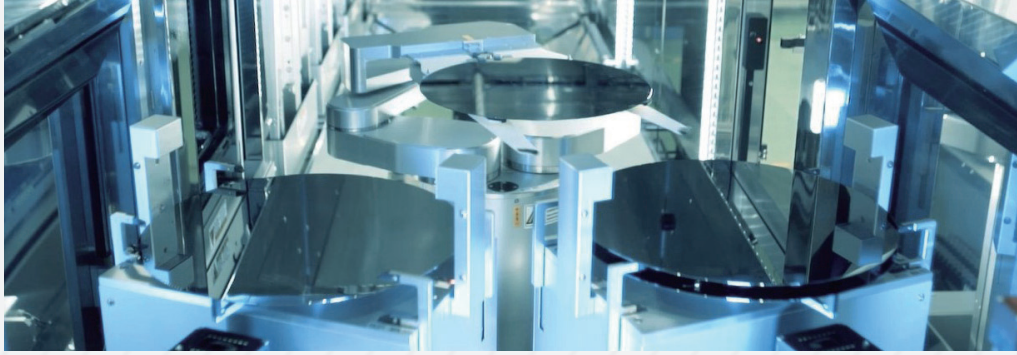
CrowdStrike 導入事例



ローツェ株式会社

1年の間に2つのMDRを経験、求める説明責任レベルを追及し Falcon Completeに運用を任せ、取引先のセキュリティ要求にも対応

米国CHIPS法を契機に、
取引先のサプライチェーン管理が厳格化

ローツェ株式会社は、広島県福山市神辺町に本拠地を要する製造事業者である。半導体関連装置、フラットパネルディスプレイ関連装置、ライフサイエンス関連装置、モータ制御機器などの開発・製造から販売までを一貫して行っている。フィロソフィーは「技術に自信を持って、楽しみながら仕事のできる集団」。事実、同社は「独自製品の開発・設計」「垂直統合型生産体制」「グローバルネットワーク」を強みに、全世界を対象としたビジネスを展開している。

米国には、同社にとって大きな取引先である半導体企業がある。同国では、2022年8月、CHIPS法が成立した。この中ではサプライチェーンの強化も盛りこまれており、セキュリティ対策も含めて、サプライチェーン管理の徹底が求められたのである。米国企業は、法案の成立を見越して2020年前後から動き出していた。ローツェの取引先もサプライチェーン企業に対策を求めた。

実際のところ、同社でも前々からサイバー脅威の増大を懸念していた。すきを見せれば、侵入され知的財産が奪われる、半導体業界の話ではないが、特定の企業でしか生産していない製品が、なぜか別の国から新製品として世に出るということが実際に起こっている事例を目にしていた。製造業としては、製品に関わる情報はビジネスにおいて最重要データである。

そのころ同社にUターン入社し、IT戦略室長に就任したのが南　勲氏だった。当時を振り返って同氏は語る。

「自らセキュリティが強化できなければ取引停止です。自ら防御力を高める以外に方策はありません。在広島ということもあってのんびりしていた当社でしたが、今までの膿をすべて出しきるつもりで、5年計画のITおよびセキュリティの大刷新を決断しました」

NGAV、EDRの選定を開始
実際の試用を経るも、ライセンスコスト効率を
重視しベンダーを選定

従来、エンドポイント保護は、アンチウイルスソフトが主軸だった。もはやパターンマッチングで攻撃を防ぐことは難しく、侵入されることを前提に対策を講じるべきと、IT戦略室は次世代アンチウイルス（NGAV）、EDR導入の検討を開始。4社4製品を候補に挙げ、実際に3製品を試用して選定を進めた。ローツェ株式会社 IT戦略室 金井 康洋氏は次のように語る。

「最も使いやすかったのはCrowdStrike Falconプラットフォームで、きちんと脅威を検知しますし、その脅威の中で行われた一連の動きが把握しやすい、何が起きたかを理解できるGUIが提供されている。これならIT戦略室での運用にも乗るなと思い、私たちの評価では一番上にランキングしました」

また、当初から生産を伴う海外拠点にも導入したいと考えていたため、グローバル対応可能であるという点も要件に合致していた。

しかしこのとき、別のベンダーが運用専門サービスMDR（Managed Detection & Response）の提供を含めて大幅なディスカウントを提案してきた。同社にとって、MDRは魅力的だった。IT戦略室は常に業務が山積している状態であったが、元々は自社運用を検討、社内工数を削減できるならそれに越したことはなかったこと、また、MDRで攻撃と対応の詳細レポートが提供されることで、万が一謝罪会見を開くような事態になった場合も説明責任が果たせると考えた。そして、価格とMDRという2つの観点から、このベンダーの製品を導入することになった。

問題が起きた際に、安心して対応を任せられる、
説明責任が果たせるMDRに投資すると判断、
リプレースを決断

期待は大きく裏切られる結果となった。MDRにより運用を一任できるはずだったのが、アンチウイルスソフト時代より社内工数が大きく跳ね上がったのである。ひとつの原因は、ベンダーのサービススコープ制限だった。NGAVについては、検知を行い、通知もするが、対応はしないというのだ。しかし、ひとたび検知されてしまったら、IT戦略室としては対応しないわけにはいかない。それに時間を取られ、日本での累積運用工数が10か月で300時間に上り、人件費に換算すると400万円以上を費やすこととなり、他の作業に支障をきたした。また海外拠点のベトナムでも600時間現地の工数を使っていた。これでは何のためにMDRを依頼しているのかわからない。また、問い合わせても対応のレスポンスや返答は求めているレベルで提供されることはなく、なかには6カ月にわたって回答が得

RORZE

業種
開発・製造

所在地
広島県福山市神辺町道上1588-2

ローツェ株式会社

「世の中にないものをつくる」を合言葉に、創業より三十余年、半導体、フラットパネルディスプレイ業界において、独自の技術と経験で最先端技術への貢献を続けてきた。高い信頼性とクリーン度を誇る搬送ロボットおよび装置は、世界中の半導体、FPD製造工場で稼働する。新たな製品の開発、新たな業界へのたゆみない挑戦を通じて、持続的な成長に努めるとともに、すべてのステークホルダーと革新的な社会の実現をめざしている。

https://www.rorze.com/

導入製品

- CrowdStrike Falcon Complete™
  - MDR (Managed Detection & Response)
- CrowdStrike Falcon Prevent™
  - 次世代アンチウイルス
- CrowdStrike Falcon Insight XDR™
  - EDR
- CrowdStrike Falcon Discover™
  - IT資産管理
- CrowdStrike Falcon OverWatch™
  - プロアクティブな脅威ハンティング

導入時期：2023年1月

られないものもあった。

IT戦略室は、1年も待たずにリプレースに向けて動き始めた。候補製品はもう、前回一番評価だったクラウドストライクしかなかった。当時は検討しなかったが、クラウドストライクもMDRサービスCrowdStrike Falcon Completeを提供していると知り、迷いはなかったと南氏は語る。

「私たちのように少ない人数でIT業務を行う組織にとって、責任のある調査と回答を得るためにMDRは必要です。コストはかかりますが、もうこれなしに説明責任を果たせないことは経営層も理解しました。何が原因で起きたといえるのか、影響範囲は限定されていると何を根拠に保証するのか。謝罪会見で『さあ、そこはちょっとわかりません』と答えるようなことになったら、社会的に信用を失いますし、どれだけ機会損失するかわからない、致命的なことになると思いました。CrowdStrike FalconCompleteは製品的に最もすぐれたCrowdStrike Falconプラットフォームの MDR。トップエンジニアでなければその職につけないと聞いていたこともあり、迷いなくリプレースを決めました」

社内工数が以前の10%未満に激減、説明責任が果たせる体制を確立

切り替えは2023年1月にスタート。約2カ月間で、NGAVであるCrowdStrike Falcon Prevent、EDRのCrowdStrike Falcon Insight XDR、プロアクティブな脅威ハンティングCrowdStrike Falcon OverWatch、IT資産管理 CrowdStrike Falcon Discoverの4製品が利用可能な状態になり、MDR運用も開始された。現在、日本国内は約600台、生産拠点のあるベトナムは約400台のエンドポイントが保護下に置かれ、それぞれ別のインスタンスとして管理されている。

導入から約半年、その最大の効果として南氏はIT戦略室での運用工数激減を挙げる。

「国内、ベトナム拠点とともに、旧ベンダー比10%未満になりました。CrowdStrike Falcon Completeが対応してくれるため、こちらはほぼ何もしなくていい状態です。自社にあった設定の適用、脅威については検知したものへの調査、対応、修復までを一環して即実施してくれます。Eメールで『こういうことがあり、こういう対応が完了した』という報告を読むことで完結します。たまに『こういうことがあり、エンドポイントを隔離しています、ここを確認してください』という、どうしても判断つかないものだけ指示連絡がありますが、それでも、こちらが何をすれば良いのかが明確にわかります。いざとなったら外部に対し説明責任を果たせる状態だと自信を持って言えるようになりました」

ローツェ株式会社 IT戦略室 松林 宏明氏は、補足してこう語る。

「私たちが行う社内の作業を挙げるとしたら、従業員との調整ぐらいです。私たちもFalconコンソールで全てのログ、対応状況が確認できます。それを見て『これは何だろう』と思ったときに問い合わせれば、詳しい回答がすぐ返ってきます。安心できるし、勉強にもなります。何を根拠として安全あるいは怪しいというのか、安全というためには何を調査すべきかといったことを極めてロジカルに担当アナリストが示してくれるからです」

実際に自社だけでセキュリティ強化を図ろうとしたら、専門家を2名は雇い入れる必要があり、その人件費を考えたら雇用の費用として少なくとも年間2,000万円はかかるが、MDRで安価に収まった。「過去導入したベンダー製品、MDRは、大幅ディスカウントされていても、追加でかかる自社メンバーの人件費コストが多大でした。Falcon Completeに置き換えた事で、コストは大幅に浮いたと言えます。」

ローツェのIT戦略室にセキュリティ組織を新設したかの様に感じるMDR

そして、CrowdStrike Falcon Completeは専門家が社内にいるのと同じ、完全に信頼できるという点も大きい、ローツェのIT戦略室にセキュリティ組織を新設したかの様に感じる、と南氏は続ける。

「当社で開発している自作ソフトがFalconで検知されるので、除外設定を考えなければいけないというケースがあったんですが、それも『A案とB案は推奨できますが、C案はこういった理由から承諾できません』とはっきりした形で出てくる。それも1時間ぐらいで返ってきます。問い合わせのキャッチボールで、私たちがボールを持ったままだと、『この件はどうなっていますか』と逆質問が来ます。言われたことだけをやるという部隊ではない、信念を感じます」（南氏）

もちろん、セキュリティレベルは大きく向上した。エンドポイントの状況がリアルタイムに可視化可能になった。実のところ、NGAVとEDRを導入すると工数は下がると思っていたが、検知され、可視化されるからこそ対応だけでなく、説明しなければならないために運用の工数は上がることが見えた。ローツェではそこをMDR活用でカバーしている。エンドユーザー自身のセキュリティ意識も向上しており、「自作ソフトをうまく使えるようにするなら、電子署名を導入すべきでは」という提案が挙がってくるほどだという。

今後ローツェは、自社の知的財産の保護を最大の防御目的に、さらなるセキュリティ強化を図っていく。

「もうビジネスの現場は、『うちは製品がいいから大丈夫』などと、のんきに構えている場合ではありません。実際にサイバー侵害を受けて工場が止まることや、知的財産が持ち出されることがあってはなりません。事故がなくともセキュリティレベルが低いために、取引を打ち切られたり、経営の手綱を握られてしまう事態もあり得ます。どの企業も、自衛力を上げるのか、外部の力を使うのか、きちんと投資の幅を決め、真剣に対処すべき岐路に差しかかっていると思います」

CrowdStrike Falcon Complete導入により、運用外部化に成功したローツェ IT戦略室の南氏は、セキュリティ対策に対峙するものづくり企業に対して、こうメッセージしていた。

ローツェ株式会社
IT戦略室 室長
南 勲 氏

ローツェ株式会社
IT戦略室
松林 宏明 氏

ローツェ株式会社
IT戦略室
金井 康洋 氏

POINT

- 米国CHIPS法を機に取引先企業から要請されたセキュリティ強化に対応
- 価格優位性で選択したNGAV,EDR,MDRは自社の求める説明責任を果たせるのか、実際の運用を経験し理解
- 問題が起きた際に、安心して対応を任せられる、説明責任が果たせるMDRに投資すると判断し、CrowdStrike Falcon Completeにリプレース
- 社内工数は10%未満に激減
  説明責任を果たせる体制が確立

CROWDSTRIKE

we stop breaches

クラウドストライク合同会社
お問い合わせ: **http://crowdstrike.jp/contact-us/**