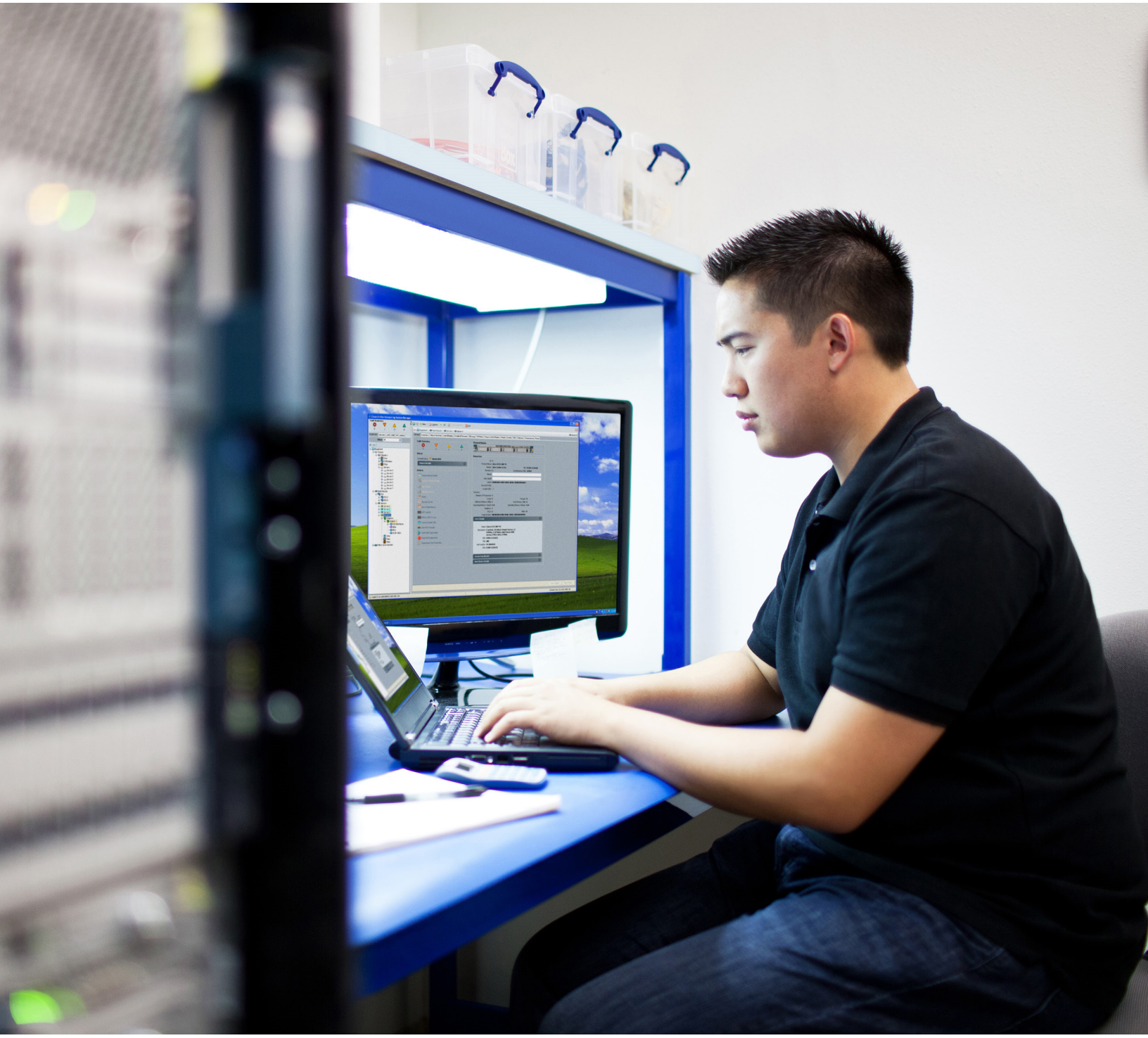
Security Analytics and More

효과적인 사고 대응 계획 준비



주요 내용

이 백서에서 IT 및 보안 팀원은 다음과 같은 효과적인 사고 대응 계획의 필수 구성 요소에 대해 알아볼 수 있습니다.

- 현재 사고 대응 계획이 기대에 못 미치는 이유 파악
- 올바른 사고 대응 팀과 협력
- 성공적인 대응 절차 개발
- 적절한 보안 기술 선택
- NetFlow 및 보안 분석을 통해 사고 대응 및 포렌식을 크게 개선

공격 증가

대규모 소매 업체에서 의료 서비스 공급업체 및 정부 기관에 이르기까지 오늘날의 정교한 표적 사이버 공격으로부터 안전한 곳은 없습니다. 공격자의 표적이 금융 데이터든, 영업 기밀이든, 기밀 정보든 간에 진화하는 위협 환경과 빠르게 증가하고 있는 네트워크 환경은 공격자가 침입할 수 있는 더 많은 경로를 제공하고 있습니다.

이제 공격자의 네트워크 침입 여부 보다는 '언제' 침입하는지가 문제입니다. 공격자들은 제로 데이 공격, 가로챈 액세스 크리덴셜, 감염된 모바일 디바이스, 취약한 비즈니스 파트너 또는 기타 전술을 사용합니다.

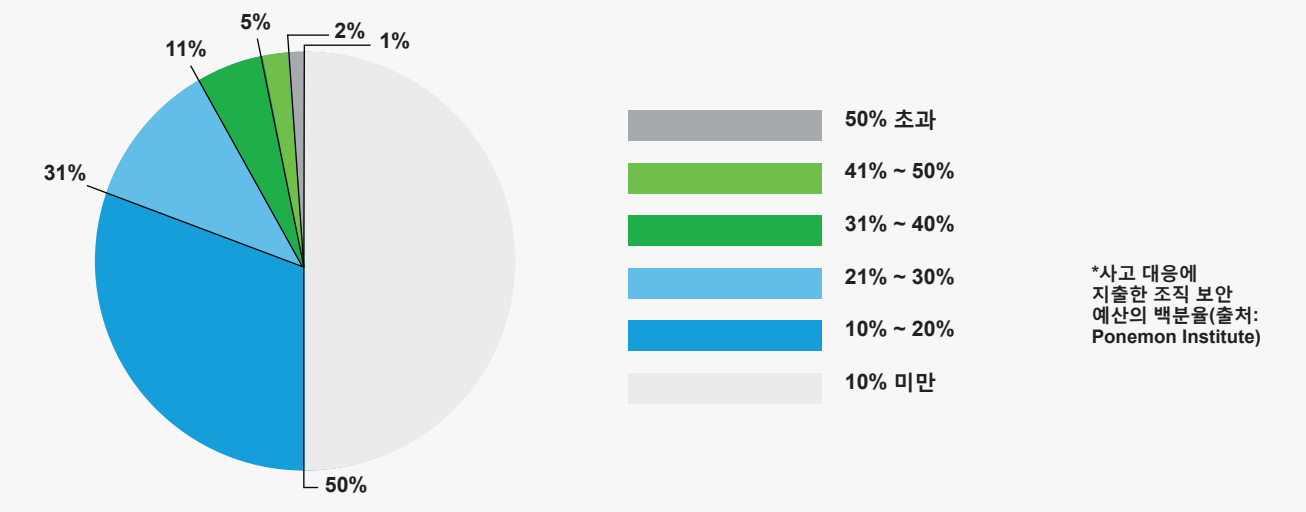
성공적인 보안이란 네트워크에서 위협을 제거하는 것에만 국한되지 않습니다. 오히려 공격이 발생할 때 이에 신속하게 대응하고 이를 무력화하는 것을 의미합니다.

Gartner에 따르면, "조직은 조기 보안 침해 탐지에 실패하고 있으며, 보안 침해를 당한 조직은 보안 침해의 92% 이상을 탐지하지 못하고 있습니다."[1] 조직을 보호하기 위해 더욱 적극적인 역할을 해야 한다는 점이 분명합니다. 인프라 내부에서 어떤 일이 일어나고 있는지 지속적으로 모니터링하고 공격자가 네트워크 및 평판을 심각하게 훼손하기 전에 확실한 주기적 대응 수단을 마련해야 합니다.

사고 대응의 단점

Ponemon Institute에서 실시한 설문 조사에서 대부분의 응답자는 조직이 향후 보안 침해를 완화하기 위해 할 수 있는 최선책은 사고 대응 기능을 개선하는 것이라는 점에 동의했습니다. 그러나 당시에 응답자의 절반은 사고 대응에 대한 지출이 전체 정보 보안 예산(그림 1)의 10%에도 미치지 못했다는 사실을 언급했습니다.[2] 다른 설문 조사에 따르면, 대기업의 90%는 1년 내내 중대한 IT 사고를 경험했지만 절반 정도에만 사고 대응 팀을 배치하여 사고를 처리했다고 응답했습니다.[3]

그림 1. 사고 대응 지출



전 세계적으로 가장 잘 알려진 브랜드 및 기관에 지속적으로 쇄도하고 있는 공격을 기준으로 판단할 때, 사고 대응에 관해서라면 아직 가야 할 길이 멉니다. 오늘날 해커는 인정하기 힘들 정도로 긴 시간 동안(평균 100일 ~200일 동안) 네트워크에서 탐지되지 않고 있습니다.[4]

[1] Gartner, "보안 정보 및 이벤트 관리에 대한 Magic Quadrant", 2013년 5월

[2] Ponemon Institute, "사이버 보안 사고 대응 - 생각하고 있는 만큼 준비되어 있습니까?" 2014년 1월

[3] Dimensional Research, "2016 주요 사고 관리 트렌드", 2015년 12월

[4] Cisco 2015 중기 보안 보고서

"조직은 조기 보안 침해 탐지에 실패하고 있으며, 보안 침해를 당한 조직은 보안 침해의 92% 이상을 탐지하지 못하고 있습니다."

– Gartner

사고 대응 계획 강화

사고 대응은 보안 사고를 탐지하고 이에 대응하는 데 사용되는 인력, 프로세스 및 기술을 포함합니다. 인력, 프로세스 및 기술이라는 각 퍼즐은 효과적인 대응 계획을 수립하고 실행하는 데 있어서 동일하게 중요합니다.

인력

조직의 사고 대응 계획에 관여해야 하는 사람은 누구입니까? 모든 사람이 참여해야 합니다.

CSIRT

무엇보다도, 엔터프라이즈 조직은 숙련된 전담 보안 전문가로 구성되어 완벽한 직무를 수행하는 CSIRT(Computer Security Incident Response Team)를 갖추고 있어야 합니다. 각 조직은 규모와 관계없이 컴퓨터 보안 사고 대응을 담당할 1명 이상의 전담 직원을 배치해야 합니다. 안타깝게도 보안 전문가라는 것이 사고 대응에서도 전문가임을 의미하지는 않습니다. 사고 대응자는 특정한 배경 지식을 보유하고 있거나 강도 높은 대응 시나리오를 처리하도록 교육을 받아야 합니다. 또한 수많은 다른 IT 및 보안 기능에 대한 책임 없이, 사고 대응만을 전담하는 전문가를 확보하는 것이 중요합니다.

사고 대응 팀은 네트워크 및 자산에 대해 심층적으로 이해하고 있어야 합니다. 오늘날 대부분의 경우, 공격자는 철저하게 정찰을 수행할 뿐만 아니라 피해자의 전담 IT 또는 보안 팀보다 더 표적 네트워크에 대해 더 자세히 알고 있습니다. 올바른 기술을 활용한다면, 사고 대응 팀은 네트워크에서 자산을 발견하고, 어떤 자산을 더 중요하게 보호해야 할지 결정하며, 정상적인 행동의 기준을 수립하여 공격을 의미할 수 있는 이상 징후를 더 빠르게 식별할 수 있습니다.

IT 경계를 너머

사고 대응을 위해서는 단순히 적절한 기술 팀을 배치하는 것보다 해야 할 일이 더 많습니다. IT 팀 외에도 법률, 경영, HR, PR 및 기타 부서의 주요 이해관계자는 조직의 사고 대응 계획에서 필수적인 역할을 해야 합니다. 조직은 사고 발생 시 해당 그룹이 어떤 역할을 해야 할지 파악해야 합니다. 조직은 사고가 발생하기 전에 역할 및 책임을 수립하고 해당하는 각 개인을 조기에 배치해야 합니다. 또한 이러한 노력이 효과를 내는 데 필요한 적절한 관심과 자금 지원을 받을 수 있도록 상위 관리층에게 사고 대응 절차, 성공, 과제에 대해 지속적으로 알리는 것이 중요합니다.

마지막으로 이상적인 상황이란 조직에서 함께 일하는 직원(서드파티도 포함)들이 모두 함께 사고 대응 팀 지원을 돕는 것입니다. 소셜 엔지니어링 시도가 발생했을 경우, 어떤 정보부터 검색해야 하는지 알 수 있도록 직원을 교육하십시오. 주의를 기울여 검사하고, 배경 조사를 수행하며, 네트워크에 대한 액세스 권한이 있는 서드파티에게 보안에 대해 문의하거나, 심지어는 단순히 회사의 기밀 정보에 대해서도 문의하십시오. 또한 내부자에 의한 위협도 잊지 마십시오. 관리자가 의심스러운 직원 행동을 찾아보고 이를 HR 팀에 보고하도록 교육하십시오. 또한, 이 문제에 대해 IT 팀과 의견을 나누도록 HR 팀을 교육하십시오.

"Stealthwatch를 통해 보안 및 사고 대응 팀은 이전보다 더 빠르게 사고를 개선할 수 있어 다운타임을 줄이고 네트워크 및 네트워크 서비스 관리에 드는 전반적인 비용을 절감할 수 있습니다."

– 노르웨이 Telenor

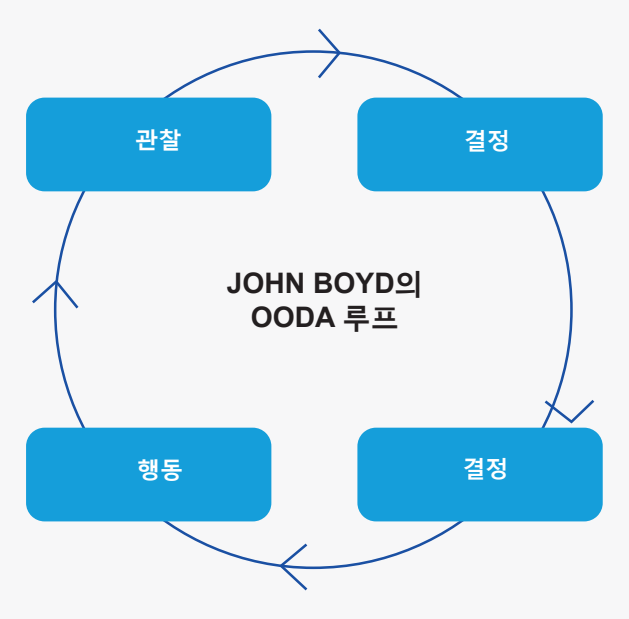
프로세스

사고 대응은 나중에 생각해서 해결할 수 있는 일이 아닙니다. 엔터프라이즈 조직은 비즈니스 전반에 걸쳐 중요한 개인 및 그룹을 통합하는 대응 계획을 세심하게 결정하고 확고하게 확립해야 합니다.

효과적인 결과를 도출하려면, 사고 대응 계획에는 다음 사항을 포함해야 합니다.

1. **모든 역할 수행자에 대한 매우 명확한 역할, 책임 및 승인 프로세스**와 특정한 작업을 수행하거나 수행하지 못하는 경우에 대한 명확한 규칙을 포함해야 합니다. 예를 들어, 사고 대응 팀은 특정한 공격을 억제하기 위해 추가 승인 없이 머신을 오프라인으로 작업하는 것이 허용됩니까? 컴퓨터를 초기화하거나 특정 서비스에 대한 액세스를 차단하는 것은 어떻습니까? 필요시 이러한 작업이 허용됩니까? 또한 보안 침해가 발생할 경우 회사의 법률, 규제 및 계약 의무사항은 무엇입니까? 사고가 발생하기 전에 이러한 질문 유형에 대한 답변을 서면으로 마련하는 것이 중요합니다. 사고 대응 계획은 위기 상황에서 올바른 의사 결정을 수행하기 위해 정책을 마련하는 한편, 숙련된 사고 대응자의 효율성을 저해하는 여러 승인 단계를 없애는 등 알맞은 균형을 유지하는 것이 이상적입니다.
2. **일반 교육 및 평가 연습.** 회사에서 보안 사고 후 다음 사고가 발생하기 까지 상당히 긴 시간이 걸릴 수 있습니다. 이 시간 동안 모든 관련 직원을 지속적으로 교육하고 사고 발생 시의 준비성을 평가하기 위해 평가 연습을 수행하는 것이 중요합니다. 또한 사고가 발생한 경우, 이러한 평가 연습을 팀의 효율성을 측정하는 기회로 활용해야 합니다. MTTI(Mean Time To Identify), 침입 경로를 파악하는 MTTK(Mean Time To Know) 및 MTTF(Mean Time To Fix)와 같은 지표를 사용할 경우 보안 문제는 응답 프로세스를 개선할 뿐만 아니라 상위 관리층에게 투자 수익률을 증명하는 데 상당히 도움이 될 수 있습니다.
3. **경영진과 사고 대응 계획 노력 및 성공에 대해 소통하는 통상적인 수단을 마련**하면 프로세스에 적절한 관심 및 투자가 이루어지고 비즈니스 연속성을 위한 핵심 역할을 이해하는 데 도움이 됩니다.
4. **조직의 인프라 및 "핵심 요소" 위치에 대한 확실한 이해.** 네트워크 내부의 일반적인 활동에 대한 가시성과 외부 세계에서 비롯된 안정적인 위협 인텔리전스는 모두 사고 대응을 위한 핵심 구성 요소입니다.
5. **피드백 체계를 갖추면 사고의 해결**은 물론 조사도 이루어질 수 있습니다. 공격자와 공격자의 공격 방법에 대한 핵심적인 정보는 유사한 공격을 방지하기 위해 포렌식 방식으로 추출되어야 합니다. 군사 전략가인 John Boyd는 전투 작업(그림 2)에서의 의사 결정을 위한 프레임워크로 OODA 루프를 개발했습니다. 오늘날에는 이 루프를 다른 수많은 규칙에 적용하고 효과적인 사고 대응에 필요한 지속적 프로세스의 훌륭한 예로 사용할 수 있습니다.

그림 2. OODA 루프



기술

사고가 발생하기 전에 적합한 기술을 구축하는 것은 적합한 직원 및 프로세스를 마련하는 것만큼 중요한 일입니다.

외부의 위협 인텔리전스는 알려진 공격을 파악하는 데 있어 중요하지만 사고 대응 팀이 네트워크 작업에 대한 중요한 인사이트를 확보하는 데 도움이 되는 툴 없이는 사고 대응 노력은 무의미해집니다. 결국 볼 수 없으면 보호할 수도 없습니다.

사고 대응은 악성코드를 단순히 정리하는 것이 아니라 감염된 컴퓨터를 다시 온라인으로 복원하는 것입니다. 공격의 전체 범위, 추가 머신이 영향을 받았는지 여부 및 공격자가 사용한 전술 유형을 판단하려면 추가 조사를 수행해야 합니다. 이 방법을 통해 사용자의 환경에서 공격을 완전히 제거하고 똑같은 공격이 다시 발생하지 않도록 보장할 수 있습니다.

> "Stealthwatch는 문제 해결 시간을 며칠에서 몇 초로 단축합니다. StealthWatch를 사용하면 잠재적인 공격과 보안 침해에 앞서 대응할 수 있습니다."
>
> **– Edge Web Hosting**

네트워크 감사 추적

오늘날의 복잡한 대규모 네트워크 내부에서 어떤 일이 일어나고 있는지 파악하는 가장 좋은 방법은 네트워크 감사 추적을 수집하고 분석하는 것입니다. 실제로 Ponemon 설문 조사 응답자의 80%가 NetFlow와 같은 소스 및 패킷 캡처를 통해 감사 추적을 분석하는 것이 보안 사고 및 보안 침해를 탐지하기 위한 가장 효과적인 접근 방식이라고 응답했습니다.[5]

네트워크 활동 로그를 사용하여 조직은 더 쉽게 공격 시도를 인식하고 차단할 수 있습니다. NetFlow는 전용 프로브 설치 없이 네트워크 전체에서 수집할 수 있기 때문에 특히나 매우 효과적인 기술입니다. 또한, 데이터가 적절한 비용으로 오랜 시간 동안 저장될 수 있습니다.

NetFlow의 이점

NetFlow(및 다른 유형의 네트워크 텔레메트리)는 Cisco에서 처음으로 생성되어, 현재는 광범위한 네트워크 인프라 디바이스에 내재되어 있으며, 가시성 및 상황 인식을 향상하기 위해 기존 라우터, 스위치 및 방화벽의 중요한 메타데이터를 제공합니다. 또한, 네트워크에서 발생하는 각 연결 기록을 제공하는데, 여기에는 '수신' 및 '발신' 주소, 포트 번호, 전송된 데이터 양 및 기타 정보가 포함됩니다.

NetFlow는 누가 누구에게 말하고 있는지, 어떤 애플리케이션이 사용되고 있는지 등 네트워크 자산 및 행동에 관한 수많은 유용한 정보를 밝힐 수 있습니다.

대부분의 조직은 이미 자사의 환경 내에서 NetFlow에 액세스할 수 있습니다. 조직은 네트워크에 대한 새로운 차원의 인사이트를 확보할 수 있도록 수집 및 분석을 시작하기만 하면 됩니다. 하지만 모든 NetFlow 모니터링 기술이 동일하게 생성되지는 않습니다.

오늘날 경험하고 있는 끊임없는 네트워크 진화를 통해 네트워크는 엄청난 양의 빅 데이터를 생산해 내고 있습니다. 올바른 첫 번째 단계는 이러한 데이터에 액세스하는 것이지만, 안타깝게도 사고 대응 팀이 이러한 데이터를 파악하여 인식 향상 및 더 나은 의사 결정을 위해 사용될 수 있도록 하지 못하는 경우에는 아무 의미가 없습니다. 이것이 Cisco® Stealthwatch와 같은 플로우 기반의 고급 모니터링 솔루션이 필요한 이유입니다.

Cisco Stealthwatch

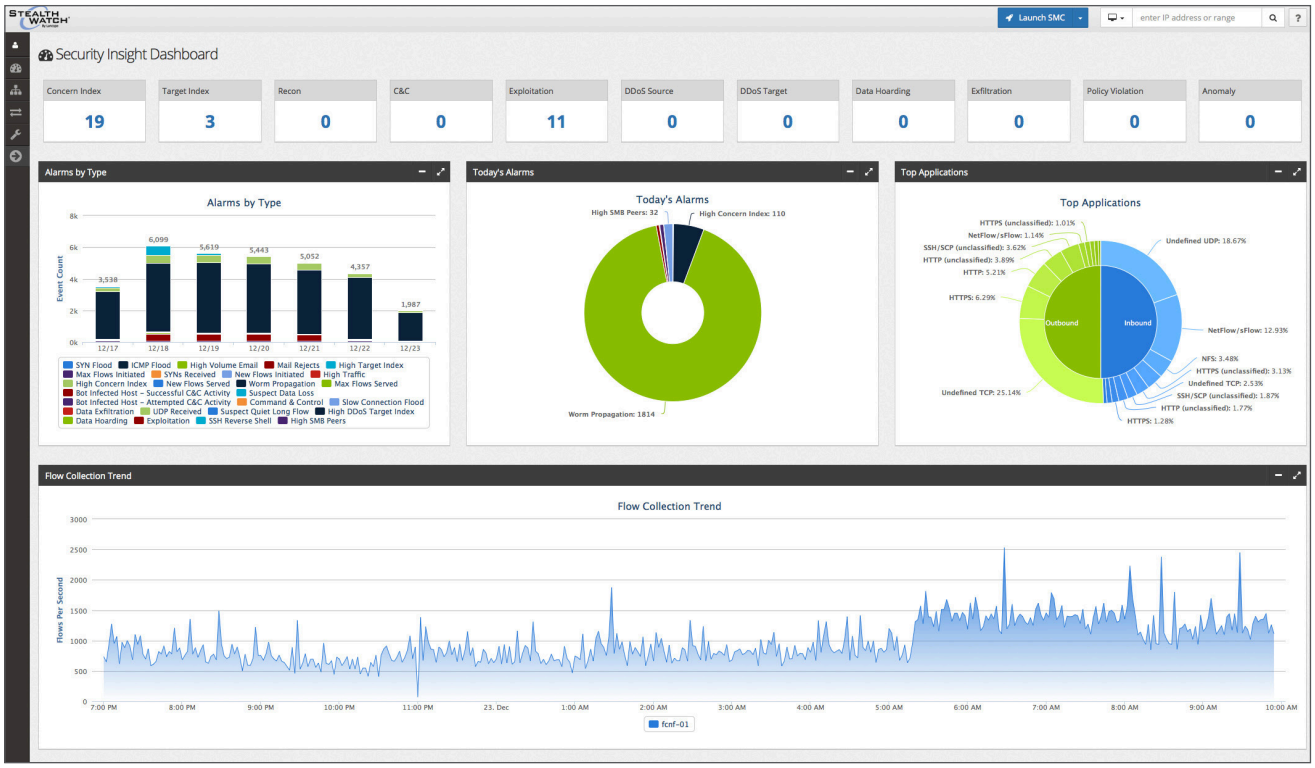
Cisco Stealthwatch는 네트워크의 눈과 귀 역할을 합니다. 빠르게 대량의 NetFlow 데이터를 수집하고 분석하여 심층적인 가시성 및 실행 가능한 인텔리전스를 보안 및 대응 팀에 제공합니다. Cisco Stealthwatch는 앞에서 논의한 심층적인 네트워크 이해 및 네트워크 활동 기준을 제공하며, 이는 강력한 사고 대응 절차를 수립하는 데 있어 핵심 사항입니다.

또한, 다른 Cisco 보안 기술과 결합될 경우, Stealthwatch는 조직이 기존의 인프라를 비용 효율적으로 활용하여 네트워크를 상시 보안 센서로 전환하고 더욱 원활한 위협 탐지가 가능하도록 돕습니다. 정교한 행동 분석을 통해 Stealthwatch는 제로 데이 악성코드 및 DDoS(Distributed Denial-of-Service) 공격에서부터 APT(Advanced Persistent Threat) 및 내부자 위협에 이르기까지 광범위한 공격을 유발할 수 있는 의심스러운 행동을 자동으로 탐지할 수 있습니다.

Stealthwatch는 사고 조사와 관련된 수동 분석을 크게 줄여줍니다. 수일에서 수개월이 걸리던 문제 해결 시간을 단 몇 분으로 단축하는 경우가 많습니다. 직관적인 대시보드 및 보고서를 통해 보안 및 사고 대응 전문가는 몇 번의 클릭만으로 네트워크 활동에 대한 전체 그림, 잠재적인 문제 목록 또는 특정 호스트에 대한 보기(그림 3) 등의 필요한 정보를 얻을 수 있습니다. 이 정보는 또한 상위 관리층과 같은 다른 이해관계자와 쉽게 공유할 수 있습니다.

[5] Ponemon Institute, "사이버 보안 사고 대응 - 생각하고 있는 만큼 준비되어 있습니까?" 2014년 1월

그림 3. Stealthwatch 대시보드



Cisco Stealthwatch는 신속한 사고 대응을 위해 지능형 네트워크 가시성 및 보안 인텔리전스를 제공합니다.

내부자가 반복적으로 네트워크의 제한된 영역에 액세스를 시도하고 있을지도 모릅니다. 또는 매우 많은 양의 데이터가 네트워크로부터 전송되는 중이거나 내부 호스트가 외국의 의심스러운 IP 주소와 통신하는 중일 수도 있습니다. 효과적인 네트워크 가시성 및 보안 분석 툴은 이러한 행동을 파악한 후 더욱 심층적으로 조사가 진행되도록 관리자에게 알림을 보낼 수 있습니다.

> "실제로 응답자의 80%가 NetFlow와 같은 소스 및 패킷 캡처를 통해 감사 추적을 분석하는 것이 보안 사고 및 보안 침해를 탐지하기 위한 가장 효과적인 접근 방식이라고 응답했습니다."
>
> **– Ponemon Institute**

Stealthwatch만의 차별화 요소

네트워크를 오고 가는 트래픽만 모니터링하는 여타 기술과 달리, Stealthwatch는 네트워크 내부에 확산되어 있는 공격을 탐지하고 내부자 위협을 식별하기 위해 측면(East-West) 트래픽을 모니터링합니다. 네트워크의 이상 행동을 지속적으로 모니터링하고 최신 보안 분석, 알람 및 보고서를 사용하여 관리자에게 잠재적인 문제를 알립니다. Stealthwatch로 더욱 빠르고 효율적인 사고 대응이 가능합니다.

NetFlow 프로세스는 일반적으로 전체 패킷 캡처와 같은 대체 솔루션보다 리소스를 덜 사용합니다. 그러나 글로벌 기업에서 광범위하게 로그인이 이루어지면 여전히 기록 수가 초당 1백만 건의 플로우를 초과하게 됩니다. 효과적인 솔루션이란 스토리지 및 전력 소비량을 줄이기 위해 적절하게 확장할 수 있어야 합니다. Stealthwatch는 대량 확장성은 물론 단방향 플로우 기록의 중복을 제거하거나 결합할 수 있는 기능을 갖추고 있으므로, 가장 크고 복잡한 엔터프라이즈 네트워크에서 조차 비용 효율적인 플로우 모니터링과 스토리지가 가능합니다.

Stealthwatch를 사용하면 실시간 위협 탐지의 개선은 물론 더 빠르고 철저한 포렌식 조사를 수행하는 데에도 도움이 됩니다. 또한 수개월 또는 수년간 플로우 데이터를 저장하고 고급 쿼리 기능을 활용하여 이전 공격에 대한 관련 정보를 빠르게 추출할 수 있습니다. 이력 보기는 사고 대응 절차를 조정하여 위협 방어를 개선하는 데 있어 중요합니다. 네트워크가 클라우드, SDN(Software-Defined Networking) 및 IoT 아키텍처를 통해 끊임없이 성장하고 진화함에 따라 엄청나게 많은 양의 네트워크 및 보안 데이터를 효율적으로 수집, 분석 및 해석하는 기능이 점점 더 중요해지고 있습니다.

"Stealthwatch 이전에는 수동으로 네트워크 활동 데이터를 분석하고 상관관계를 분석했습니다. Stealthwatch는 사용하기 쉬운 단일 인터페이스를 통해 자동으로 세부적인 네트워크 인사이트를 제공하며, 보안, 네트워크 운영 및 컴플라이언스 노력을 지원합니다."

– 테네시 주의 BlueCross BlueShield

보안 상황 정보 및 통합 개선

연구에서 69%의 조직이 자사의 보안 툴이 위험을 이해하는 데 충분한 상황 정보를 제공하지 않는다고 답변한 것으로 밝혀졌습니다.[6]

Stealthwatch는 다른 Cisco 기술과의 긴밀한 통합을 비롯한 자체 기술 및 업계 협업을 통해 추가적인 보안 상황 레이어를 제공하여 사고 대응 및 포렌식 속도를 높이고 이를 개선합니다.

부가 가치 인텔리전스 레이어의 예는 다음과 같습니다.

- 사용자 및 디바이스 인식
- 클라우드 가시성
- 애플리케이션 인식
- 위협 피드 데이터
- 엔드포인트 보안 통합
- 프록시 가시성
- 패킷 캡처

단일 콘솔에서 이 모든 정보에 액세스한다면 위협 조사 및 치료를 크게 간소화할 수 있습니다. 실제로, Enterprise Strategy Group에 따르면 80%의 조직이 보안 기술 통합이 부족하여 사고 탐지 및 대응 프로세스에 지장을 받고 있다고 생각합니다.[7] 안타깝게도, 통합되지 않은 솔루션은 위협 완화 속도를 더디게 만들고 공격자가 더욱 쉽게 공격할 수 있도록 보안 격차를 남깁니다. 개선된 상황 정보 레이어 및 심층적인 통합을 통해 오늘날의 조직이 직면하고 있는 모든 유형의 위협에 대해 더욱 자동화되고 유동적이며 효과적인 대응이 가능합니다.

결론

안타깝게도 오늘날의 어떠한 기술도 기업 네트워크로부터 해커를 완벽하게 차단할 수 없습니다. 그러나 조직이 적절하게 혼합된 인력, 프로세스 및 기술과 함께 자사의 환경을 정기적으로 모니터링한다면 보안 팀은 공격이 발생하는 동안에도 공격을 정확히 찾아내고 중단시킬 수 있으며 치명적인 결과를 방지하고 데이터 보안 침해로 인해 발생하는 비용을 피할 수 있습니다.

[6] Ponemon Institute, "권한 있는 사용자 남용 및 내부자 위협", 2014년 5월
[7] Enterprise Strategy Group, "공격 탐지 및 사고 대응 과제", 2015년 4월

추가 정보

Cisco의 폭넓은 보안 포트폴리오와 결합된 Stealthwatch는 네트워크, 데이터 센터, 엔드포인트, 모바일 디바이스 및 클라우드 전반에 걸쳐 에지에서 액세스에 이르기까지 포괄적인 보호 및 간소화된 사고 대응 기능을 제공할 수 있습니다.

Cisco의 자체 CSIRT에서 사고 대응 및 포렌식을 개선하기 위해 Stealthwatch를 사용하여 악성 트래픽을 탐지하고 분석하는 방법을 알아보려면 여기를 클릭하십시오.

자세히 보기. 데모 요청하기.
stealthwatch@cisco.com

"80%의 조직이 보안 기술 통합이 부족하여 사고 탐지 및 대응 프로세스에 지장을 받고 있다고 생각합니다."

– Enterprise Strategy Group

C11-737531-00 07/16