Google Cloud

Cybersecurity Forecast 2024

将来への指針となるインサイト

はじめに

この先 1 年について考えるとき、人によっては「predictions」（直観的な予測）という単語を使います。しかし、Google Cloud では、常に現在観察されているトレンドに基づいて来年のサイバー セキュリティ情勢を予想しているため、「forecast」（根拠に基づいた予測）といった方が意図を正確に表わせるように思います。

Google Cloud Cybersecurity Forecast 2024 レポートには、Google Cloud のセキュリティ リーダー数名と、Mandiant Intelligence、Mandiant Consulting、Chronicle Security Operations、Google Cloud の CISO オフィス、VirusTotal など、多数のセキュリティ チームの専門家数十人による今後の見通しを掲載しています。これらの方々は常に最新かつ大規模な攻撃の最前線に立っており、2024 年に組織やセキュリティ チームが考慮すべきことを認識しています。

テクノロジーの進歩とともに脅威は進化し、攻撃者は戦術、技術、手順（TTP）を変化させてきました。防御側はこれに後れをとらないように対応していく必要があります。Google Cloud Cybersecurity Forecast 2024 レポートは、サイバー セキュリティ業界が 2024 年のサイバー攻撃者との戦いについて構想を練るうえで役立つ情報を提供することを目的としています。

Google Cloud

AI

改良、専門化されて規模が拡大したフィッシング

フィッシング、SMS、その他のソーシャル エンジニアリングのコンテンツや素材（音声や動画を含む）を本物らしく見せるために、生成 AI や大規模言語モデル（LLM）が利用されるようになるでしょう。これによってスペルミス、文法上の誤り、文化的背景の欠如が減るため、フィッシングメールや不正なメッセージを見分けるのが難しくなります。LLM は翻訳して翻訳文を整えることもできるため、ユーザーが言葉遣いを基にフィッシングを見分けるのはさらに困難になります。LLM を活用すれば、攻撃者は正当なコンテンツを取り込んで、元のコンテンツと同じような見た目、流れ、文章で攻撃者の目的に合わせた改ざんしたバージョンを生成できるようになります。

また、生成 AI を使用することで、このようなキャンペーンを大規模に実行できるようになります。攻撃者が名前、組織、役職、部門、さらには健康に関するデータにアクセスできると、受信者に合わせてカスタマイズされた説得力のあるメールで多数の個人を標的にできるようになります。たとえば、請求書の督促状の下書きに生成 AI を使用すること自体は悪意のある行為ではないため、このようなメールを作成するには悪意のある LLM は必要さえないかもしれません。

スケーラブルな情報操作

賢い生成 AI プロンプトには、フェイク ニュースの作成、受信者と積極的にやり取りするニセの電話呼び出し、生成 AI が作成したフェイク コンテンツを基にしたディープフェイク写真や動画の作成のために攻撃者が必要とするすべてが揃っています。このような捏造された情報が主流のニュース サイクルに入り込む可能性はますます高まっています。このような情報操作が広がるにつれて、ニュースや（オンライン）情報に対する国民の信頼が低下し、誰もがより懐疑的になったり、単純に自分が見たり読んだりするものを信用しなくなってしまう危険性があります。そうなると、近い将来、企業や政府が国民と関わるのがしだいに困難になっていく可能性があります。

このような生成 AI テクノロジーは、Metasploit や Cobalt Strike などのエクスプロイト フレームワークで得られるメリットと同様に、脅威アクターが限られたリソースと能力で攻撃することが可能になるため、将来的に情報操作やその他の侵入などの操作を大幅に増加させる可能性を秘めています。攻撃者はすでに生成 AI のテストを進めており、今後これらのツールの使用が増えていくと予想されます。

攻撃に活用されるサービスとしての生成 AI と LLM

LLM やその他の生成 AI ツールは、攻撃者による標的の侵害を支援するサービスとして開発、提供されることが増えていくでしょう。開発されたサービスはアンダーグラウンド フォーラムで有料サービスとして提供され、フィッシング キャンペーンや虚偽の情報の拡散などのさまざまな目的に使用されるでしょう。サイバー犯罪に使用されているランサムウェアなど、攻撃者が他のアンダーグラウンドでサービスとして提供されているものを使用して攻撃を成功させているのがすでに確認されています。

データの解釈、脅威の理解、防御の強化

サイバー防御者は、生成 AI や関連するテクノロジーを利用することで、攻撃者の検知、対応、アトリビューションを大幅に強化でき、また分析やその他リバース エンジニアリングなどにかかる時間も短縮できます。AI の主なユースケースは、組織が大量のデータを統合し、脅威インテリジェンスにおいてそれをコンテキスト化して実用的な検出やその他の分析につなげられるようにすることです。これは 2024 年に実を結び、AI および 生成 AI によって、これらの大規模なデータセットから取るべき行動を分析および推測する人間の能力が強化されると見ています。お客様固有のデータを機密性の高い方法でオーバーレイする新しい方法が登場し、組織は迅速かつ大規模に重要なアクションを起こせるようになるでしょう。セキュリティ目的に AI を利用する組織にとって、これは今後数年間の大きな変革の 1 つとなり、最終的には労力を削減し、脅威の過度な負担に対処し、拡大する人材不足を解消するのに役立つでしょう。

ビッグ 4

中国

中国発信のサイバー攻撃は、台湾、中国の地域的な覇権と影響力、主要市場に対する経済的影響力に関連する問題など、国内の安定と領土保全といった長期的な優先事項によって引き続き推進されるでしょう。中国のサイバースパイ活動家は今後もステルス性を維持し、検知の機会を抑制し、アトリビューションを妨害するでしょう。ゼロデイ悪用、ネットワークエッジ上のシステムの標的化、サプライ チェーンの侵害、感染ネットワーク内および脅威アクターと被害組織間の両方のトラフィックを偽装するように設計されたボットネットやプロキシネットワークなどの戦術が引き続き使用されることが予想されます。

また、中国は国家の政治的および軍事的目的を支援するために、破壊活動やキャンペーンを開始できる軍事力と民間力を引き続き育成していくと予想されます。紛争が活発化する中で、中国の脅威アクターによって破壊活動が実行される可能性があることに世界中の組織が脅威を感じており、日々の業務や生活、重要インフラ、安全性に影響を及ぼす可能性があります。

ロシア

2024 年以降も引き続き、ウクライナがロシアのサイバー脅威活動の主な焦点となり、情報収集、破壊的攻撃、情報操作が頻繁に行われると予想されます。また、政府、国防、市民社会、非営利団体、エネルギーを標的とするなど、長年にわたり優先事項としているウクライナ国外でのロシアのサイバースパイ活動（戦略的情報収集任務など）を引き続き観察していきます。

ロシアに対する制裁は、同国の技術革新や軍事革新に悪影響を及ぼし続けるでしょう。ロシアは国内の専門知識の不足を補うために、知的財産窃取を増やすという手段にでる可能性があります。この振る舞いは、過去数年間に発生した中国の知的財産窃取をモデルにしたものになるでしょう。

北朝鮮

北朝鮮を拠点とするサイバー脅威活動では、金銭目的の活動がますます重視されており、特に暗号通貨業界やその他のブロックチェーン関連プラットフォームが標的となっています。2024 年には、北朝鮮はサイバー攻撃やインフラ取得のためだけでなく、兵器や核開発計画の資金調達のために、暗号通貨や NFT の窃盗にさらに重点を置くと予想されます。

特に、北朝鮮の中央統治機関の財政的負担を軽減するために、同国が自立的運営を行っていることが観察されています。この資金調達のアプローチは、集団的繁栄につながる「チュチェ（主体）思想」という国家イデオロギーに沿っています。近年、スパイ活動の資金調達に利用されるサイバー犯罪キャンペーンが相対的に増加していることが観察されており、このトレンドは今後も続くと予想されます。また、北朝鮮がサプライ チェーン攻撃を仕掛ける機会を利用することも予想されます。

イラン

イランの地政学的野心、経済発展のニーズ、地域のライバルであるサウジアラビアやイスラエルとの競争、政権の安定性と存続に対する脅威、イラン人ディアスポラ（離散民）や反政府勢力の監視が、来年の国家主導によるサイバー脅威活動の主要な推進要因となると予想されます。

2023 年 10 月 7 日にイスラエル中南部の民間標的および軍事基地を標的としたハマスの多方面からの奇襲攻撃を受けて、イランと関係のあるサイバースパイ活動家やパレスチナおよびレバノンの脅威アクターが、イスラエルに対する脅威を増大させていると考えられます。イランの脅威アクターは、情報収集、情報操作、そして潜在的にはハイブリッド型のハックアンドリークやその他の破壊的攻撃を実行する可能性が高いと予想されます。

世界的な脅威予測

攻撃者によるゼロデイ脆弱性 (およびエッジデバイス) の継続的な活用

2012 年以降、ゼロデイ脆弱性の利用は全体的に増加していることが観察されており、2023 年は 2021 年に更新された前回の記録を上回る勢いで推移しています。2024 年には、国家の支援を背景とする攻撃者とサイバー犯罪グループの両方によるゼロデイ脆弱性の利用がさらに増えると予想されます。その理由の 1 つとして、攻撃者が環境への永続的なアクセスをできるだけ長く維持することを望んでいることが挙げられます。ゼロデイ脆弱性（およびエッジデバイス）を悪用することで、たとえば、フィッシング メールを送信してからマルウェアをデプロイする場合よりもずっと長く環境へのアクセスを維持できます。セキュリティ チームおよびソリューションは、悪意のあるフィッシング メールやマルウェアを特定する能力が大幅に向上しているため、攻撃者は検出を回避するために他の手段に目を向けるようになるでしょう。エッジデバイスと仮想化ソフトウェアは監視が難しいため、脅威アクターにとって特に魅力的なものとなっています。サイバー犯罪者は、ゼロデイ脆弱性を悪用すれば、被害組織の数が増え、最近の大規模な恐喝事件のように、ランサムウェアや身代金要求に対して高額な料金を支払う可能性がある組織の数も増えることを認識しています。

米大統領選を標的としたサイバー活動

米国大統領選挙の年を迎えるにあたり、国家やその他の脅威アクターが、選挙制度を標的としたスパイ活動や影響力作戦、ソーシャル メディアでの候補者へのなりすまし、有権者自身を標的とした情報操作など、さまざまなサイバー活動に関わることが予想されます。また、選挙後に活動が減少するとは考えられません。国家、特に中国、ロシア、イランが（政権交代の可能性の際に）決定的な優位性を得ようとする中で、米国政府に対するスピア フィッシングやその他の攻撃が増加する可能性が高いとみています。2024 年には、攻撃の規模やペースを高めるために生成 AI ツールが利用されることを考えると、このようなキャンペーンがさらに蔓延する可能性があります。

破壊的なハクティビズムの台頭

2022 年と 2023 年は、ロシア侵攻が続く中で、特にロシアまたはウクライナへの支持を表明している脅威アクターに関連する、ハクティビストの活動が再び活発化していることが観察されました。同様に、ハマスとイスラエル間で勃発した最近の紛争に伴ってハクティビストの活動が急増しています。観察された活動として、分散型サービス拒否（DDoS）攻撃、データ漏洩、改ざんなどがあります。Mandiant Intelligence の追跡によると、注目すべきは、表向きはハクティビストに見える攻撃グループが、いずれのケースにおいても平均以上の能力を有していることです。現時点では国家機関とのつながりは確証できていませんが、ロシアとイランのグループが過去にニセのハクティビスト戦術を利用していたことにも注目しています。このような作戦が成功して犯行を疑われた場合に十分に関連を否認できることがわかると、国家が民間や軍を標的にそのようなサイバー攻撃を仕掛ける可能性が高まると Mandiant Intelligence は判断しています。そして最終的にはこのような戦術を駆使して物理的損害をもたらす可能性があると推測されます。

ワイパーがすべての国家サイバー兵器庫の標準機能に

2022 年のロシアによるウクライナ侵攻の前に、ロシアの APT グループはウクライナの標的へのアクセスを獲得し、物理的な軍事作戦と同時に破壊攻撃を開始しました。他の国家も、この手法を真似てワイパー マルウェアをサイバー兵器に加えるようになるでしょう。台湾海峡の緊張など、世界中のセキュリティ上の脅威に備えて、2024 年には戦略的に重要な標的に対して破壊的なワイパー マルウェアが仕込まれることが予想されます。

宇宙ベースのインフラが標的に

ウクライナの状況は、紛争時における宇宙関連技術 (スターリンクなどの衛星通信ネットワーク) への依存の高まりを実証しています。2024 年には、国家の支援を受けた高度なサイバー攻撃者が、宇宙および関連する地上支援インフラや通信チャネルを侵害するために多方面にわたる工作活動を行い、敵対勢力の活動を妨害し、混乱させ、無力化し、弱体化させ、破壊して欺こうとするスパイ活動の痕跡が見つかると予想されます。

ハイブリッド環境やマルチクラウド環境を標的とした攻撃は成熟し、より影響力を増している

2023 年、Mandiant は VMware と協力して、攻撃者がゲスト仮想マシン（VM）上でコードを実行できるゼロデイ脆弱性を修正しました。この脆弱性の影響を受けたのは 1 つのハイパーバイザに限られていましたが、攻撃者は永続性を確立して横方向に移動する方法を求めてクラウド環境を標的にしていたことが明らかになりました。2024 年には、このような手法がクラウド環境の垣根を越えて進化していくと見られます。脅威アクターは、異なるクラウド環境間を横方向に移動するために、構成ミスや認証の問題を悪用することに目を向けるでしょう。

脅威アクターによるクラウドのサーバーレス サービスの悪用が増加

2023 年は、サーバーレス インフラストラクチャにデプロイされたクリプトマイナーの増加が見られました。2024 年には、サイバー犯罪者や国家の支援を背景とした攻撃グループがクラウドのサーバーレス テクノロジーをより積極的に活用するようになると予測されます。開発者がサーバーレスを採用するのと同じく、拡張性と柔軟性に優れており、自動化ツールを使用してデプロイできるという理由から、攻撃者もサーバーレスに移行していくでしょう。

恐喝型攻撃は続く

恐喝型攻撃は、依然として世界中の企業や社会に最も影響を与えるサイバー犯罪形態です。2022 年には大きな変化はありませんでしたが、盗まれたデータに関する宣伝活動や恐喝の推定被害額から、2023 年はこの脅威が増大していることが見てとれます。また、2024 年もこの脅威は増加傾向が続くと予想されます。

スパイ活動と「スリーパー ボットネット」

サイバースパイ活動は、攻撃を拡大するさらなる方法を模索し続けると同時に、その活動のためにOPSEC をさらに向上させていくでしょう。スパイグループは、新旧の脆弱性利用型不正プログラムを組み合わせて、脆弱なモノのインターネット、小規模オフィス、ホームオフィス（SOHO）、サポートが終了したデバイスやルーターから「スリーパー ボットネット」を作り上げます。これらの「スリーパー ボットネット」は必要に応じて使用され、捕らえられるか役に立たなくなったら破棄されるため、脅迫活動を追跡してアトリビューションを行う作業が複雑になります。このような「スリーパー ボットネット」は、DDoS 攻撃のように、多数のデバイスを利用して攻撃を増幅する従来のボットネットとは異なります。

旧来の手法の復活

攻撃者は検出を回避するために新たな手法を組み込もうとする一方で、広く報道されていない旧来の手法を復活させるアクターも現れることが予想されます。たとえば 2013 年に、ある研究者が、文書化された Windows API で暗号化関数を使用する代わりに、文書化されていない SystemFunctionXXX 関数を使用する方法について、ブログ投稿で紹介しています。この手法は 2022 年第 4 四半期までは普及しませんでしたが、その後、何人かのセキュリティ研究者がこれについて取り上げ、個人のブログや GitHub でコード スニペットを公開し始めました。ちょうどその頃、この手法を実装したマルウェアのサンプルが VirusTotal に多く出現するようになりました。また、2012 年発行のマルウェア解析に関する書籍で詳述されている仮想マシン対策（VM 対策）手法が最近使用されたことも観察されています。ほとんどの国でハイパーバイザーはあまり使用されていないため、この手法は検出ルールで対象となっていませんでした。

マルウェア作成者は引き続き最新プログラミング言語へ移行

マルウェア作成者は引き続き、Go、Rust、Swift などのプログラミング言語を使用したソフトウェアを多く開発していくでしょう。その理由として、これらの言語の優れた開発エクスペリエンス、最小限の機能、大規模な標準ライブラリ、サードパーティ パッケージとの統合しやすさなどが挙げられます。これらの言語やエコシステムを使用することで、複雑なマルウェアを迅速に開発でき、より安価に新種のマルウェアを記述して検出を回避できます。すなわち、アクターが使用するツールセットが頻繁に変化することになり、それに対応する新しい検知シグネチャが必要になります。残念なことに、これらの最新言語では、大規模なランタイム（Go）や最新のコンパイラ技術（Rust）が使用されていることが多く、リバース エンジニアリング作業は困難さが増します。言い換えれば、プロテクターを使用せずにパッキングと難読化が可能になります。

ソフトウェア パッケージ管理システムを介して開発者がサプライチェーン攻撃の標的に

近年、IconBurst などの NPM（Node.js パッケージ管理システム）に対するサプライ チェーン攻撃で、脅威アクターがソフトウェア開発者を標的にしていることが実証されました。特に懸念されるシナリオは、悪意のあるパッケージをインストールすることで開発者が侵害されることです。これにより、脅威アクターは開発者のソース コードにアクセスしてバックドアを追加できるようになります。これは低コストで影響力の大きい攻撃となります。その結果、特に脅威アクターが、PyPI（Python）や crates.io（Rust）などの監視の少ない他のパッケージ管理システムに移行するようになると、この種の攻撃がさらに蔓延していく可能性があります。このようなソフトウェア ライブラリのソースを、油断せずに慎重に監視していく必要があります。

蔓延し続けるモバイル サイバー犯罪

2024 年も引き続き、サイバー犯罪者や詐欺グループは、国内のヘルプサービスの模倣、ソーシャルメディア、銀行、政府関係者などからのニセのメッセージ、ニセのポップアップ通知といった最新のソーシャル エンジニアリング戦術を採用して、被害者がモバイル デバイスに悪意のあるアプリケーションをインストールするよう誘導すると予想されます。

サイバー保険料は横ばい

保険市場は常に変動することが知られています。市場のハード化とは、保険料が上昇する一方で保証範囲が制限されており、ソフト化とは保険料が低下し、保証範囲が拡大することを示します。保険料の上昇と補償範囲の制限を特徴とする、ここ数年間のサイバー保険市場の強い調整局面の後、市場はソフト化し始めています。システミック リスクの補償範囲は引き続き縮小傾向が予想されますが、保険会社がこの新たな状況で勝ち抜くために他の方法で補償範囲を拡大する可能性もあります。

SecOps に関する統合

リスク インテリジェンスと脅威インテリジェンスが統合されたセキュリティ運用ソリューションを求める声が強まっており、2024 年には SecOps における統合がいっそう進むと予想されます。顧客はネットワーク資産全体（クラウド、マルチクラウド、オンプレミス、ハイブリッド環境）をカバーする統合エコシステムを求めており、セキュリティ プログラムをすぐに開始できるベンダー独自のワークフロー、ガイダンス、コンテンツにますます期待を寄せるようになるでしょう。

JAPAC に関する予測

選挙を巡るサイバー活動

2024 年には台湾、韓国、インド、インドネシアで選挙が実施されます。これまで、サイバースパイ活動、サイバー犯罪、ハクティビズム、情報操作のアクターが、このような極めて重要なイベントに関心を表明しているのを観察してきました。選挙をおとりにして、詐欺や情報収集のために利用されるであろうと予想しています。中国が新たに作成した地図は、インドおよびインドネシアの選挙でも論争を巻き起こす可能性があります。

「豚の食肉解体（pig butchering）」詐欺は引き続き問題に

サイバー犯罪と人身売買の両方の要素を併せ持つ豚の食肉解体詐欺は、JAPAC 諸国の法執行機関にとって 2024 年も引き続き問題となるでしょう。豚の食肉解体詐欺はオンライン詐欺の一種で、詐欺師は被害者の信頼を得るために、長期間にわたって恋愛関係を装います。詐欺師は被害者の信頼を獲得すると、さまざまな不正な金融スキームに投資するよう説得し始めます。2023 年 8 月の国連報告書には、これらの詐欺師の多くは自らが被害者であり、人身売買されて詐欺活動を強要されていることが詳述されています。2023 年 7 月、フィリピンで 2,700 人がサイバー犯罪の強制労働から救出されました。国連報告書は、「状況は依然として流動的であり、地域内外の何十万人もがオンライン犯罪に強制的に関与させられている」と主張しています。

戦術、技術、手順の変化

JAPAC 地域ではエンドポイント検出や対応ソリューションがさらに普及し、組織全体のセキュリティ成熟度が高まりつつあります。結果として、十分なリソースを備えた脅威アクターは、検知を回避する戦術を使うことが多くなるでしょう。すでに世界中でこの傾向が見られます。この地域の防御者は、セキュリティ、ネットワーキング、仮想化ソフトウェアにおけるゼロデイの悪用、ルーターやその他のエッジデバイスの標的化、その他の方法による被害を受けたネットワークの内外両方での攻撃者のトラフィックの中継および偽装に備えて準備する必要があります。

EMEA に関する予測

欧州議会選挙が標的になる可能性が高い

サイバースパイ活動と情報操作のどちらも行う脅威アクターにとって、6 月の欧州議会選挙は魅力的な標的となるでしょう。ヨーロッパ全土でのロシアの活動レベルを考えると、ロシアが最も大きな脅威であることは明らかです。ウクライナ侵攻以来、APT29 は大陸全土の政府機関を標的に活動を活発化しており、親ロシア派の情報操作は欧州内に分裂の種を蒔こうとしています。こうした取り組みは選挙に向けてさらに強まる可能性があります。ロシアは過去に、情報操作を利用してサイバースパイ キャンペーンで盗んだ情報を広めています。このため、欧州政府は情報操作とネットワーク侵入の間のさまざまなつながりを把握することが不可欠です。

欧州の選挙はロシアを超えた幅広い脅威に直面する可能性もあります。近年、ベラルーシに関係する脅威アクターの活動がますます活発化しており、東ヨーロッパでは情報操作への技術サポートが行われています。親中派による情報操作もまた、ヨーロッパ諸国にわたってキャンペーンの範囲と規模を拡大しています。欧州政府は、事前にレジリエントな防御を構築できるように、情報操作に採用されるさまざまな手法を理解しておく必要があります。

アフリカにおける情報操作活動

デジタル時代において、虚偽の情報は地政学的な影響を及ぼす強力なツールとなります。ロシアと中国は、アフリカ諸国を標的として、虚偽の情報を拡散して不和の種をまき散らし、民主主義を弱体化させることを意図したサイバー キャンペーンを展開する傾向が強まっており、2024 年もその傾向は変わらないと見ています。レアアースはスマートフォン、コンピュータ、電気自動車など、多くのハイテク製品に不可欠であるため、中国とロシアのグループがレアアース業界を標的にすることが予想されます。これらの資源を掌握することで、ロシアと中国はアフリカにおける経済的、戦略的立場を強化できます。

ロシアと中国が虚偽の情報を利用してアフリカに影響を与えるもう 1 つの方法は、独裁政権を支援することです。独裁政権は多くの場合、反対意見を厳しく取り締まり、情報を規制します。このため、ロシアと中国ではプロパガンダを広めて民主主義の価値観を弱体化させることが容易です。アフリカを標的とした偽情報キャンペーンは長期戦であり、この活動は 2024 年にピークに達すると予測しています。

2024 年オリンピックで攻撃対象領域がパリ（およびその先）まで拡大

2024 年パリ夏季オリンピック期間には、特に金融情報や認証情報を要求するフィッシング キャンペーンが急増し、チケット発券システムや商品を標的としたサイバー犯罪者が現れることが予想されます。公的機関や銀行は引き続き警戒する必要があります。また、地政学的な活動を通じて、オリンピックを利用してフランス、さらにはヨーロッパとそれに関連する政治体制を不安定にして圧力をかけようとする試みが確認される可能性もあります。また、オリンピックは、イベントに直接関係する情報（チケット販売など）も間接的に関係する情報（宿泊施設、公共交通機関）も、誤った情報や虚偽の情報の標的になる可能性があります。

まとめ

新しいテクノロジーはセキュリティ チームに役立つと同時に、攻撃対象領域を拡大する可能性もあります。生成 AI の世界が急速に進化する中、2024 年には攻撃者は新たな方法で説得力のあるフィッシング キャンペーンや大規模な情報操作を実施できるようになるでしょう。ただし、防御側はその同じテクノロジーを使用して、攻撃者の検出、対応、アトリビューションを強化し、手間のかかる作業を軽減してセキュリティ運用業務を効率化し、優先度の高い脅威に適切に対応できるようにすることで、拡大するスキルギャップを埋めることになるでしょう。

来年も、ビッグ 4（中国、ロシア、北朝鮮、イラン）では継続的な活動が実施され、それぞれの目標を達成するためにスパイ活動、サイバー犯罪、情報操作、その他のキャンペーンが繰り広げられると予想されます。組織のセキュリティは向上しているため、これらの攻撃の多くには、ゼロデイ脆弱性の使用やエッジ デバイスの標的化など、検出を回避するための手法が組み込まれるでしょう。

米国を含めてどの国も、2024 年を通じて開催されるさまざまな主要イベント、欧州議会やその他の選挙、そしてパリの夏季オリンピックなどを標的にしたグローバルなサイバー活動に備える必要があります。さらに、世界的な大規模紛争が来年も続くため、破壊的なハクティビズムの増加にも備える必要があります。

サイバーセキュリティ情勢は変化し続けており、ときには新しい予想外の展開が起こります。防御側のリソースには限りがあることが多く、最新の展開についていくのは並大抵のことではありません。Google Cloud Cybersecurity Forecast 2024 レポートにおいて、セキュリティ担当者がこの先 1 年間に確実に起きるであろうことと不確実なことの両方に備えるために役立つ情報をお届けできたでしょうか。最前線から得た知識が皆様のお役に立つことを願っています。

寄稿者

Cybersecurity Forecast 2024 レポートは、以下に挙げる Google Cloud のセキュリティ リーダーからのインサイトを基に作成されました。

Mandiant Consulting の CTO、Charles CarmakalMandiant Intelligence の VP、Sandra Joyce、Google Cloud セキュリティ担当 GM 兼 VP、Sunil Potti、最高情報セキュリティ責任者、Phil Venables

その他多数の Google Cloud チーム メンバーによって作成されました。

Willi Ballenthin
Dan Black
Sarah Bock
Anton Chuvakin
Jamie Collier
Vivek Chudgar
Charles deBeck
Vicente Diaz
Eric Doerr
Renato Fontana
David Grout
Scott Henderson
Mike Hom
Renze Jongman
Dan Kennedy
Cris Kittner
Karen Kukoda
Steve Ledzian
Yihao Lim
Keith Lunden
Jens Monrad
Joseph Pisano
Fred Plan
Ofir Rozmann
Mike Raggi
Alice Revelli
Nick Richard
Matt Shelton
Monica Shokrai
Daniel Sislo
Genevieve Stark
Kelli Vanderlee
Alden Wahlstrom
Dominik Weber
Richard Weiss
Jess Xia