v8
- Forrester. (2022). “The Total Economic Impact of Ivanti Unified Endpoint Management (UEM) Solutions”: https://rs.ivanti.com/reports/forrester-tei-of-ivanti-uem-solutions-2022.pdf
- Forrester. (2022). “The Total Economic Impact of the Ivanti Enterprise Service Management. A Forrester Total Economic Impact Study Commissioned by Ivanti”: https://rs.ivanti.com/reports/forrester-tei-ivanti-enterprise-service-management-platform-2021.pdf
- GDPR.EU. (n.d.) “GDPR Checklist for Data Controllers”: https://gdpr.eu/checklist
- Goettl, C. (25 March 2021). “Automated Patch Management and Team Swarming are Key Security Practices.” Ivanti: https://www.ivanti.com/blog/automated-patch-management-and-team-swarming-are-key-security-practices
- Goettl, C., & Masserini, J. (1 September 2022). “Vulnerability Management in Real Life: 5 Best Practices from Real-World RBVM Programs.” Ivanti: https://www.ivanti.com/webinars/2022/vulnerability-management-irl-5-best-practices-from-real-world-rbvm-programs
- Goettle, C. & Stryker, A. (11 May 2023). “Vulnerability Patch Prioritization Problems: Cybersecurity Research Results Part 2.” Security Insights: https://ivantiinsights.buzzsprout.com/1554237/12876518-vulnerability-patch-prioritization-problems-cybersecurity-research-results-part-two
- Harvard Business Review. (29 August 2022). “How Much Time and Energy Do We Waste Toggling Between Applications?”: https://hbr.org/2022/08/how-much-time-and-energy-do-we-waste-toggling-between-applications
- Ivanti. (18 August 2018). “7 Experts on What Shift Left Means for IT Departments”: https://www.ivanti.com/blog/7-experts-on-what-shift-left-means-for-it-departments
- Ivanti. (2022). “The NIST Cybersecurity Framework (CSF): Mapping Ivanti’s Solutions to CSF Controls”: https://www.ivanti.com/resources/v/doc/ivi/2694/63935da433e2
- Ivanti. (2022). “The Ultimate Guide to Risk-Based Patch Management”: https://www.ivanti.com/resources/v/doc/ivi/2705/11190ce11e80
- Ivanti. (2023). “Press Reset: A 2023 Cybersecurity Status Report”: https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465
- Ivanti. (2023). “ITSM+ Toolkit”: https://www.ivanti.com/resources/v/doc/ivi/2760/e094c24df239

参考文献

- Ivanti. (2023). “The Ultimate Guide to Unified Endpoint Management (UEM)”: https://www.ivanti.com/resources/v/doc/ivi/2508/b7d55619d0ee
- Ivanti. (28 June 2022). “2022 Digital Employee Experience Report”: https://rs.ivanti.com/ivi/2700/4e528f833de3.pdf
- Ivanti. (n.d.) “IT Jargon Explained: CMDB:” https://www.ivanti.com/glossary/cmdb
- Ivanti. (n.d.) “IESO Shifts Left for Streamlined IT Operations”: https://www.ivanti.com/customers/ieso
- Ivanti. (n.d.) “Southstar Bank “Shifts Left” with Ivanti Neurons”: https://www.ivanti.com/customers/southstar-bank
- Miller, T., & Spicer, D., Stryker, A. (19 January 2023). “IT vs Security: When Hackers Patch for Profit.” Security Insights: https://ivantiinsights.buzzsprout.com/1554237/12071546-it-vs-security-when-hackers-patch-for-profit
- Morning Consult and IBM. (3 October 2022). “IBM Security Incident Responder Study”: https://www.ibm.com/downloads/cas/XKOY5OLO
- National Institute of Standards and Technology. (2018). “Framework for Improving Critical Infrastructure Cybersecurity” (p14): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Official Journal of the European Union. (14 December 2022). “Directive (EU) 2022/2555 of the European Parliament and of the Council”: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- Oltsik, J. (2022). “ESG Research Report: Technology Perspectives from Cybersecurity Professionals.” Enterprise Strategy Group - Information Systems Security Association International: https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Security-Process-and-Technology-Trends-Jul-2022.pdf
- Perri, L. (2023, April 19). “Top Strategic Cybersecurity Trends for 2023.” Gartner: https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023
- Pickering, D. (2022, May 5). “What is DevSecOps? How Great Developers Shift Left for Security.” Ivanti: https://www.ivanti.com/blog/what-is-devsecops-how-great-developers-shift-left-for-security
- Rundle, J. and Nash, K. (2023, May 22). “Security Chiefs Trim the Fat.” The Wall Street Journal: https://www.wsj.com/articles/security-chiefs-trim-the-fat-as-budgets-bite-83c82f99
- SAM. (July 2022). “IoT Security Landscape Report”: https://securingsam.com/wp-content/uploads/2022/04/SAM_IOT-Security-Report.pdf Program.” Ivanti: https://www.ivanti.com/webinars/2022/win-budget-and-influence-non-infosec-stakeholders-for-your-2023-cybersecurity-program
- Shackleford, Dave. (March 2022). “SANS 2022 Cloud Security Survey”: https://8645105.fs1.hubspotusercontent-na1.net/hubfs/8645105/white-paper/sans-2022-cloud-security
- Verma, A., Goettl, C., & Hindman, M. (2022). “How to Win Budget and Influence Non-InfoSec Stakeholders for Your 2023 Cybersecurity Program.” Ivanti: https://www.ivanti.com/webinars/2022/win-budget-and-influence-non-infosec-stakeholders-for-your-2023-cybersecurity-program

敵対者から同盟者へ

セキュリティチームをIT部門と連携させる5つの方法

ivanti

より詳しくは、ivanti.com/jaをご覧ください。