アンラボ・セキュリティレター

Press Ahn

2024.10 Vol.127

AhnLab ISF 2024: AI と統合セキュリティで成し遂げる革新

AhnLab ISF 2024: AI と統合セキュリティで成し遂げる革新

秋が深まるころ、アンラボは最新のセキュリティトレンドを貫くカスタマイズ型セキュリティ戦略を準備し、顧客会社のセキュリティ担当者との面談を行った。9月 26日、グランドインターコンチネンタルホテルでアンラボの統合セキュリティカンファレンス「AhnLab ISF 2024」が開催された。今年、アンラボはグローバルトレンドに合わせてセキュリティソリューションおよび AI 技術の高度化、プラットフォームベースの連携強化などに集中してきた。今回のイベントも、AI と統合セキュリティに対するよりセキュリティの具体的なコア戦略を紹介する場となった。今回はその現場の様子をうかがっていく。

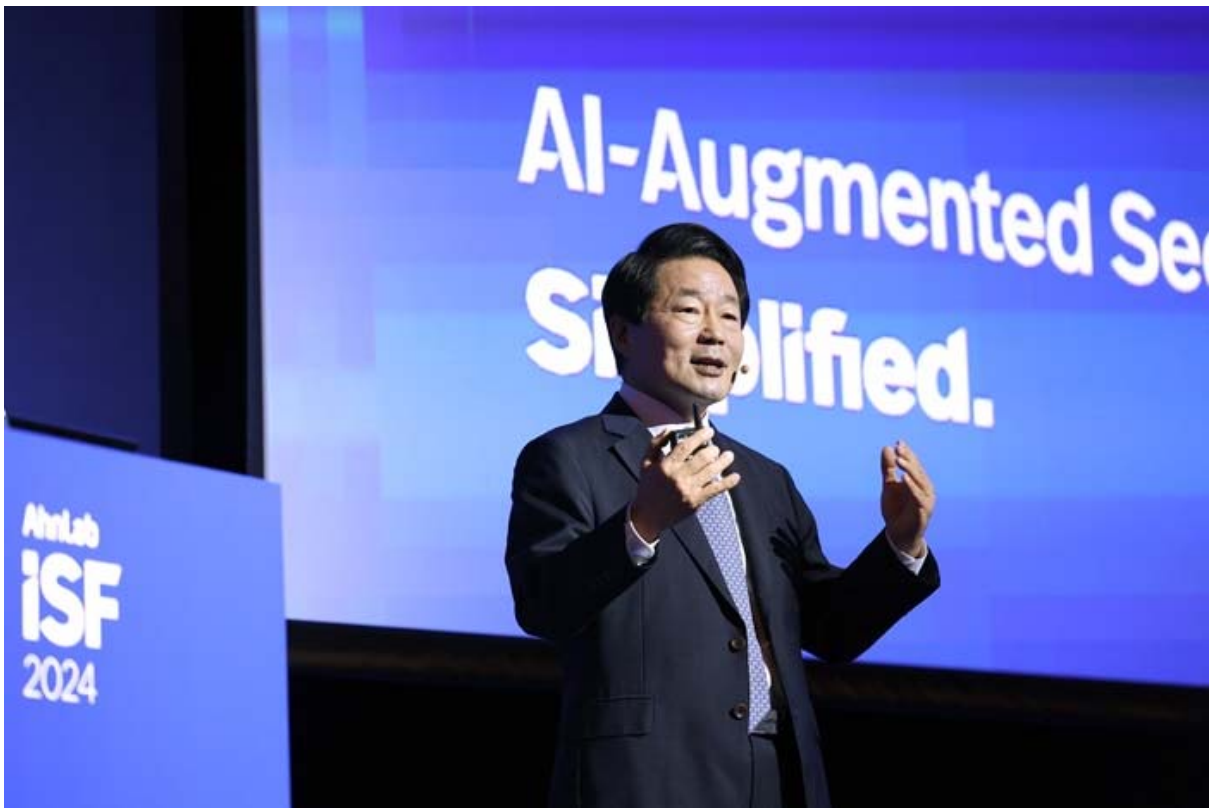
AhnLab ISF 2024 では、「AI-Augmented Security. Simplified.（AI を適用してセキュリティを単純化する）」というスローガンのもと、AI を活用してより強力かつシンプルなセキュリティを実現するための案を紹介した。アンラボのカン・ソクギュン代表による開催の挨拶を皮切りに、チョン・ソンハク研究所長、キム・チャンヒ製品サービス企画室長の基調演説、そして ▲能動的な脅威予測（**P**roactive）▲柔軟な連携（**L**ow-friction）▲統合プラットフォーム（**U**nified）をテーマに説明するトラック（Track）発表セッションが行われた。

[写真 1] AhnLab ISF 2024 入場を待つ参観者たち

カン・ソクギュン代表は、開催の挨拶でアンラボが過去数年間にわたり自社製品とプラットフォームに様々な方法で AI 技術を導入し、検知および対応能力を強化していると述べた。カン・ソクギュン代表は「最近、サイバー脅威の高度化、セキュリティの複雑性の増大に対応するための主要トレンドとして『人工知能（AI）』と『セキュリティ運用の効率性（Efficiency）』が注目されている。アンラボも統合をベースにセキュリティ効率性を強化し、ユーザーのビジネス生産性を高めることを目標とし、その延長線上で AI 技術を高度化している」と強調した。

さらに、「本日、公式の場において初めて紹介する『AhnLab PLUS』は、エンドポイントとネットワーク、クラウド、サービス、セキュリティ運用、CPS（Cyber-Physical System）など、合計 6つのプラットフォームを融合した統合セキュリティプラットフォームであり、▲能動的な脅威予測（Proactive）▲柔軟な連携（Low-friction）▲統合に基づくシナジー（Unified）▲強力なセキュリティ（Secure）など、4つの志向点に応じて製品間、プラットフォーム間の統合を持続的に発展させ、ユーザーのビジネス生産性の向上に貢献できるはず」と述べた。

また、カン・ソクギュン代表は製品と技術の統合以外に、人と組織間の協力の重要性も強調した。カン・ソクギュン代表は「1つの組織がすべてのセキュリティミッションを解決することには限界があるため、複数の組織が力を合わせて進化する脅威に対応する必要がある。AhnLab ISF 2024 がその連帯をリードする中心的役割となることを願う」と付け加えた。



[写真 2] アンラボのカン・ソクギュン代表は、統合セキュリティプラットフォームの必要性と組織間の協力の重要性を力説した。

カン・ソクギュン代表の挨拶が終わると、アンラボのチョン・ソンハク研究所長が「生成 AI の脅威と AI を活用した将来のセキュリティ」をテーマに基調演説を行った。チョン・ソンハク研究所長は AI 技術、AI を活用した攻撃が発展する中、AI を活用して将来のセキュリティを安全にリードしていく案を共有した。

チョン・ソンハク研究所長は、攻撃者による AI を使用したフィッシングメールの配布、マルウェアの作成、ディープフェイク映像の作成など、AI をベースとするセキュリティ脅威が急激に増加しており、これらの脅威による侵害を防ぐには、防御者の観点から AI 技術を搭載したセキュリティソリューションで攻撃をどのように検知するかを考え続けるべきだと助言した。

チョン・ソンハク研究所長は「アンラボは AhnLab EDR、MDS、V3 モバイルセキュリティ (V3 Mobile Security)、XDR 製品に AI 技術を導入し、URL 情報、イベントログなどを学習させて不正な振る舞いとフィッシングメール、振る舞いベースの異常な兆候を検知することで脅威インテリジェンスを提供し、先制的に対応する。AhnLab XDR の場合、AI セキュリティアシスタント (AI Security Assistant) である生成 AI『AhnLab Annie AI』を活用できる。AhnLab Annie AI は、プロンプトを入力することで退勤から出勤までのセキュリティイベントの発生と措置、レポート出力の有無など、ユーザーのセキュリティ運用をサポートする役割を担う」と説明した。

[写真 3] アンラボのチョン・ソンハク研究所長は生成 AI を活用した脅威に対応するための具体案を共有した。

2番目の基調演説者、アンラボのキム・チャンヒ製品サービス企画室長は「Empowering the Future of Cyber Security: Everything Everywhere All at Once」について発表した。このセッションは、急変するビジネス環境において組織が直面するミッションと、アンラボが提示する解決案に重点を置いた。

キム・チャンヒ室長は、「サイバー脅威が進化する中、クラウド使用の増加、リモートワークの活性化、攻撃対象領域の拡大などが一気に発生し、大多数の組織が効率的なセキュリティ運用、生産性向上に難渋している。これを克服するには『統合』が重要である。AhnLab PLUS はエンドポイントとネットワーク、クラウドなど、様々なセキュリティプラットフォームが集中管理能力をもとに運用され、AhnLab XDR が最上位に位置して複数のセキュリティ領域のデータを収集、分析することにより、最適なリスク管理ソリューションを提示する」と述べた。

また、キム・チャンヒ室長は「これに加え、アンラボはエンドポイントとクラウド、サービス領域それぞれにデバイス制御、コンテナセキュリティ、マネージド検知・対応 (MDR) など、新たな製品とサービスを追加し AhnLab PLUS プラットフォームを発展させ続けている。さらに、ゼロトラストネットワークアクセス (ZTNA)、攻撃対象領域管理 (ASM) サービスなど、未来志向的なオファリングを通じてセキュリティの複雑性を解消し、ユーザーの業務環境を安全に保護していく」と発表した。

[写真 4] アンラボの製品サービス企画室キム・チャンヒ室長は、
ビジネス環境におけるセキュリティ脅威に対応するための解決策を提示した。

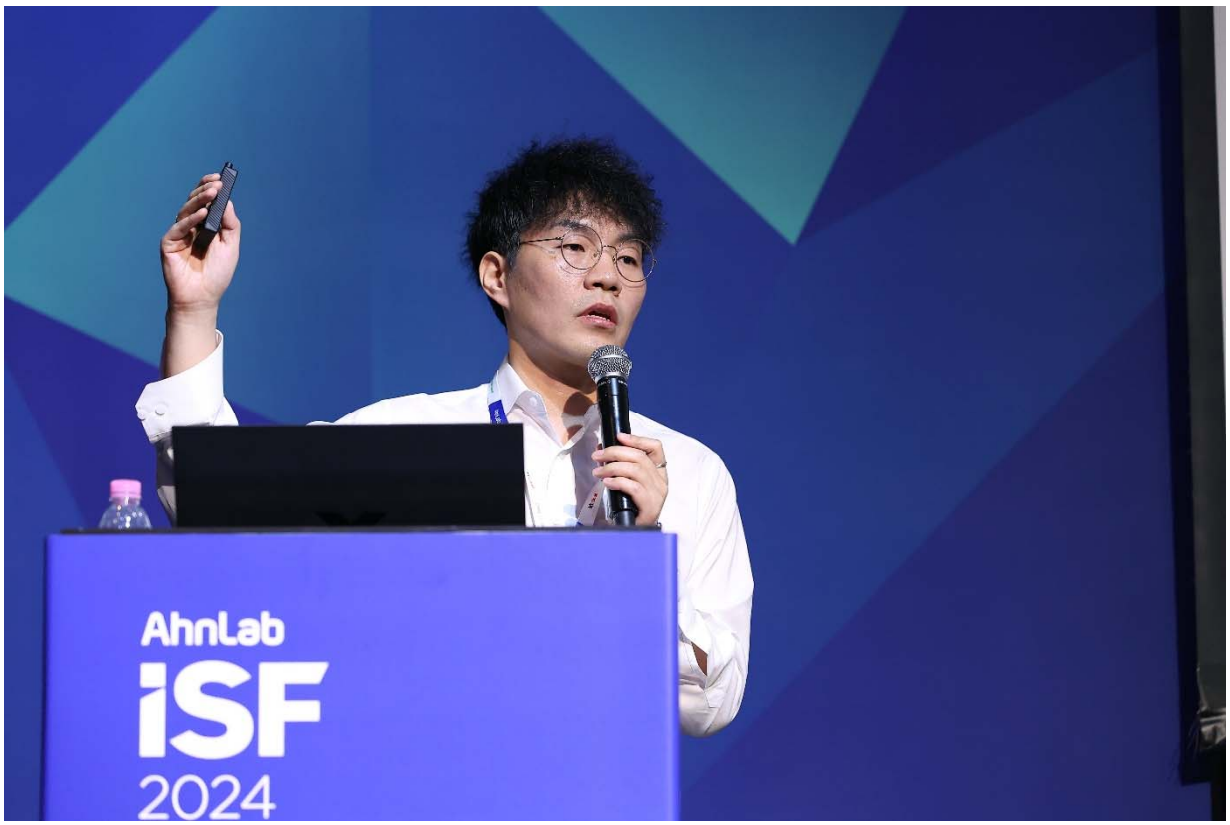
Protect Today for Resilient Tomorrow: 今日の安全が明日の回復力を生む

アンラボ A-FIRST チームのイ・ミョンスチーム長は、「Ransomware ran somewhere」をテーマに 2024年第 3四半期までのランサムウェア動向とセキュリティインシデントの事例、対応案について発表した。

イ・ミョンスチーム長は「最近脆弱性を利用したランサムウェア攻撃が急増しているが、代表的な事例には ESXi、スクリーンコネクト(ScreenConnect)、クリックセンス (Qlik Sense)、Windows、PHP などのソフトウェア脆弱性攻撃がある。特に ESXi は VMware が作成した仮想マシンで、ランサムウェアに感染するとシステム全体が動作しなくなり、被害者は交渉に応じざるを得ない。このような理由で多くの攻撃者が ESXi を主な標的として捉えている」と警告した。

イ・ミョンスチーム長は、ランサムウェアに対応するためには事前準備、リアルタイム防御、侵害の検知、インシデント対応などのプロセスを備えることはもちろん、韓国インターネット振興院 (KISA) とアンラボが提供するランサムウェア対応ガイドを参考にし、最新の動向と対応方法を持続的に確認する必要があると呼びかけた。

イ・ミョンスチーム長は「『株式投資は毎月注意するべきだ』というマーク・トウェインの有名な格言と同じく、ランサムウェアに対するセキュリティも常時警戒心を緩めてはならない」と述べた。



[写真 5] アンラボ A-FIRST チームのイ・ミョンスチーム長は、
今年第 3四半期までのランサムウェアトレンドとランサムウェア対応戦略を紹介した。

「セキュリティにおける AI: AI-Augmented Security」というテーマで発表を行ったアンラボの人工知能チームイ・スンギョンチーム長は、LLM を始めとする AI 技術を組み合わせたセキュリティ技術が進む方向を提示した。特に、セキュリティと AI の積集合を通じて AI をセキュリティに導入する方法、セキュリティ運用の難しさを解消するにあたっての AI の役割を強調した。

イ・スンギョンチーム長は、「セキュリティにおいてもデータ規模と複雑性が大きな問題として作用するが、以前のビッグデータ時代のように、このような問題を解決するのに AI が代案となることができる。セキュリティ運用で発生する様々な問題は AI で増強されたセキュリティによって解決することができ、アンラボの AI は共通モデルをベースとするサービスプラットフォーム形式でこれを提供している」と述べた。

イ・スンギョンチーム長は、セキュリティ運用において直面する 2つの主な問題として「脅威の過負荷」と「セキュリティツールの複雑性」を挙げた。この問題を AI で解決できる案について「脅威の過負荷問題は AI が受動的かつ反応的な検知方式を脱し、能動的に潜在的脅威を早期に発見する。データを分析して異常な振る舞いを検知し、これによってセキュリティアナリストはより効果的に潜在的脅威に対応できる。セキュリティツールの複雑さの場合、AI を介してユーザーのプロセスを単純化できる。これまでのセキュリティツールは、複雑なメニューでユーザーが直接分析する必要があったが、AI アシスタントは必要なデータを自動で分析し、適切な対応策を提案することができるため、セキュリティ専門家がツールの使用に対する負担を軽減し、本来の業務に集中できる」と説明した。

[写真 6] アンラボ人工知能チームのイ・スンギョンチーム長は、AI 技術を組み合わせたセキュリティ技術が進む方向を説明した。

アンラボ融合製品サービス企画チームのイ・ゴンヨンチーム長は「f(X)D+R=0perational Efficiency、AhnLab XDR」の発表セッションで AhnLab XDR によってセキュリティ担当者がより効率的なセキュリティ運用環境を構築し、ビジネス競争力を高められる案を紹介した。

イ・ゴンヨンチーム長は、AhnLab XDR が ▲ログ統合連携分析 ▲リスク検知および通知 ▲対応など、主に 3つの側面から効率化をサポートすると発表した。イ・ゴンヨンチーム長は「AhnLab XDR は様々な発信元のデータを収集して統合分析し、セキュリティ担当者が潜在的脅威を早期発見できるようにするとともに、不要な通知を減らして ML (Machine Learning) ベースの振る舞い検知技術を活用することで、より危険度の高い通知を発見する。このほか、AI モデルをベースに推奨および自動対応をサポートし、今後公開する MXDR (Managed XDR) サービスを通じてセキュリティ担当者の業務効率性を向上させることに重点を置いている」と述べた。

イ・ゴンヨンチーム長は「AhnLab XDR は、すべてのリスクを分析して対応することで、リスクを『ゼロ』の状態にすることを目標としている。現在サービス中のパブリッククラウドだけでなく、今年の下半期にはプライベートクラウドへと対応を拡大する計画だ」と発表した。

[写真 7] アンラボ融合製品サービス企画チームのイ・ゴンヨンチーム長は、
AhnLab XDR を通じてビジネス競争力を高められる案を紹介した。

実際に AhnLab XDR を導入したアンラボの顧客、GOLFZON のセキュリティ担当者の発表も行われた。GOLFZON 情報セキュリティチームのキム・ジョンフンチーム長は、GOLFZON の AhnLab XDR 導入背景と運用ノウハウを紹介した。

キム・ジョンフンチーム長は、「AhnLab XDR が EDR と簡単に連携でき、SaaS 型で迅速な構築が可能であるという点に注目した。GOLFZON はインターネット、IDC、AWS、電子金融ネットワークなど、様々なネットワークにインストールされた EDR を XDR で統合管理しており、そのおかげでセキュリティリスクが大幅に減少した。これは、XDR を活用した脅威イベントの連携分析、根本的な原因解決により可能であったものと考えている」と述べた。

キム・ジョンフンチーム長によれば、GOLFZON は AhnLab XDR を導入したあと、不正と疑われる IP アドレスの遮断、VPN による異常なログインの遮断、BruteForce 攻撃の遮断、ファイアウォールポリシーの高度化以外にも、セキュリティソリューションログの相関関係分析による直観的かつ有意味な結果の導出などの効果を経験した。

キム・ジョンフンチーム長は「XDR を使用したとしてもすべてのリスクが自動で解決されるわけではなく、リスクの優先順位を設定して直接対応しなければならない負担は変わらず存在する。そこで GOLFZON は、AhnLab MDR を併せて導入することでエンドポイントで発生する脅威を管理しており、外部専門家のリアルタイムモニタリングと対応サポートを受け、セキュリティチームの業務負担を減らしている」と言及した。

[写真 8] GOLFZON 情報セキュリティチームのキム・ジョンフンチーム長は、
自社システムに AhnLab XDR を導入することで得たセキュリティ効果を紹介した。

アンラボのヤン・ハヨン ASEC 室長は 「Inside Out: The Anxiety (不安) in Cyber Threat Intelligence」をテーマに発表を行った。ヤン・ハヨン室長は、私たちがセキュリティで不安を感じる理由は、脅威が隠されていることを知っているのに、いつ・どこで・どのように侵害が発生するか分からないためだと説明した。これは、脅威を事前に認知して予防することができれば、セキュリティ担当者が感じる不安も軽減するということを意味する。

この観点から、ヤン・ハヨン室長は最新の脅威動向を ▲脆弱性攻撃 ▲フィッシング攻撃 ▲インフォスティーラー (InfoStealer) の 3つに分類して紹介した。各攻撃のタイプに関して実際に発生した事例と ASEC (AhnLab SEcurity intelligence Center) が分析した内容を共有した。また、アンラボの脅威インテリジェンスプラットフォームである AhnLab TIP が最新の脅威についてどのような脅威インテリジェンスを提供するのかも同時に取り上げた。

ヤン・ハヨン室長は、「AhnLab TIP は脅威が発生したあとに対応する他のセキュリティソリューションとは異なり、脅威を事前に識別して予防する事前対応の観点からアプローチする。単純に分析レポートなどのコンテンツのみを提供するのではなく、▲侵害指標 (IOC) フィード ▲脅威グループ分析 ▲サンドボックス分析 ▲ダークウェブモニタリングなど、企業および機関がサイバー脅威を先制的に理解して予防するのに役立つ様々な機能を提供している」と強調した。

[写真9] アンラボのヤン・ハヨン ASEC 室長は、
アンラボの CTI (Cyber Threat Intelligence) を活用して不安なサイバー脅威に備える案を共有した。

Simplify and Secure: Seamless Security Solutions: シームレスなセキュリティソリューションで実現するセキュリティの簡素化

アンラボのオ・サンオンソリューションコンサルティング本部長は、「Why and How to Adopt CTEM (Continuous Threat Exposure Management) 」の発表セッションで CTEM が脅威環境の制御、組織のセキュリティ強化のためのコア戦略であることを強調した。

オ・サンオン本部長によれば、在宅勤務の増加とクラウド環境の導入などでセキュリティ管理領域が拡大するにつれ、従来のデータセンターおよびオフィスネットワーク中心のセキュリティから脱却し、より広い領域を包括するセキュリティ管理が必要とのことだ。CTEM はこれらの環境に対応するための新たな手法であり、攻撃対象領域を事前に把握し、優先順位を定めて持続的に管理する戦略である。

オ・サンオン本部長は「CTEM の核心は事前予防的なセキュリティ管理である。これは単純なセキュリティソリューションの導入の枠を越え、リスクにさらされた組織の資産を持続的にモニタリングし、管理することを意味する。特に脆弱性の管理とパッチ管理のような基本的な措置を疎かにしてはならない」と呼びかけた。

また、「アンラボは CTEM の概念を AhnLab XDR に適用している。これにより、AhnLab XDR はエンドポイント、ネットワーク、クラウドなど、様々な領域のセキュリティソリューションを統合し、これに脆弱性情報や脅威インテリジェンスを連携して総合的なリスク管理が可能である。これだけでなく、自動化された対応とリスクの優先順位設定により、セキュリティチームの業務効率性を高め、必要に応じて MXDR サービスの形で提供することで組織のセキュリティ能力を強化することができる」と付け加えた。

[写真 10] アンラボソリューションコンサルティング本部のオ・サンオン本部長は、
脅威環境の制御および組織のセキュリティ強化において CTEM が核心であることを強調した。

アンラボのウォン・ナムホ技術支援本部長は「夜を『徹した』のか? 夜を徹して『泣いた』のか? (feat.Work Diet) 」というテーマでセッション発表を行った。このセッションでは、アンラボのエンドポイント保護プラットフォーム、「AhnLab EPP」を活用してセキュリティ脅威に対応し、業務効率を高める案を取り上げた。

AhnLab EPP はアンチウイルス、パッチ管理、個人情報保護、デバイス制御、EDR など、様々なセキュリティ機能を単体のエージェントで統合管理できるプラットフォームである。これにより、ユーザー PC の負担を軽減し、管理の効率性を向上させることができる。特に、「連結規則」によりセキュリティイベントに対する自動化された対応を行うことができ、セキュリティ管理者の手動介入の最小化および迅速な対応が可能となる。

ウォン・ナムホ本部長は、「AhnLab EPP は脆弱なソフトウェアを自動で検知し、削除またはアップデートすることで、企業の全般的なセキュリティ状況の改善に大きく貢献する。このほかにも、アンチウイルスのリアルタイムスキャン状態の確認、マルウェア検知時の自動隔離、個人情報流出の疑いがある振る舞いの検知など、様々なシナリオに対し自動化された対応規則を設定できる」と説明した。

これに付け加えて、「AhnLab EPP は、セキュリティパッチやエンジンアップデートの安全な配布のための段階的な配布機能を提供する。この機能を活用すれば、パッチやアップデートを段階的に適用し、潜在的な問題を事前に把握して対応することにより、企業のエンドポイントセキュリティ管理に安定性を付け足すことができる」と述べた。

[写真 11] アンラボ技術支援本部のウォン・ナムホ本部長は、
AhnLab EPP を活用したセキュリティ脅威対応および業務効率性の向上案について発表した。

アンラボのパク・テファン ACSC 本部長は「MDR と共に」をテーマに、組織で多く発生するサイバー脅威シナリオと共に、MDR の導入によって組織が得られる具体的なメリットを共有した。

パク・テファン本部長は、「これまでに組織で確認された代表的なサイバー脅威としては、攻撃者の総当たり攻撃によるランサムウェアの配布事例、電子メールに隠されたトラッキングピクセルを活用したフィッシング攻撃の試み、ライセンス認証回避ソフトウェア KMSAuto に隠されたマルウェアによる被害事例などがある。このように、企業は様々なサイバー脅威にさらされているが、MDR サービスを通じてアンラボのセキュリティアナリストによるサポートを受けることができる。MDR チームは顧客の傍らで脅威を分析し、対応案を提示する。さらには、MDR プレミアムサービスでは脅威の深層詳細分析および能動的な脅威ハンティングサービスも提供する」と発表した。

パク・テファン本部長は、ネットワーク接続が不可能な環境、クラウド環境など様々な事例において MDR サービスの対応が可能である点を強調した。パク・テファン本部長によれば、サービス導入を検討する際はアンラボの営業担当者との相談を通じて企業環境に合ったサービス案を模索できるとのことだ。

パク・テファン本部長は「AhnLab MDR サービスを通じて急変する IT 環境を狙った各種サイバー脅威に先制的に対応し、組織のセキュリティ態勢を一段階アップグレードできるだろう」と提言した。

[写真 12] アンラボのパク・テファン ACSC 本部長は、
AhnLab MDR サービスの導入によって組織が得られるメリットを紹介した。

Manage Less、Defend More: 管理よりも防御に集中せよ

「Endpoint? And Point Security!」というテーマで発表を行ったアンラボ戦略製品サービス企画チームのチョン・グァンウ部長は、ハイブリッド業務環境に最適化されたワークスペースセキュリティ（Workspace Security）戦略と、エンドポイントセキュリティの統合および連携、連動案を紹介した。

チョン・グァンウ部長は「業務環境の拡大にともない、エンドポイントセキュリティの要件も変化した。したがって、これからはエンドポイントと連結したインフラ全般にわたる包括的なセキュリティ制御が必要である」と指摘した。

チョン・グァンウ部長は、ワークスペースセキュリティのためのエンドポイントセキュリティの必須要件として ▲Platform-based ▲User-centric ▲Integration を提示した。これに関連し、チョン・グァンウ部長は「アンラボは AhnLab EPP をもとに、拡張する可視性と対応、管理および運用の複雑性減少などを実現し、最適なエンドポイントセキュリティを提供している。また、この AhnLab EPP は、ユーザー情報が含まれたサーバーおよび DB と連携し、ユーザー情報をベースに端末を識別する柔軟なアクセス方式を利用する。さらには、様々な異機種セキュリティ製品の連携および連動が可能な syslog と API も提供する」と説明した。

チョン・グァンウ部長によれば、エンドポイントセキュリティの側面において最も重要視すべき点は「Consolidation」と「Integration」だという。この 2つをユーザーの観点からどのように活用し、提供するのかをよく考える必要がある。

[写真 13] アンラボ戦略製品サービス企画チームのチョン・グァンウ部長は、エンドポイントセキュリティに重点を置き、ハイブリッド業務環境に最適化されたワークスペースセキュリティ戦略を説明した。

アンラボ融合製品サービス企画チームのユン・ビョンソン次長の「Network PLUS: A to Z AhnLab ZTNA」発表セッションでは、ゼロトラスト導入のために知っておくべき基本概念と AhnLab ZTNA の現在と未来を重点的に取り上げた。

ユン・ビョンソン次長は、「ゼロトラスト導入のための核心的な要素は ▲識別子および身元 ▲機器とエンドポイント ▲ネットワーク ▲システム ▲応用およびワークロード ▲データであり、これらを貫通する交差機能としては ▲可視性および分析 ▲自動化および統合がある。ゼロトラストの成熟度段階は『既存』、『向上』、『最適化』に区分されるが、短期間で最適化の水準に移行することは不可能だ。したがって、『準備 – 計画（設計）– 実装（導入）– 運用』のゼロトラスト導入段階を何度か繰り返すことでようやくゼロトラストの高度化が可能である」と述べた。

また、ユン・ビョンソン次長は AhnLab ZTNA に関して、ZTNA ポリシーと規則設定、認証、デバイス確認を担当する「ZTNA Manager」と、接続およびアクセス制御、モニタリングを遂行する「ZTNA Gateway」がインストールされており、これらは物理的に分離されていると説明した。すなわち、制御領域とデータ領域が完全に分かれており、より強力なセキュリティを提供するということである。

ユン・ビョンソン次長は「この 2つの領域にアンラボのファイアウォール・アプライアンスである XTG を始めとして EPP エージェント(Agent)、ESA（EPP Security Assessment)、V3 を連携すれば、より多様なデバイス情報を収集できる。AhnLab ZTNA は今後、ハイブリッドクラウドおよびネットワーク分離、自社およびリモート接続環境に幅広く構築される可能性がある」と付け加えた。

[写真 14] アンラボ融合製品サービス企画チームのユン・ビョンソン次長は、
ゼロトラストおよび ZTNA の概念と導入案を紹介した。

アンラボクラウド開発室のノ・ヨンジン常務は、「コンテナ中心のクラウドセキュリティ: SBOM と eBPF を活用した最新のセキュリティ戦略」をテーマに、SBOM およびランタイムセキュリティ戦略をもとに、安全なコンテナ運用案を提示した。

ノ・ヨンジン常務は「クラウドの核心である柔軟な運用に最も重要な役割を担う要素は、『コンテナ』である。しかし、このコンテナはオープンソースに対する可視性がなく、発見されていない脆弱性が存在し、DoS 攻撃によって無力化するリスクがある。そのような理由から、コンテナのセキュリティを強化するには、既存のカーネルセキュリティ以外に体系的なオープンソース管理のための SBOM (Software Bill of Materials) が必要である」と強調した。

また、ノ・ヨンジン常務は、「開発およびサプライチェーンの段階で防ぐことができないセキュリティリスクの場合、ランタイムセキュリティで解決する必要がある。ランタイムセキュリティは、最新のコンテナ環境におけるリアルタイムモニタリングと制御を通じて、より安全な環境を構成する。このほか、セキュリティモジュールの強力な集中統制が可能でありながらも、ブルースクリーン (BSOD) イシューなく安全なセキュリティ適用のためには eBPF も必須である。ただし、eBPF をセキュリティ要件に合わせて幅広く適用できるようにするべきだ」と提言した。

[写真 15] アンラボクラウド開発室のノ・ヨンジン常務は、
安全なコンテナ環境作りのための SBOM とランタイムセキュリティの必要性を強調した。

アンラボ融合製品サービス企画チームのファン・ジェフン部長は「Continuous Puzzle Games in CPS World」に関する発表を行った。CPS (Cyber-Physical System) 環境の様々なセキュリティイシューと動向を紹介し、これに対するアンラボの対応戦略を共有した。

ファン・ジェフン部長によれば、CPS 環境には多くの技術とデバイスがパズルピースのように絡んでいるという。したがって、セキュリティの脆弱性も非常に多種多様であり、これらに対する対応能力もまだ不足しているのが実情である。さらに、最近では攻撃者が IT と OT 環境の両方を狙う脅威や、AI 技術を活用した攻撃も増加しており、セキュリティの危険性がより重みを増しているという。

ファン・ジェフン部長は、CPS セキュリティは主に ▲可視性 ▲検知 ▲対応の側面から考慮する必要があると言及した。アンラボも、現在この 3つにすべて対応している。

ファン・ジェフン部長は、「CPS 環境において、運用に影響を及ぼすことなく可視性を効果的に確保する最良の方法は、ネットワークトラフィックをもとに分析することである。別途エージェントをインストールしなくても、パケットさえ収集できれば資産を識別できるためである。これに加え、エンドポイントベースの識別を並行すれば、より向上した可視性を確保できる。さらに、CPS セキュリティ資産に対するエンドポイントのハードニングを通じて、資産で使用されるプロセスとリムーバブルメディア、ネットワーク通信に対し、許可リスト (Allow List) をもとに事前に登録したものだけを許可するよう制御すれば、ランサムウェア、APT 攻撃などの新種・変種の脅威から資産を効果的に保護できる」と助言した。

[写真 16] アンラボ融合製品サービス企画チームのファン・ジェフン部長は、
CPS 環境の高度化するセキュリティ脅威に対応する方法を紹介した。

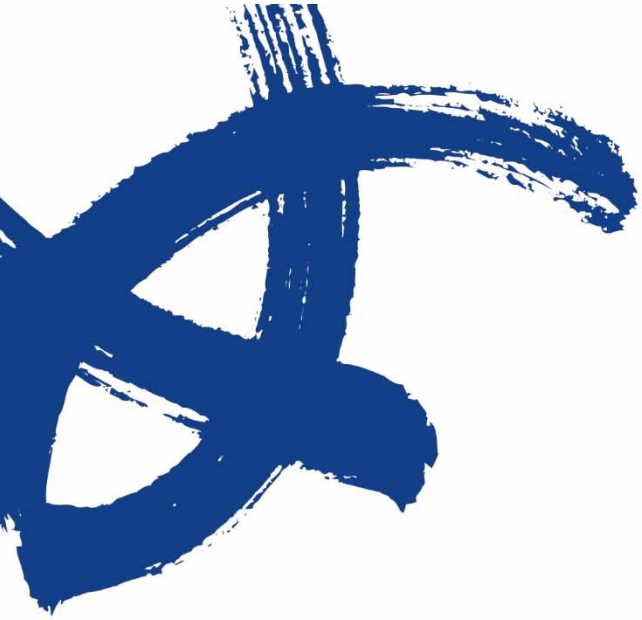
すべての発表セッションが終了したあと、アンラボは景品抽選を行い、盛り上がったイベントの雰囲気にさらに拍車をかけた。これに加え、イベント会場のロビーには、アンラボとアンラボ子会社のグローバル戦略製品およびサービスを直接体験できるデモブースが設けられた。ブースを訪れた参観者には、アンラボセキュリティソリューションの効果的な導入のためのカスタマイズされた相談も提供された。

[写真17] イベント会場ロビーのデモブースで製品を試演する様子 (1)

[写真 18] イベント会場ロビーのデモブースで製品を試演する様子 (2)

結び

今年で 16年目を迎えた AhnLab ISF 2024 は、AI と統合セキュリティというキーワードを中心に大勢の参観者とセキュリティインサイトを共有することができた連帯の場となった。参考までに、AhnLab ISF の正式名称は「AhnLab Integrated Security Fair」であるが、アンラボは 16年前から統合の重要性を強調し続けており、これからも AI のような新技術、および自社プラットフォームを高度化してユーザーのビジネス生産性向上に貢献していく計画である。冒頭で述べたように、今や 1つの企業ですべてのサイバー脅威を解決することはできない状況であるだけに、アンラボを含むより多くの企業や機関が共に協力し合い、進化する脅威に賢く対応していくことを願う。



https://www.ahnlab.com/jp

https://www.ahnlab.com/en

https://www.ahnlab.com/ko

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)