FORTINET 제공

THE GORILLA GUIDE TO...®

확장된 탐지 및 대응(XDR)

Lawrence Miller

가이드 요약:

- 가장 큰 사이버 보안 문제
- 확장된 탐지와 대응에 대한 이해
- 적절한 XDR 솔루션 찾기

HELPING YOU NAVIGATE THE TECHNOLOGY JUNGLE!

ActualTech Media
www.actualtechmedia.com

파트너

FORTINET®

고릴라 가이드...

확장된 탐지 및 대응(XDR)

Lawrence Miller

ACTUALT ECH MEDIA

6650 Rivers Ave Ste 105 #22489
North Charleston, SC 29406-4829
www.actualtechmedia.com

출판사 감사말

편집자
Keith Ward, ActualTech Media

프로젝트 관리자
Wendy Hernandez, ActualTech Media

편집 총괄
James Green, ActualTech Media

레이아웃 및 디자인
Olivia Thomson, ActualTech Media

정글을 향해서

이 책에 사용된 기호

고릴라는 사람들의 학습을 돕는 것을 좋아하는 교수와 같은 존재입니다. School House 기호가 나오면 메인 주제에서는 벗어나지만 중요한 주제에 대한 정보를 얻을 수 있습니다.

책자에 나온 부수적 주제에 대해 좀 더 자세히 알아볼 수 있는 특별한 곳입니다.

좋은 아이디어가 있으면 Bright Idea 섹션에서 설명합니다.

특정 주제에 대해 매우 심층적으로 살펴봅니다.

비즈니스 리더가 전략적으로 관심을 가질 만한 내용을 설명합니다.

이 책에 사용된 아이콘

정의

단어, 문구 또는 개념을 정의합니다.

이해도 확인

읽은 내용에 대한 이해도를 테스트합니다.

중요

이 내용은 꼭 확인하십시오!

GPS

여러분을 적절한 지식으로 안내합니다.

주의!

이 내용은 꼭 읽어보고 중대한 실수 예방하십시오!

팁

책 내용을 바탕으로 한 유익한 조언입니다.

소개

데이터와 인프라를 보호하는 새로운 방법

고릴라 가이드® 확장된 탐지 및 대응(XDR)에 오신 것을 환영합니다! 이 책은 XDR이라는 약어조차 처음 들어보는 분을 위한 것입니다. XDR에 친숙한 분에게도 좋습니다!

IT 보안은 지금 그 어느 때보다 복잡하고, 빠르게 발전하고 있다고 해도 과언이 아닙니다. 퍼블릭 클라우드, 엣지 컴퓨팅, 사물 인터넷 등이 폭발적으로 늘어나고 있는 가운데, 사이버 보안 위협은 더욱 다양화되고 공격 벡터도 급증하고 있는 와중에 이 모든 것을 적시 적소에 보호하는 작업은 불가능에 가깝고 고단하기 짝이 없습니다.

그렇다면 어떻게 해야 할까요? 우선, 이 가이드를 읽어보는 것도 좋은 출발점이 될 수 있습니다! 이 간단한 책자에서는 데이터와 인프라에 대한 보안 위협을 찾아내서 해결하기 위한 새로운 방법으로 등장한 '확장된 탐지와 대응(XDR)' 기술에 대한 기본 지식을 제공합니다. XDR은 범죄자보다 한발 앞서서 가장 중요한 IT 자산을 지킬 수 있는 흥미로운 기술입니다.

이 책자는 보안 아키텍트, CISO, 보안관제 인력, 사이버 보안 관리자를 비롯한 IT 보안에 종사하는 사람이라면 누구나 읽어보시면 좋습니다. 책자를 다 읽고 나면 XDR 프레임워크의 장점이 무엇이고, 적절한 솔루션을 어떻게 선택해야 할지 알 수 있게 됩니다.

출발할 준비가 되셨다면, 모자를 쓰고 단검을 들고서 고릴라의 안내에 따라 정글로 들어가십시오. 사이버 보안 문제와 XDR의 개요를 살펴본 후, XDR이 중요한 이유를 설명하겠습니다.

1장

문제 해결

요약:

- 데이터는 그 어느 때보다 위협에 노출되어 있습니다.
- 범죄자가 더욱 지능적으로 시스템 취약점을 찾아냅니다.
- IT인프라 복잡성 증가 = 사이버 보안 위험의 증가

모든 산업 조직은 생산성 향상, 비용 절감, 우수한 고객 환경 제공, 경쟁력 있는 차별화, 산업 및 사업 모델 재편을 위한 전략으로 디지털 혁신을 추구하고 있습니다. 자연스럽게 이런 디지털 혁신은 조직의 IT 에코시스템과 공격면을 확장시키는 부작용을 유발합니다. 그와 동시에 사이버 보안 위협도 더욱 지능화되어 엄청난 파괴력을 자랑하고 있습니다. 보안 팀은 확장된 공격면에 대한 정보를 얻고 이를 제어하는 데 어려움을 겪고 있으며, 단일 기능의 보안 도구 솔루션이 늘어나서 기존의 복잡한 환경이 더욱 복잡해지면서 혼란을 경험합니다. 게다가 보안 전담 인재가 부족한 시장에서 우수한 보안 인력을 데려와서 유지하고 늘어나는 보안 투자에 대한 수익을 확보하느라 운영 비용도 상승합니다.

디지털 공격면의 확장

최근 10년 사이에 여러 가지 중요한 트렌드가 나타나면서 사이버 범죄자에게는 먹잇감이 풍부한 환경이 조성되었습니다. 예를 들어, 클라우드 및 모바일 컴퓨팅이 대두되고, 사물 인터넷(IoT)이 성장하였고, 최근 들어서는 (글로벌 팬더믹으로 인해) 언제 어디서나 또는 재택근무를 하는 업무 방식이 급격히 확산되었습니다. 디지털 공격면은 확장 수준이 아니라, 폭발 수준으로 늘어났습니다.

"충분히 예상하실 수 있듯이, 기회주의적인 피싱 범죄자에서부터 계략을 꾸미는 국가를 뒷배경으로 둔 자들에 이르기까지 온갖 종류의 사이버 범죄자들이 팬더믹을 이용해 금전적인 이익을 취하려는 방법을 찾아냈습니다. 전 세계의 각 기업 조직은 하루아침에 대다수 직원의 재택근무 환경 수요를 지원해야만 했습니다. 공격자들은 이런 변화 덕분에 사이버 보호 체계가 약한 원격 네트워크, 소비자 기기, VPN 연결, 영상 통신, 협업 도구 등을 타겟팅하여 기업 네트워크로 침투할 수 있는 절호의 기회를 얻었습니다." (포티넷 2020년 1분기 위협 동향 보고서)

이제 보안 관제(SecOps) 팀은 사용자, 기기, 네트워크 내부(캠퍼스, 지점, 공장)와 외부(가정 및 모바일) 연결, 퍼블릭 및 프라이빗 클라우드 환경이 공존하는 하이브리드 디지털 영역에서 위험을 관리해야 합니다. SecOps 팀은 IT 환경에 대한 전체적인 가시성과 통제권을 얻는 데 어려움을 겪고 있어서, 그야말로 엣지(예: 자격 증명 엣지, 엔드포인트 엣지, WAN 엣지, 홈 엣지, 데이터 센터 엣지, 클라우드 엣지) 위를 걷는 생활을 합니다(**그림 1** 참조).

하이브리드 네트워크

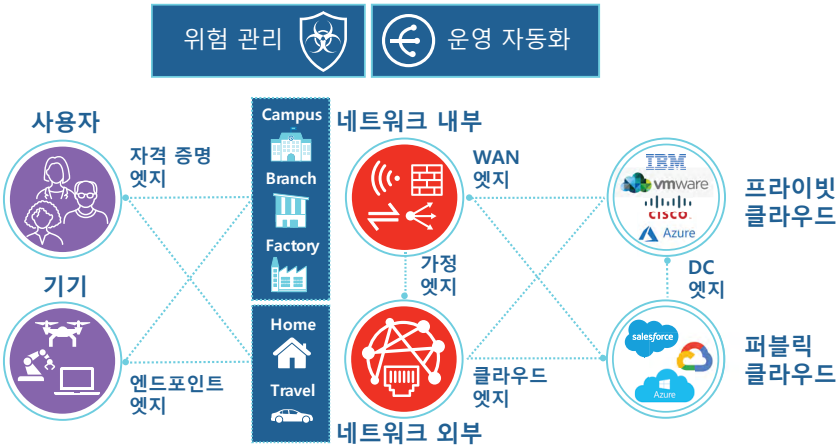


그림 1: 하이브리드 환경에서 여러 엣지의 위험 관리 포인트.

Flexera 2020 State of the Cloud Report에 따르면, 기업의 93%가 평균 7개 이상의 퍼블릭 및/또는 프라이빗 클라우드가 혼재된 멀티 클라우드 전략을 사용한다고 합니다. 상당수 기업이 앞으로 12개월 이내에 모든 워크로드(60%)와 데이터(58%)의 절반 이상을 퍼블릭 클라우드에서 운영할 계획입니다. 이런 기업 중 86%가 멀티 클라우드 전략을 하이브리드 클라우드 모델로 확장했습니다. 멀티 클라우드를 지원하는 가장 일반적인 아키텍처 유형인 데이터 통합(41%)을 필두로 클라우드 간 워크로드 이동성(36%), 재해 복구 및 클라우드 간 장애 조치(35%), 퍼블릭 및 프라이빗 클라우드를 연결하는 개별 애플리케이션(34%)이 이어집니다. 이러한 환경 변화가 보안에 의미하는 것은 무엇일까요?라는 질문에 조사 대상 기업의 83%가 클라우드를 이용할 때 가장 큰 문제가 보안이라고 답했습니다.

위협의 지능화

그와 동시에 사이버 보안 위협 자체도 끊임없이 변형되고 진화합니다. 지능적 사이버 보안 위협의 빈도, 속도, 규모, 정교한 수준이 점점 높아지고 있습니다. 글로벌 팬더믹에도 이러한 위협 세력은 건재합니다. PurpleSec에 따르면, 2020년에 사이버 공격이 600%나 증가했습니다.

지능적인 피싱 이메일 캠페인은 재택근무자를 노리고, 랜섬웨어는 코로나바이러스와의 싸움의 격전지인 병원과 의료 기관은 물론이고 생명공학 및 제약 연구 시설까지 괴롭힙니다. Verizon의 2020 Data Breach Investigations Report에 따르면, 2020년에 보안 침해가 약 4,000건 발생하였고 그중 521건이 의료 산업에서 일어났습니다. 피싱과 랜섬웨어 외에도 취약점 익스플로잇, 기타 멀웨어, 봇넷, 운영 기술과 IoT를 노리는 위협이 더욱 기승을 부리며 지능화되고 있습니다.

사이버 보안 위협을 주도하는 적대 세력 자체도 지능적으로 바뀌었습니다. FortiGuard Labs에 따르면, "전체 사이버 공격의 절반 이상이 대부분 기업보다 철저하게 관리되는 사이버 범죄 조직에서 관리합니다". 사이버 범죄 산업에서 형성된 서비스형 사이버 범죄 에코시스템도 급격히 덩치를 불렸고, 연 매출이 1조 달러 이상에 달해 사실상 누구나 사이버 범죄에 뛰어들 수 있게 되었습니다. 각 국가에서도 Ramsay, Gamaredon, APT32, Kimsuky와 같은 지능적 지속 위협(APT) 그룹을 통해 전략과 기술을 발전시키고 있습니다.

최근 몇 년 사이에는 랜섬웨어 공격이 상당히 증가했습니다. 2020년 3분기에만 전 세계적으로 2억여 건의 랜섬웨어 공격이 보고되었고(Security Boulevard 기준) 기업이 랜섬웨어 공격에 치르는 평균 비용은 $133,000였습니다(PurpleSec 기준). 공격을 시작하기가 쉬워졌기 때문에 랜섬웨어 공격이 늘어나게 되었습니다. 아마추어 사이버 범죄자는 서비스형 랜섬웨어(RaaS) 상품이나 다크 웹에서 바로 구매할 수 있는 랜섬웨어 키트를 사용할 수 있습니다.

팬더믹으로 인해 경제적 피해를 본 기업이 보안 침해나 공격을 당하면 운영을 지속할 수 없을 만큼 타격을 받을 수 있습니다. PurpleSec에 따르면, 사이버 범죄의 43%가 소규모 기업을 노리고 피해 기업의 60%가 사이버 공격을 받고 6개월 이내에 사업 운영을 중단합니다.

보안 에코시스템의 복잡성으로 인한 대응 지연

효과적인 사이버 보안 전략을 수립하려면 예방 및 탐지/대응 기능을 모두 포함한 균형 잡힌 방법이 필요합니다. 현재 조직에서는 사이버 공격과 보안 침해를 막기 위해 여러 가지 보안 기술을 배포합니다. 예를 들어 다음과 같은 기술이 있습니다.

- 차세대 방화벽(NGFW)
- 네트워크 액세스 제어(NAC) 및 자격 증명과 액세스 관리(IAM)
- 보안 이메일 게이트웨이(SEG)
- 웹 애플리케이션 방화벽(WAF)
- 엔드포인트 보호 플랫폼(EPP)
- 클라우드 액세스 보안 브로커(CASB) 및 클라우드 워크로드 보호(CWP)

그러나 100% 공격 차단은 불가능하다는 것을 깨닫고 신속하고 효과적인 탐지 및 대응 전략으로 옮겨가는 움직임이 늘어나고 있습니다.

노이즈 속에서 중요한 신호를 찾다 보면 위협과 공격을 신속하고 효과적으로 탐지하여 대응하는 능력에 부정적 영향을 미치기 때문에 SecOps 팀이 엄청난 위협 횟수와 알림을 감당하기 어려울 수 있습니다.

2017년에 Enterprise Strategy Group(ESG Research Report: Cybersecurity Analytics and Operations in Transition)과 시장 조사 기업 Ovum이 실시한 조사에 따르면, 많은 IT 및 보안 전문가가 25개 이상의 사이버 보안 도구를 사용하고 상당수가 100개 이상의 보안 도구를 사용합니다. 최근 들어서는 그 숫자가 더욱 늘어났을 것이 틀림없습니다.

이런 트렌드는 계속 이어졌습니다. 이는 최근 Forrester Research 조사(The 2020 State of Security Operations)에서 SecOps 팀이 평균 10가지 이상의 보안 도구 카테고리를 이용한다는 결과가 나온 것에서도 알 수 있습니다. 설상가상으로 이런 보안 도구 대부분은 단독 기능을 수행하는 포인트 제품이라서 타 시스템과의 통합과 자동화 기능이 제한되어 있고, SecOps 분석가는 보안 에코시스템에 존재하는 다양한 관리 콘솔에서 위협과 이벤트 정보와의 상관관계를 빠르고 정확하게 찾아낼 수 없습니다.

운영 비용 상승

보안 에코시스템의 복잡성은 인시던트 탐지와 대응을 지연시킬 뿐만 아니라 운영 비용도 상승시킵니다. 공격면의 엣지 수가 기하급수적으로 늘어나면서 필요한 정책과 제어 포인트도 마찬가지로 늘어납니다. 특히, 자격 증명, 기기, 클라우드, 홈 엣지에서 그런 현상이 두드러집니다. 이런 식으로 확장이 일어나면 하드웨어, 소프트웨어 및/또는 가상 보안 기기와 도구는 물론이고 이런 새로운 정책과 제어 포인트를 배포, 구성, 관리, 유지, 사용할 숙련된 사이버 보안 인력에 대한 투자가 추가로 필요합니다.

그러나 안타깝게도 사이버 위협과 공격의 빈도, 속도, 규모, 정교한 수준이 높아지는데도 불구하고 오늘날 보안 인력 시장의 보안 인력 풀이 심각하게 부족한 것이 현실입니다. 2019년에 공개된 International Information System Security Certification Consortium(ISC)[2] Cybersecurity Workforce Study는 일자리와 근로자의 수급 불균형이 완전히 해소되려면 현재 전 세계적으로 280만 명이 일하고 있지만, 여기에 400만 명의 사이버 보안 전문가가 추가되어야 한다는 결론을 내렸습니다.

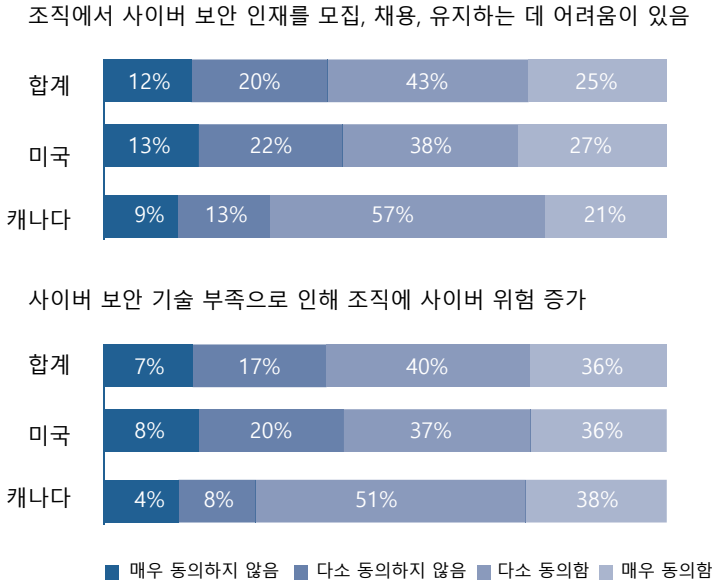


그림 2: 조직의 채용난과 관련 사이버 위험.

포티넷이 의뢰한 2020년 3월 설문조사에 따르면, 조직의 68%가 사이버 보안 인재를 모집, 채용 및 유지하는 데 어려움을 겪고 있고(**그림 2** 참조) 76%가 기술 부족으로 인해 조직 내 보안 위험이 증가했다고 답했습니다.

기술 부족으로 인해 조직 내 보안 위험이 증가한다는 인식은 근거 없는 생각이 아닙니다. 설문조사에 참여한 조직의 약 3/4(73%)이 지난해에 사이버 보안 기술 인력이 부족한 것이 보안 침입/침해사고 발생 원인인 비율이 한 건 이상이었다고 답했습니다. 이들 조직의 절반(47%) 정도에서 보안 침입이 3건 이상 발생했습니다(**그림 3** 참조).

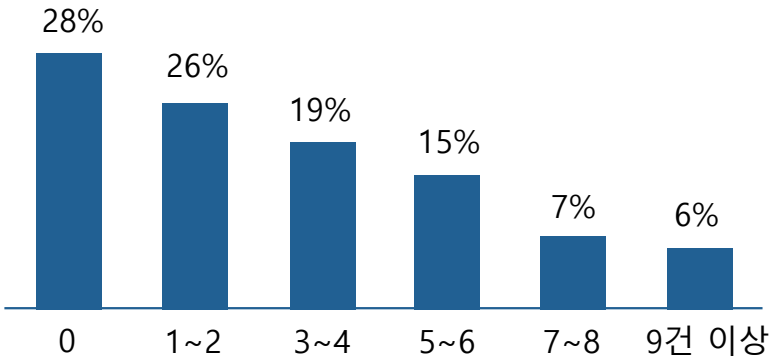


그림 3: 사이버 보안 기술 인력 부족으로 인해 발생한 보안 침입/침해 건수.

요컨대 조직에 자격을 갖추고 경험이 풍부한 사이버 보안 전문 인력이 없다면 네트워크, 시스템, 애플리케이션, 민감한 고객 데이터와 기밀 데이터가 사이버 공격과 보안 침해에 노출될 위험이 훨씬 큽니다.

보안 KPI 설정 및 추적

조직에서 보안 기술과 사이버 보안 인력에 대한 투자가 지속되면서 사이버 보안 리더들은 더욱 조직에 투자 수익(ROI)을 내야 한다는 압박에 시달립니다.

그러나 이는 사이버 보안의 역설입니다. 사이버 보안 전략이 성공적일수록 사이버 공격과 보안 침해를 더 많이 막아낼 수 있습니다. 그렇다면 그 반대는 어떻게 입증합니까? 발견되었다면 '알려지지 않은 공격이 아니기 때문에 알려지지 않은 공격이 조직에 침투한 적이 없다는 것은 증명할 수 없습니다.

2장

XDR이란?

요약:

- XDR의 정의
- 주요 기능 설명
- XDR이 제공하는 보안상의 이점

엔드포인트 보호는 30년 이상 발전을 거듭해 왔습니다. 안티바이러스 소프트웨어, 호스트 기반 침입 탐지 시스템 등의 초기 독립형 보안 제품에서 시작했고, 지금은 다양한 예방 기술과 추가적인 탐지 기술을 결합해 최대 규모의 공격면(즉, 엔드포인트)을 보호하는 포괄적인 통합 EPP 제품군으로 발전했습니다. 오늘날 엔드포인트 탐지 및 대응(EDR) 기능은 보안 인시던트 대응 팀이 기본으로 사용하는 도구이고, 최근 들어서는 EPP에 통합되고 있습니다. 이제는 EDR이라는 성공적 모델을 더욱 광범위한 엔터프라이즈 보안 에코시스템까지 확장하려고 합니다.

확장된 탐지 및 대응(XDR)의 정의

XDR은 새롭게 등장한 보안 제품 카테고리로, Gartner에서는 이를 일컬어 "여러 보안 제품을 하나의 일관적인 보안 관제 체제로 기본 통합한 SaaS 기반 공급업체별 보안 위협 탐지 및 인시던트 대응 도구"라고 정의합니다.

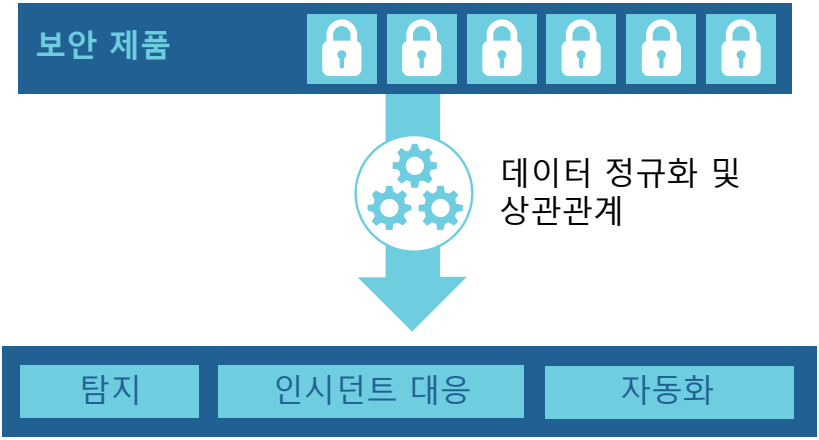


그림 4: XDR의 기본 기능

XDR의 기본 기능(**그림 4** 참조)은 다음을 하나로 통합합니다.

- 보안 에코시스템에서 데이터 수집 및 정규화
- 원격 측정 데이터의 상관관계를 액션 가능한 알림과 인시던트로 변환
- 각 보안 제품의 인시던트 대응 기능을 오케스트레이션 및 자동화

Gartner가 말하는 XDR의 장점은 다음과 같습니다.

- 보호, 탐지 및 대응 기능 향상
- 전반적인 운영 보안 인력의 생산성 향상
- 총소유비용(TCO)을 낮추어 효과적인 탐지 및 대응 기능 구성

XDR이 보안 정보 및 이벤트 관리(SIEM) 또는 보안 오케스트레이션, 자동화 및 대응(SOAR) 도구의 이름만 바꾼 새로운 유행어처럼 들릴 수도 있습니다. 유사한 기능이 많기는 하지만, XDR은 SIEM이나 SOAR와는 다릅니다.

제품 간 인시던트 탐지

이제 SecOps 팀은 그 어느 때보다 많은 센서와 원격 측정 데이터를 접하게 되었습니다. 문제는 나무만 보이고 전체 숲 형상을 볼 수가 없다는 것입니다. SecOps 팀은 그야말로 매일 수천 개의 알림에 시달리고, 그로 인한 노이즈 현상에 의해서 이미 외부 보안 기관에서 확정된 보안 침해 지표(IoC)와 매치되는 인시던트를 오랫동안 알아차리지 못하는 상황이 발생합니다.

XDR의 핵심 기능은 조직의 보안 영역에 있는 다양한 제품 및 도구 포트폴리오에서 제때 정확한 인시던트를 탐지하는 것입니다. 하지만 XDR은 SIEM, SOAR 도구와 달리 모든 보안 공급업체의 모든 도구를 통합하는 "무모한" 시도는 하지 않습니다. XDR은, SIEM과 SOAR 도구의 주요 이슈가 여러 보안 솔루션 공급업체의 이벤트를 심층적으로 통합하지 못하는 것이라는 인식에서 출발합니다. 그 대신 XDR은 기본적으로 하나의 보안 솔루션 공급업체 포트폴리오 내에서 네이티브 수준의 통합을 제공하는 데 초점을 맞춥니다. 이런 공급업체 통합 전략은 조직의 위험 대비 태세와 보안 관제를 개선하고 복잡성과 비용을 낮추려고 보안 공급업체를 통합하고자 하는 현재의 흐름과도 일치합니다.

공급업체 통합은 공급업체를 바꾸지 못할 우려가 있습니다. 공급업체의 보안 포트폴리오를 여러모로 신중하게 평가하여 보안 아키텍처에 필요한 기본 구성 요소, 비즈니스 요구 사항에 맞는 배포 및 라이선스 옵션을 제공하는지 확인한 다음, 공급업체를 선택한다면 이러한 위험을 완화시킬 수 있습니다. 또한 공급업체의 경험, 평판, 업계 리더십, 혁신에 대한 의지도 신중하게 고려해야 합니다.

보강, 분석 및 분류를 통한 인시던트 검증

첫 탐지가 끝나면 본격적인 작업이 시작됩니다. 인시던트의 성격, 범위, 단계, 영향을 평가해야 합니다. 적어도 XDR은 쇄도하는 알림 속에서 컨텍스트와 상관관계를 분석하여 조사 및 분류 프로세스를 지원하고, 적절한 완화 조치를 수행해야 합니다. 1장에서 설명한 사이버 보안 기술 부족 문제로 인해, 이런 프로세스를 오케스트레이션 할수록(또는 자동화할수록) 좋습니다. 인시던트 조사는 보안 업계에서 비교적 희귀한 전문 기술, 도구, 프로세스가 필요합니다. 예를 들어, 중요한 필수 기술은 다음과 같습니다.

- 멀웨어 헌팅/분석
- 리버스 엔지니어링
- 다수의 스크립팅 언어
- 포렌식
- 위협 행위자 전술, 전략 및 절차(TTP)
- 기타

인시던트 복구 업데이트를 통한 위협 억제, 복구 및 운영 재개

EDR 플랫폼이 보안 인시던트를 자동 복구하기 위해 조치를 하는 것처럼(예: 멀웨어에 감염된 파일 격리, 네트워크에서 일시적으로 기기 분리), XDR도 보안 인프라 전체에서 자동 억제, 복구 업데이트, 복구를 실행하고, 네트워크 일부에 대한 네트워크 액세스를 제한하고, 자격 증명을 철회하고, 클라우드 기반 애플리케이션 사용을 제한하고, 받은 편지함에서 메시지를 제거할 수 있습니다.

하지만 지금과 같이 수준 높은 여러 가지 엔터프라이즈 아키텍처만 중구난방으로 결합하여 구축된 환경에서는 말처럼 쉽지 않습니다. 제품, 관리 콘솔, 공급업체 언어별로 많은 추가 조치를 해야 합니다.

XDR 플랫폼은 조직 내 보안 아키텍처에서 다양한 유형의 보안 도구와 기기가 존재해야 할 필요성은 인정합니다. XDR은 보안 공급업체의 개별 솔루션에 부가가치를 더하고 이러한 시스템에 기본 통합을 제공해 다음과 같은 효과를 얻습니다.

- SecOps 팀에게 단일 창 관리 콘솔을 통해 상관 관계성이 표시된 조직 전체 뷰를 제공합니다.
- 잠재적 보안 인시던트를 식별 및 조사합니다.
- 인시던트 대응 기능을 조정해 즉각적으로 위협을 억제, 복구 업데이트 및 수정합니다.

3장

XDR에 대한 다양한 접근법

In Thi

- 개방형 vs. 폐쇄형 시스템
- 산업 표준의 중요성
- XDR 자동화의 힘

XDR이 비교적 새로운 개념이기는 하지만, 이미 여러 가지 방법이 등장했습니다. 예를 들어, 폐쇄형 시스템인지, 개방형 시스템인지, 자동화를 사용하는지, 오케스트레이션을 사용하는지 등의 기본 원리에 차이가 있습니다. 이런 차이는 양자택일보다는 제어하는 정도의 문제에 가까운데, 대부분의 XDR 솔루션은 영역별로 어느 한쪽에 조금 더 치우치는 형태입니다.

개방형 vs. 폐쇄형 시스템

XDR에서는 단일 공급업체 포트폴리오로 제한할지, 다양한 공급업체의 여러 보안 제품 대상으로 개방해야 할 것인지 가장 먼저 고려해야 합니다.

단일 공급업체가 제공하는 제품으로 제한하면 심층적 네이티브 통합에는 용이하고 기본적인 데이터 정규화 문제를 빠르게 해결할 수 있습니다. 그래서 탐지 기능을 개선하고 조사와 복구 업데이트 기능의 속도를 높이는 데 개발 노력을 집중할 수 있습니다. 하지만 폐쇄형 시스템을 위한 선택된 보안 공급업체는 조직에 필요한 다양한 솔루션을 공급할 만큼 광범위한 보안 제품 에코시스템을 갖추고 있어야 합니다.

반면, 개방형 시스템은 데이터 정규화 노력이 훨씬 더 많이 필요한데, 대개는 탐지와 조사 분야를 혁신하는 시간을 희생해야 하는 경우가 많습니다. 개방적 애플리케이션 프로그래밍 인터페이스(API)를 사용해서 통합할 수도 있지만, 대체로 기능이 제한됩니다. 개방형 시스템의 가장 큰 장점은 이미 상당 기간 투자된 현존 보안 제품을 활용할 수 있다는 것입니다.

개방형 시스템과 폐쇄형 시스템 중 어떤 것을 선택하든, 산업 표준과 투명성을 준수하는 XDR 솔루션과 공급업체를 선택해야 합니다. 예를 들어, 해당 공급업체가 참여하는 표준 단체 협회나 인증 여부를 확인하는 것입니다.

인증 요청

International Computer Security Association (ICSA) Labs: 미국 Verizon의 독립적인 사업부이며, 보안 및 의료 IT 제품, 네트워크 연결 기기의 객관적인 테스트 및 인증을 통해 제품 규정 준수, 안정성, 성능을 측정합니다. 자세한 내용은 https://icsalabs.com을 참조하십시오.

Virus Bulletin: 보안 소프트웨어 테스트를 전문으로 수행하는 세계적인 기관입니다. 정규 공개 테스트 보고서에서는 각종 안티 멀웨어 보호와 엔터프라이즈 수준 이메일 및 웹 보안 솔루션을 다룹니다. 자세한 내용은 https://virusbtn.com을 참조하십시오.

AV Comparatives: 체계적인 테스트를 통해 보안 소프트웨어(예: PC/Mac 기반 안티바이러스 제품, 모바일 보안 솔루션)가 주장하는 대로의 기능을 제공하는지 검사하는 독립적인 기관입니다. AV Comparatives의 인증은 국제적으로 인정되는 소프트웨어 성능의 공식적 승인과 같은 효력이 있습니다. 자세한 내용은 https:// www.av-comparatives.org를 참조하십시오.

U.S. DODIN APL(Department of Defense Information Network Approved Products List): 사이버 보안(CS) 및 상호운용성(IO) 인증을 완료한 제품의 통합적 목록입니다. 자세한 내용은 https://aplits.disa.mil/process-APList.action을 참조하십시오.

Federal Information Processing Standard(FIPS) 140-2: FIPS는 미국과 캐나다 정부가 공동으로 운영하는 암호화 검증 프로그램입니다. 자세한 내용은 https://csrc.nist.gov/publications/detail/fips/140/2/final을 참조하십시오.

공통 기준: International Organization for Standardization(ISO) 및 International Electrotechnical Commission(IEC) 표준(ISO/IEC 15408)은 17개 인증 국가에서 운영하고, 31개 국가 정부에서 IT/네트워크 인프라 구매 요구 사항으로 활용합니다. 자세한 내용은 https://www.cyber.gc.ca/en/common-criteria 및 https://www.niap-ccevs.org/를 참조하십시오.

MITRE ATT&CK: 실제 보안 침해 사건에서 조사된 정보를 바탕으로 한 공격 전술과 기술에 관한 지식 DB 자료입니다. 자세한 내용은 https://attack.mitre.org를 참조하십시오.

자동화 및 오케스트레이션

XDR의 접근법에서 두 번째 차이는 솔루션에서 오케스트레이션(지침)과 자동화(조치)를 활용하는 정도에 있습니다.

대부분 XDR 솔루션은 보안 팀에게 권장 조치를 제공(또는 각 조직이 추천하도록 허용)하여 기존 SecOps 팀을 보조하는 도구로 활용하는 것이 가장 기본입니다. 적어도 대부분 XDR 솔루션은 보안 분석가에게 상관관계가 파악된 보안 정보를 제공하고 기본적인 수동 작업을 자동화하는 수준의 기능은 갖추었지만, 여전히 보안 운영 인력의 전문성과 조사 및 대응을 결정하기 위한 조치가 필요합니다.

좀 더 고도화된 XDR 접근 방법은 다양한 수준의 자동화를 추가합니다. 이는 간단한 사전 정의 조치(예: Virus Total과 같이 위협 인텔리전스 검사, 방화벽 차단 리스트에 IP 주소 추가)에서부터 각 인시던트 유형을 지능적으로 조사한 결과를 완벽히 반영한 일련의 지능적 조치에 이르기까지 여러 가지가 있습니다. 고도화된 접근 방법을 통해서 보안 팀의 해석 범위를 넓혀 탐지 능력을 증가시켜주는 도구로 활용할 수 있습니다.

XDR 솔루션의 접근법을 이해하는 것 외에도 오케스트레이션과 자동화된 요소를 XDR 공급업체가 지속적으로 관리하는지, 조직에서 관리해야 하는지도 고려해야 합니다. 조직마다 오케스트레이션, 자동화의 기능과 원하는 수준이 다르기 때문입니다.

인력 문제와 기술 요구 사항을 해결하지 않고 더 많은 정보를 수집하고 조사해야 할 이벤트가 늘어나기만 한다면 SecOps 팀의 부담만 커집니다. 인력과 기술이 한정되어 있다면 광범위하게 자동화를 사용하는 것이 좋습니다.

4장

우리 조직에 적합한 XDR은?

요약:

- XDR 준비 상태 평가

XDR이 무엇이고, 어떻게 현대적 보안 문제와 위협을 해결하는지 이해했다면 이제 자신의 조직에 알맞은 XDR을 도입할 수 있는지 궁금해 하실 것 입니다. 현재 보안 팀 구성, 조직 구조, 기능, 업무 프로세스에 대한 몇 가지 질문에 답하면 결정을 내리는 데 도움이 됩니다. 그런 후에 본인 조직에 어떤 XDR 솔루션이 가장 알맞을지 결정할 수 있습니다.

보안 알림을 모니터링하는 전담팀이 있습니까?

강력한 예방 전략을 세웠더라도, 인시던트 모니터링 환경을 파악하는 것이 중요합니다. 가장 기본적으로 보안 알림을 모니터링하고, 이벤트를 알아채고 대응하는 훈련을 받고, 적절히 모니터링을 할 수 있을 만큼 시간 여유가 있는 전담팀(적어도 여러 업무 책임을 맡은 전담 담당자 선정)이 필요합니다. 헬프 데스크나 네트워킹 팀에 보안 모니터링을 부수적인 책임으로 맡기는 방법으로는 오늘날의 지능적인 위협에 대응할 수 없습니다.

전담 보안 팀 외에도 업무 환경에 존재하는 다양한 소스에서 원격으로 측정 데이터를 수집할 수 있는 최소한의 기본 도구가 필요합니다. 적어도 네트워크 방화벽, 침입 방지 시스템, 이메일 보안, 엔드포인트 보호, 서버 및 애플리케이션 로그가 포함되어야 합니다. SIEM은 좋은 시작점이기는 하지만 많은 조직에서 오랫동안 사용해본 결과, 이 솔루션만으로는 충분하지 않다는 것이 확인되었습니다. 보안 팀이 이벤트의 상관관계를 파악하고 시기적절하고 효과적으로 대응에 나서 위협을 억제 및 복구 업데이트하는 데 도움이 되는 도구가 필요합니다.

지속적 모니터링을 할 인력이 없거나 부족한 조직에는 XDR이 이상적 솔루션입니다. 지금까지 설명한 대부분 사용 사례에서는 SOC 팀이 부족한 인력으로 과중한 업무에 시달리며 보안 아키텍처의 복잡성을 해결해야 했지만, 이제 혼란스러운 상황과 씨름할 필요가 없습니다.

잠재적 인시던트를 조사할 전문성과 시간이 있습니까?

SIEM으로 알림을 모니터링할 인력이 있다해도 잠재적 인시던트를 조사할 시간과 전문성을 보유하고 있습니까? 엔터프라이즈 환경의 수많은 이벤트 소스에서 데이터가 넘쳐나는 데다 보안 위협 수가 늘어나고 그 형태가 지능화되면서 알림 과부하는 SecOps 팀의 골칫거리로 떠올랐습니다. 이 경우에는 SecOps 팀이 IoC와 공격자의 최신 전술, 기술 및 절차(TTP)를 알아볼 수 있는 기본 전문 지식과 지속적인 경계, 학습이 필요합니다.

이런 문제를 완벽히 해결할 만큼 보안 전문가를 충분히 두고 있는 조직은 매우 드뭅니다. XDR을 통해서 알림 과부하 이슈를 해결함으로써, 보안 분석가가 인시던트의 상관관계를 자동으로 파악하여 인시던트를 탐지하고 대응조치를 취할 수 있도록 합니다.

조직에 알맞은 대응 프로세스가 명확하게 마련되어 있습니까?

잠재적 보안 인시던트가 일어날 때마다 즉흥적으로 대응하는 방법은 권고하지 않습니다. 오늘날 사이버 공격은 속도가 빠르고 지능화되었기 때문에 위협을 신속히 억제하여 조사하고, 이에 대응할 방안을 미리 마련해두는 것이 중요합니다. 어떤 보안 위기이든 명확한 해결 절차가 중요하고 사이버 보안 인시던트도 예외는 아닙니다.

하지만 일률적인 프로세스를 한번 설정해 놓는 것만으로는 충분하지 않습니다. 인시던트 대응 프로세스는 위협이 진화할 때마다 지속적으로 업데이트해야 합니다. 그렇지 않으면 보안 위협의 변화에 뒤처져서 효과가 없습니다. XDR 플랫폼은 공급업체, 위협 조사 팀, 대응 전담 담당자가 협업하여 보안 위협 동향과 위협이 최종 사용자 조직에 미치는 형태와 관련된 이벤트를 추적하고, 축적된 과거 지식과 보안 기술 전문성을 통합해 대응 프로세스가 장기적으로 지속적인 효과를 유지하도록 수정합니다.

보안 인력이 경영진이 원하는 가치 높은 역할에 시간을 사용하고 있습니까?

평범한 조직의 보안 팀이라면 사건이 생긴 뒤에 대응하는 과정을 반복하며 알림의 홍수 속에서 진짜 위협을 찾아내는 데 허덕이고, 최선의 노력으로 빠르게 인시던트에 대응해서 피해를 줄이고 정상 운영을 회복하는 과정을 반복합니다.

XDR 솔루션이 부담이 큰 작업(예: 이벤트 상관관계 파악, 원격 측정 데이터 분석, 인시던트 조사, 위협 억제, 인시던트 대응)을 해결해준다면, 보안 팀은 가치가 높은 활동(예: 보안 조사 및 계획, 위협 헌팅, 레드 팀/블루 팀 연습, DevSecOps)에 집중해야 할 시간 여유가 생겨서 조직 보안을 최대한 보장하는 데 노력을 기울일 수 있습니다.

5장

가장 적합한 XDR을 찾는 방법

요약:

- 적절한 솔루션 선택
- XDR 체크리스트

조직에 가장 알맞은 XDR 솔루션은 무엇입니까?

자신의 조직에 적합한 XDR 솔루션을 찾으려면 다양한 옵션을 평가하면서 몇 가지 중요한 질문에 대한 답을 생각해보는 것이 좋습니다.

XDR 솔루션에서 어떤 공격 벡터가 얼마나 많이 커버됩니까?

XDR 솔루션에서 커버되지 않는 공격 벡터는 사이버 범죄자에게 악용되기만을 기다리는 구멍입니다. 중요한 공격 벡터가 포함되지 않았다면 포인트 제품을 통합하거나 독립적으로 운영해야 할 수도 있습니다. 다음의 공격 벡터가 조직에 얼마나 위험한지 평가하고 조직의 요구 사항과 XDR 솔루션의 기능을 비교해보십시오.

- 회사 및 개인 소유 데스크톱 PC, 노트북, 모바일 기기 등 (관리형 및 비관리형) 사용자 엔드포인트

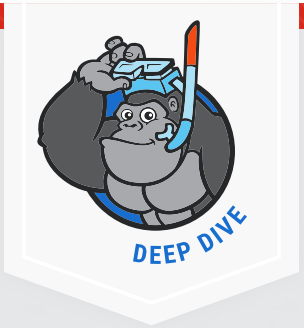
- 운영 기술(OT)(예: 헤드리스 IoT, 산업용 IoT 기기)
- 네트워크 액세스 (유무선)
- 자격 증명 및 액세스 관리
- 네트워크(재택, 지점 사무소 및 본사)
- 클라우드(퍼블릭, 프라이빗, SaaS)
- 이메일 시스템
- 웹 애플리케이션

XDR 솔루션에서 사이버 킬 체인이 얼마나 많이 커버됩니까?

Lockheed Martin의 Cyber Kill Chain® 모델(MITRE ATT&CK 프레임워크와 유사)에서는 공격자가 표적에서 목표를 달성하는 데 필요한 7단계(그림 5 참조)를 설명합니다.

공격자는 각 단계를 완료해야 표적을 공격할 수 있습니다. 사이버 킬 체인에서 한 단계만 깨트려도 공격이 차단됩니다. 조직에 얼마나 강력한 보안 태세(및 체인을 깨트릴 기회)가 필요한지 생각한 다음, XDR 솔루션을 적용할 단계를 평가하십시오. 많은 단계에 적용할수록 사이버 보안 침해를 예방할 가능성이 커집니다.

사이버 킬 체인



정찰 단계: 공격의 첫 단계로 목표하는 피해자에 대한 정보를 수집합니다. 주로 소셜 엔지니어링 기술, 이메일 주소 및 화상 회의 정보 수집, 네트워크 및 포트 스캔 등이 포함됩니다.

그림 5: Lockheed Martin Cyber Kill Chain®

무기화: 공격자가 IT 인프라 환경의 취약성을 알아내면, 백도어를 통해서 피해자에게 전송할 알려진 익스플로잇을 페이로드로 작성합니다.

전달: 표적이 된 피해자는 무기화된 페이로드를 받습니다. 일반적으로 이메일(예: 피싱 사기), 웹(예: 악성 웹사이트, 드라이브 바이 다운로드), 채팅, USB 기기 등의 수단을 사용합니다.

익스플로잇: 무기화된 페이로드는 피해자의 시스템에 코드를 실행하고 공격자가 정찰 중에 찾아낸 취약점으로 익스플로잇 합니다.

설치: 침입한 시스템에 멀웨어를 심은 다음, 공격자의 흔적을 덮습니다.

명령 및 제어(C2): 공격자가 공격 인프라(예: 봇넷)와 통신하는 C2 채널을 설정합니다. 공격자는 필요에 따라 공격을 수정하고, 네트워크에서 수평으로 이동해 다른 시스템과 기기에 침입할 수 있게 됩니다.

목표 달성: 공격자가 공격 목표(예: 데이터 유출, 데이터 조작/파괴, 서비스 거부)를 실행하거나 2차 표적에 공격을 시작합니다.

XDR 솔루션 구성 요소가 얼마나 효과적입니까?

공격면이나 공격 단계를 차단하는 기능을 사용하는 것만으로는 보호 효과를 보장할 수 없습니다. 보안 효과는 기술, 제품, 공급업체마다 큰 차이가 있습니다. 보안 효과를 정기적으로 평가하는 권위 있는 독립적 테스트 및 인증 기관은 여러 곳이 있습니다.

권위 있는 독립적 기관(예: AV Comparatives, SE Labs, Virus Bulletin, ICSA Labs)을 통해서, 원격 측정 데이터를 제공하고 대응 조치를 실행하는 제품이 XDR 솔루션과 상호 기능 연동 테스트를 받았는지, 그리고 정기적으로 지속적인 보안 효과 우수성 검증이 수행되었는지 확인하십시오.

또한, 여러 기능이 통합된 하나의 XDR을 운영하는 효과와 업계 최고의 단독형 보안 솔루션을 여러 개 운영하는 효과 중 어느 것이 더 나을지에 대해서도 함께 평가해 보십시오.

직원이 얼마나 편리하게 XDR 솔루션을 사용할 수 있습니까?

모든 조직의 보안 팀은 규모, 구조, 기술 세트, 프로세스 안정화 수준이 저마다 다릅니다. 앞서 설명하였듯이, 각 XDR 솔루션은 다양한 수준의 통합, 오케스트레이션, 자동화를 제공합니다. (기존 SIEM처럼) 간단하게 보안 정보의 상관관계를 파악하고 (SOAR처럼) 오케스트레이션 프레임워크를 제공하는 XDR 솔루션을 경험이 풍부한 인력과 기존 프로세스를 보조하는 도구로 사용할지, 상관관계, 탐지, 조사 및 대응 기능을 완전히 자동화하여 바로 사용할지 고려해보십시오.

XDR 평가 체크리스트

- ☐ XDR 솔루션에서 어떤 공격 벡터가 얼마나 많이 커버됩니까?
- ☐ XDR 솔루션에서 어떤 사이버 킬 체인이 얼마나 많이 커버됩니까?
- ☐ XDR 솔루션 구성 요소가 얼마나 효과적입니까?
- ☐ 직원이 얼마나 편리하게 XDR 솔루션을 사용할 수 있습니까?
- ☐ XDR 솔루션이 하나의 공급업체에 종속됩니까? 아니면 개방되어 있습니까?, 혼합되어 있습니까?

XDR 솔루션이 하나의 공급업체에 종속됩니까? 아니면 개방되어 있습니까?, 혼합되어 있습니까?

특정 벤더에 특화된 XDR 솔루션은 일반적으로 통합 기능은 우수하지만, 공급업체 솔루션 포트폴리오에서 해당 벤더의 보안 제품을 선택해야 합니다. 개방형 XDR 시스템은 효과적인 것 같지만, 데이터를 정규화하고 상관관계를 파악하는 데만 지속적인 엔지니어링 노력이 많이 필요한 경우가 많아서 시간이 지나면서 탐지와 조사 기능이 부족해집니다. 자동화를 확대하는 대신 공급업체 포트폴리오를 한정해도 괜찮은지 생각해보고, 동일한 공급업체 또는 소수의 공급업체에서 사용 중인 구성 요소가 얼마나 있는지 고려해보십시오.

포티넷은 수년 전부터 각 조직들이 확대되는 공격면을 커버하는 데 어려움을 겪고 있고, 보안 위협이 가속화되고, 인프라가 복잡해지며, 규제 환경도 확장되고 있다는 것을 인지하고 있었습니다. 포티넷은 이러한 문제를 해결하기 위해 보안 및 네트워킹 제품 포트폴리오를 매끄러운 보안 패브릭으로 원활하게 연결하는 작업을 시작했습니다. FortiGuard Labs의 위협 인텔리전스로 보호되는 보안 패브릭은 확장성, 통합성, 자동화를 제공하고 조직의 다른 전략적 기술 공급업체에 개방되도록 설계했습니다.

6장

포티넷 솔루션

요약:

- 포티넷 보안 패브릭
- FortiXDR 소개
- 포티넷의 장점

포티넷 보안 패브릭

현재 포티넷 보안 패브릭(그림 6 참조)은 XDR 솔루션의 기반으로 자연스럽게 자리 잡았고, 다음과 같은 요소로 구성됩니다.

- **제로 트러스트 네트워크 액세스(ZTNA)**, 네트워크 안팎에서 사용자와 기기를 식별하여 보호.
- **보안 중심 네트워크**, 네트워크 및 사용자 환경을 보호하고 가속화.
- **민첩한 클라우드 보안**, 클라우드 인프라 및 애플리케이션을 보호하고 제어.
- **AI 기반 보안관제**, 사이버 위협을 자동 예방, 탐지하고 이에 대응.
- **패브릭 관리 센터**, 단일 윈도우 사용자 인터페이스를 통한 가시성 및 제어 제공.
- **패브릭 커넥터 및 API**, 자동화 대상을 타사 보안 솔루션 구성 요소로 확장.

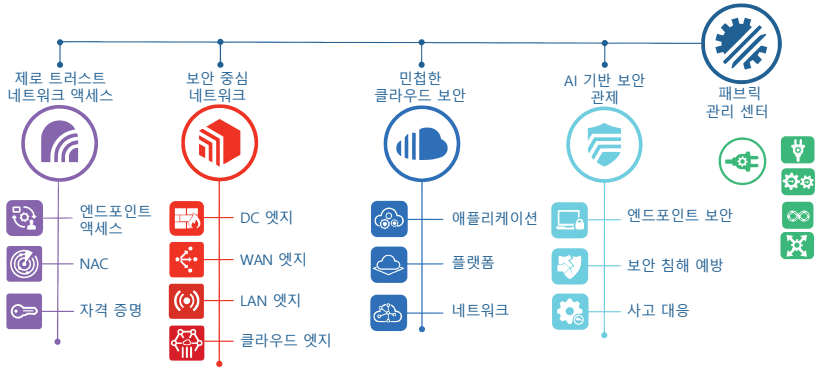
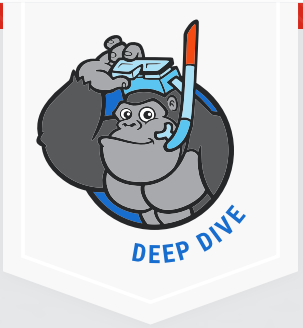


그림 6: 포티넷 XDR 솔루션 서비스의 기반이 되는 포티넷 보안 패브릭.

FortiXDR에 정보 공급



네트워크 보안

FortiGate 차세대 방화벽은 보안 중심 네트워크를 지원하며, 하이브리드 클라우드, 하이퍼스케일 데이터 센터 환경 등의 모든 유즈 케이스 사례에 이상적입니다. 최신 네트워크 프로세서와 콘텐츠 프로세서 기술을 비롯한 특수 설계된 보안 처리 장치(SPU)가 내장된 FortiGate NGFW는 독보적인 고성능과 소형/중형/대형 규모로 규모가 아주 작은 곳에서 넓은 곳까지 모두 트래픽을 검사합니다. 포티넷 NGFW는 독립적인 타사 테스트에서 꾸준히 높은 순위를 차지하였고(자세한 내용: https://www.fortinet.com/kr/corporate/about-us/product-certifications), Gartner 엔터프라이즈 방화벽 및 WAN 엣지 부문 매직 쿼드런트에서 리더로 선정되었습니다.

이메일 보안

보안 이메일 게이트웨이는 가장 큰 공격 벡터인 이메일에 대한 1차 방어 수단을 제공합니다. FortiMail은 업계 최고의 보안 이메일 게이트웨이 솔루션으로, 수신되는 이메일 트래픽에서 위협을 찾아내 차단하고 데이터 손실 방지(DLP) 및 규정 준수 정책을 발송하는 이메일 트래픽에 적용합니다. FortiGuard Labs의 위협 인텔리전스를 최대로 활용할 뿐만 아니라, ICSA Labs와 SE Labs의 독립적인 타사 테스트에서 꾸준히 높은 순위를 차지하고 있습니다.

웹 애플리케이션 보안

FortiWeb은 웹 애플리케이션과 API를 대상으로 하는 포괄적인 위협 보호를 제공합니다(예: 머신 러닝 모델을 적용하여 기존의 지속적 튜닝 업무 부담 완화). Amazon Web Services(AWS), Google Cloud Platform(GCP) 또는 Microsoft Azure 퍼블릭 클라우드 리전에서 클라우드 네이티브 서비스로 제공되는 FortiWeb은, 애플리케이션과 WAF 사이의 트래픽을 위한 낮은 지연 속도와 리전 간 대역폭 속도라는 장점을 이용할 수 있습니다. 또한, 하드웨어 어플라이언스와 가상 머신 어플라이언스 형태로도 제공됩니다.

엔드포인트 보안

FortiEDR은 포티넷의 주력 엔터프라이즈 엔드포인트 보호 플랫폼입니다. 실행 전/후 보호는 물론이고, 운영 체제 버전을 가리지 않고 워크스테이션과 서버, POS, 제조, 운영 기술 시스템을 대부분 기기에 적합하게 오케스트레이션된 인시던트 대응을 제공합니다. 기기가 작동하는 상태에서 특정 악성 활동을 제거하는 고유한 기능 덕분에 조직과 데이터를 보호하면서도 생산성과 가용성을 유지할 수 있습니다. FortiEDR의 효과는 다양한 독립적 시험 기관에서도 검증되었습니다. 또한, FortiEDR은 포티넷 보안 패브릭을 활용하여 FortiGate, FortiNAC, FortiSandbox, FortiSIEM과 통합하고 클라우드, 온프레미스, 에어-갭 환경에 배포하거나 하이브리드 형식으로 배포할 수 있습니다.

클라우드 보안

FortiCWP은 포티넷의 클라우드 네이티브 클라우드 워크로드 보호(CWP) 서비스로, 포티넷 보안 패브릭과 긴밀히 통합되어 통합 클라우드 사용 관리와 보고 기능을 제공합니다. FortiCWP는 클라우드 공급업체(AWS, GCP, Microsoft Azure)가 제공하는 API를 통해 인프라 구성, 사용자 활동, 트래픽 플로우 로그 등의 모든 보안 구성 요소를 모니터링하고 추적합니다. 또한 FortiCWP는 클라우드 데이터 저장 공간을 스캔하여 중요한 콘텐츠나 악성 콘텐츠가 있는지 검사하고 자사 환경이 보편적인 규정 표준을 준수하는지 보고서를 작성합니다.

FortiCASB는 포티넷에서 개발한 클라우드 네이티브 클라우드 액세스 보안 브로커(CASB) 구독 서비스로, 기업에서 사용하는 클라우드 기반 서비스에 가시성, 규정 준수 여부, 데이터 보안, 위협 보호를 제공하도록 설계된 다양한 클라우드 보안 태세 관리(CSPM) 기능이 제공됩니다.

FortiCASB는 주요 SaaS 애플리케이션에 저장된 사용자, 동작, 데이터에 대한 정책 기반 통찰력과 포괄적인 보고 도구를 제공합니다.

샌드박스 분석

FortiSandbox는 포티넷 보안 패브릭과 기본적으로 통합되고 보안 침해 보호 전략을 자동화합니다. 이 제로 터치 자동화 모델은 동적인 서로 다른 국가와 시간대에 걸친 인텔리전스 공유와 보호에 이상적입니다. 의심스럽거나 위험한 파일을 먼저 분석하고 FortiSandbox의 AI 기반 통계 분석 기능으로 알려진 멀웨어와 새로운 멀웨어를 신속히 찾아냅니다. 2단계 동적 분석은 격리된 환경에서 동작 기반 AI로 완전한 공격 수명 주기를 찾아냅니다. 이 AI는 새로운 멀웨어 기술을 끊임없이 학습하고 멀웨어 동작에 자동으로 적응합니다. FortiSandbox는 악성 코드가 발견되면 위험 등급을 반환하고, 위협 인텔리전스를 공유하며, 포티넷 보안 패브릭의 위협 완화 프로세스를 자동화합니다.

사용자 및 엔티티 동작 분석(UEBA)

FortiInsight는 포티넷의 UEBA 솔루션으로, 자동 탐지 및 대응 기능을 사용하여 사용자와 엔드포인트를 지속적으로 모니터링하고 내부자 위협으로부터 조직을 보호합니다. 머신 러닝과 지능적 분석을 활용하는 포티넷은 규정에 어긋나거나, 수상하거나, 비정상적인 동작을 자동으로 찾아내 대응 담당자에게 신속히 알립니다. 이런 선제적 위협 탐지 방식은 사용자가 회사 네트워크에 연결되었는지 여부와 관계없이 한 겹의 보호와 가시성을 추가로 제공합니다.

네트워크 액세스 제어

FortiNAC은 네트워크에 연결된 모든 자산에 대한 가시성, 제어 및 자동 대응을 제공합니다. FortiNAC는 여러 자산 정보 및 동작 소스를 사용하여 자세한 기기 프로파일링(헤드리스 기기 포함)을 제공하고 네트워크에 있는 기기를 정확히 찾아냅니다. IoT 위협에 대한 보호를 제공하고, 타사 장치까지 제어를 확장하며, 다양한 네트워킹 이벤트에 대한 자동 대응 정책을 수행합니다.

LAN 엣지

FortiSwitch 보안 액세스 스위치는 보안, 성능, 관리 기능을 LAN 엣지에 제공합니다. FortiLink 관리 프로토콜을 통해 포티넷 보안 패브릭과 긴밀히 통합된 FortiSwitch는 FortiGate를 통해서 직접 관리할 수 있습니다. 이 단일 창 관리 콘솔은 연결 방식과 관계없이 네트워크상의 사용자와 기기에 대한 모든 정보를 확인할 수 있고 제어가 가능합니다. FortiSwitch는 데스크톱에서 데이터 센터에 이르기까지 다양한 애플리케이션을 사용하는 SD-Branch 배포에 이상적이며, 기업들은 이를 통해 보안과 네트워크 액세스를 융합할 수 있습니다.

FortiAP은 캠퍼스에서 지점 무선 배포까지 LAN 엣지를 보호하는 데 이상적입니다. FortiAP 액세스 포인트는 FortiGate 보안 어플라이언스의 통합 무선 LAN(WLAN) 컨트롤러 또는 FortiAP Cloud 프로비저닝 및 관리 포털을 통해 한 곳에서 관리됩니다. 포티넷의 보안 패브릭을 사용하면 단일 창 관리 콘솔에서 유무선 보안을 간편하게 관리할 수 있습니다.

AI 기반 확장된 탐지 및 대응

FortiXDR은 포티넷 보안 패브릭 전체 솔루션과 연동되어 인시던트 탐지, 조사, 대응을 완전히 자동화합니다. 포티넷에서 연동한 안정적인 분석 도구 세트를 포티넷 보안 패브릭 구성 요소에서 집계 및 정규화되고 상관관계를 찾은 보안 정보에 적용한 후, 잠재적 보안 인시던트를 탐지합니다.

AI 기반 의사 결정 엔진은 초기 탐지 유형에 따라 자동 조사 프로세스를 동적으로 따라가면서 사람이 수행하던 보안 분석가의 통상적이고 전문적인 조치 내용을 그대로 모방합니다. 이 AI 기반 의사 결정 엔진은 보강과 추가적 분석을 제공하는 다양한 마이크로서비스를 호출합니다. 예를 들어, FortiGuard Labs와 타사의 위협 인텔리전스, 파일 분석(예: 통계적 Yara 규칙), 동적 샌드박스 평가, 커뮤니티 평판, 사용자 행동 기준 등이 포함됩니다.

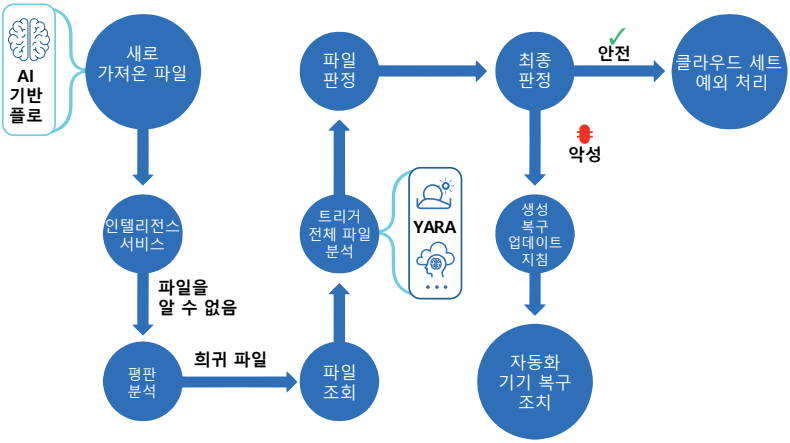


그림 7: FortiXDR AI 기반 조사 플로 결정 엔진

그림 7은 포티넷의 AI 기반 조사 및 마이크로서비스 워크플로의 예시입니다.

자동화된 대응

탐지되지 않은 상태로 IT 시스템 내부에 침투해 조직에 피해를 주는 보안 위협을 탐지하고 조사하는 것이 중요한 기능이기는 하지만, 위협 억제 및 제거 작업이 수행되기 전에는 이러한 보안 기능은 완료될 수 없습니다.

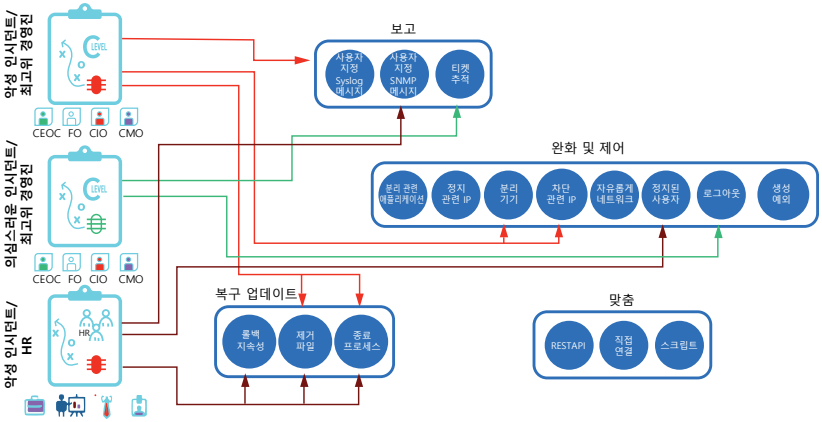


그림 8: FortiXDR 자동화 대응 프레임워크

조직은 식별자, 사용자 그룹, 위험 노출 등의 기준에 따라 취할 조치를 미리 지정하는 정책을 설정할 수 있습니다. (그림 8 참조). 따라서 최종적 복구 속도와 대응 속도가 빨라지고, 공격자가 IT 시스템에 머물 수 있는 시간과 그 과정에서 일으키는 피해가 줄어듭니다.

근본적으로 다른 전략

오늘날 보안 위협 동향의 횟수, 지능화 수준, 전파 속도가 높아지고 있어 보안 팀은 사이버 보안 인력과 기술 공급이 부족한 시기에 그 어느 때보다 힘든 어려움에 처해있습니다. 관리해야 할 업계 대표적인 포인트 제품들이 너무 많고, 분석할 보안 정보가 넘쳐나고, 조사해야 할 잠재적 인시던트까지 수행하기 어려워지면서 보안에 접근하는 방식에 근본적인 변화가 필요합니다.

요즘 많은 조직이 보안 아키텍처와 운영에서 복잡성을 제거하는 방법으로 보안 공급업체의 통합을 꾀하고 있습니다. 더불어 XDR과 같은 새로운 솔루션이 이런 문제를 해결할 잠재력이 매우 큽니다.

FortiXDR은 탐지, 조사, 대응을 완전히 자동화하는 독특한 방식을 취합니다. 데이터 침해나 랜섬웨어 인시던트가 일어나기 전에 현재 진행 중인 사이버 공격을 찾아낼 가능성도 커집니다. FortiXDR은 보안 팀의 부담을 완화하고 조직을 보호하는 데 더욱 중요한 전략적 활동에 참여할 기술과 도구를 제공합니다. FortiXDR, 포티넷 보안 패브릭, 포티넷 보안 솔루션 전체 포트폴리오에 대한 자세한 내용은 https://fortinet.com을 참조하십시오.

시대에 앞서 나가기

이 고릴라 가이드에서 보안 관제 프로세스에 XDR을 추가하는 것이 얼마나 중요한지 살펴보았습니다. XDR을 통해서, 보안 위협 트렌드에 맞서는 보안 접근 방식의 변화를 도모할 수 있고, 기존보다 빠르게 보안 위협을 찾아서 처리할 수 있도록 도와줍니다.

이러한 변화를 통해서 새로운 보안 위협에 대응할 수 있다는 자신감과 마음의 평화를 찾을 수 있을 것입니다. 사이버 공격은 앞으로도 끊임없이 발생하겠지만 적절한 안전장치를 마련한다면 중요한 비즈니스 자산을 오랫동안 안전하게 보호할 수 있습니다.

읽어주셔서 감사합니다. 건강 조심하시기 바랍니다!

FORTINET 정보

포티넷(NASDAQ: FTNT)은 전 세계 최대 규모의 대기업, 서비스 제공업체 및 정부 산하 기관 등의 사이버 보안을 책임집니다. 포티넷은 공격 면을 지능적인 방식으로 원활히 보호하며 현재는 물론, 미래의 경계 없는 네트워크에 대한 점차 커지는 성능 요구사항을 충족하고 있습니다. 오직 포티넷 보안 패브릭 아키텍처만이 네트워크 어느 곳이든, 애플리케이션, 클라우드, 모바일 환경에 상관없이 '허점 없는 보안'을 제공함으로써 가장 중요한 보안 과제를 충족시킬 수 있습니다. 포티넷은 가장 많은 보안 어플라이언스를 출하한 전 세계 출하량 1위 업체로 선정된 바 있고 전 세계 450,000명 이상의 고객이 비즈니스 보안을 위해서 포티넷을 신뢰합니다.

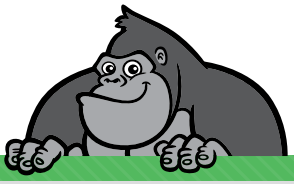
ACTUALTECH MEDIA 정보

ActualTech Media

ActualTech Media는 혁신적인 잠재 고객 생성 프로그램과 매력적인 맞춤형 콘텐츠 서비스로 엔터프라이즈 IT 공급업체와 IT 구매자를 연결해주는 B2B 기술 마케팅 기업입니다.

ActualTech Media 팀은 엔터프라이즈 IT 업계에 있었기 때문에 엔터프라이즈 IT 업계를 대상으로 마케팅합니다.

ActualTech Media의 경영진은 전 CIO, IT 관리자, 아키텍트, 보안 전문가, 마케팅 전문가로 구성되어 있으며, 고객이 기술의 기능을 설명하는 시간을 단축하고 성과를 높이는 전략을 세우는 데 더욱 집중할 수 있습니다.



IT 마케터이거나 회사를 위해 Gorilla Guide® 책자를 제작하고 싶다면 https://www.gorilla.guide/custom-solutions/를 방문하십시오.