Talos Group

네트워크 보호

Talos에서는 매직 박스나 특효약 같은 보안 솔루션이 존재하지 않음을 알고 있습니다. Talos는 보안이 어려운 문제이며 고객이 보안 문제를 해결할 수 있도록 고객의 역량을 강화하는 새로운 접근 방식이 필요하다는 점을 알고 있습니다. Talos는 고객에게 신속하게 정보를 제공하고 고객을 보호하기 위해 인텔리전스로 무장하고 탐지 기술을 구축하기 위해 노력하고 있습니다.

디지털 세상은 전례 없는 속도로 확장되고 있으며 표적 및 공격 기회도 똑같이 빠르게 늘어나고 있습니다. 이러한 위협과 효과적으로 싸우기 위해서 보안 전문가는 추적 및 탐지를 넘어서서, 오늘날 보안 기술의 경계를 미래의 공격에 대비하는 수준까지 확장해야 합니다. Talos는 업계에서 가장 포괄적인 사전 대응적 보안 및 위협 인텔리전스 솔루션을 제공하며 결과적으로 Cisco 보안 에코시스템의 견고한 기초를 이루고 있습니다.

Talos의 핵심 목표는 고객이 클라우드에서 코어에 이르는 자산을 신속하게 보호하도록 돕는 검증 가능하고 맞춤 설정이 가능한 방어 기술을 제공하는 것입니다. Cisco의 임무는 고객의 네트워크를 보호하는 것입니다.

TALOS란?

Talos는 Cisco의 위협 인텔리전스 조직으로, 고객과 제품 및 서비스를 위해 탁월한 보호를 제공하는 업무를 전담하는 엘리트 보안 전문가 그룹입니다. Talos는 5가지 주요 영역(탐지 연구, 위협 인텔리전스, 엔진 개발, 취약점 연구 및 개발, 서비스 지원)을 다룹니다.

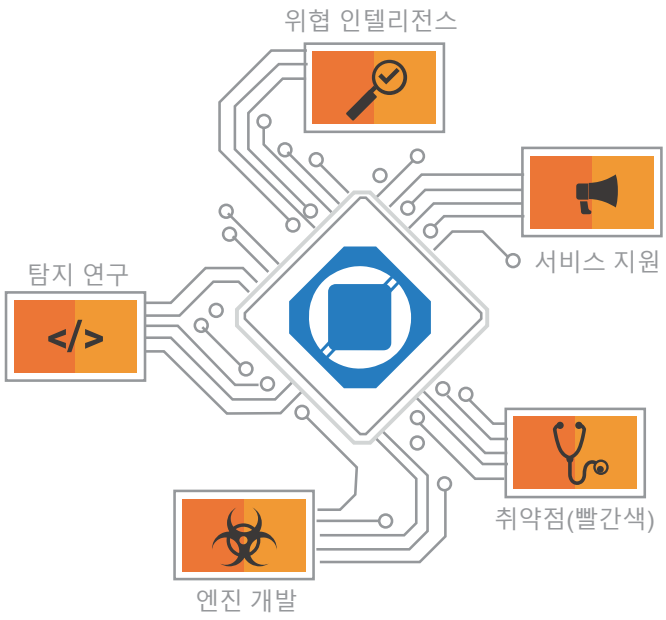
탐지 연구는 모든 Cisco 보안 제품의 탐지 콘텐츠 개발로 이어지는 취약점 및 악성코드 분석으로 구성됩니다. 탐지 연구에는 각 플랫폼에서 가능한 한 가장 효율적이고 효과적인 방식으로 각 위협을 해결하기 위한 분석, 리버스 엔지니어링, POC(Proof of Concept) 코드 개발이 포함됩니다.

위협 인텔리전스는 위협 상관관계 분석 및 추적으로 구성됩니다. 따라서 특성 정보를 실행 가능한 위협 인텔리전스로 전환할 수 있습니다. 위협 및 위협 행위자를 더 신속하게 파악함으로써 Talos 인텔리전스를 통해 고객을 빠르고 효과적으로 보호할 수 있습니다.

엔진 개발 노력을 통해 검사 엔진을 최신 상태로 유지하고 새로운 위협을 탐지하고 해결하는 기능도 유지할 수 있습니다.

취약점 연구 및 개발 부서는 고객이 의존하고 있는 플랫폼 및 운영 체제에서 "제로 데이" 보안 문제를 식별하는 방법을 개발하고 있습니다. 또한, 프로그램을 통한 반복적인 방법을 통해 보안 문제를 찾고 방어하기 위한 새로운 방법을 파악하고 있습니다.

서비스 지원 프로그램에는 공격자가 피해자를 공격하기 위해 사용하는 새로운 트렌드에 대한 연구, 식별 및 커뮤니케이션이 포함됩니다.



Talos는 5가지 주요 영역(탐지 연구, 위협 인텔리전스, 엔진 개발, 취약점 연구 및 개발, 서비스 지원)으로 구성됩니다.

탁월한 보호

깊이 있고 폭넓은 보안 적용 범위

네트워크를 보호하려면 깊이 있고 폭넓은 보안 적용 범위가 필요합니다. 일부 연구 팀에서는 몇 가지 영역에만 중점을 두도록 제한하지만, Talos는 광범위한 위협을 차단하도록 지원하는 데 중점을 두고 있습니다. Talos의 위협 인텔리전스

Next-Generation IPS(통합 애플리케이션 컨트롤 포함/미포함), Next-Generation Firewall 및 AMP(Cisco의 지능형 악성코드 분석 및 차단), Email Security Appliance, Web Security Appliance 및 ThreatGrid뿐만 아니라 수많은 오픈 소스 및 상용 위협 차단 시스템을 포함하는 광범위한 보안 솔루션을 지원합니다. 고객은 Talos 위협 피드에 반영되는 광범위한 Cisco 보안 제품의 고유한 이점을 누릴 수 있습니다. 이로써 모든 자산 유형을 보호하기 위해 Talos의 인텔리전스 및 위협 연구가 모든 환경에 구축될 수 있습니다.

이메일 보안

Talos가 SenderBase© 및 SpamCop©를 활용하여 이메일 기반 위협에 대한 고유한 인사이트를 가지게 된 것은 놀라운 이야기는 아닙니다. Cisco의 다양한 고객 기반으로 얻은 추가적인 관점을 바탕으로 비교할 수 없는 속도와 민첩성으로 위협을 해결하고 식별할 수 있습니다. Cisco의 AMP(Advanced Malware Protection)와 더불어 탐지 기술(예: Outbreak Filter 및 머신 러닝 기반 평판 필터) 레이어를 활용하여 매일 3,000억 개 이상의 이메일을 검사합니다. 모든 기능이 결합된 Talos는 매일 약 2,000억 개의 악성 이메일 또는 초당 230만 개의 이메일을 차단합니다.

최고의 웹 가시성

Cisco Web Security 기술은 새롭게 부상하는 웹 익스플로잇 기술 탐지 및 식별 부문에서 명성을 떨치고 있습니다. 예를 들어, Angler 익스플로잇 킷은 사용자 공격 시 40%의 성공률을 보이기 때문에, 인터넷에서 사용자를 공격하기에 가장 효과적인 방법으로 알려지게 되었습니다. Talos는 매일 약 170억 건의 웹 요청을 파악하며, Cisco의 AMP 기술을 비롯한 여러 가지 보호 방법을 활용하여 사용자를 보호합니다.

검증된 IPS 취약점 기반 보호

Talos는 매일 등장하는 수많은 취약점, 익스플로잇 및 악성코드를 탐지하는 뛰어난 능력으로 업계에 정평이 나 있습니다. 고품질의 신속한 릴리스를 사용하여 고객이 최신 위협에 대한 취약점 기반 차단을 통해 최신 상태를 유지하도록 도와드립니다. 다른 벤더에서는 보안 적용 범위가 유사하다고 주장하지만, Talos만이 유일하게 서드파티 검증에서 Cisco의 탐지 콘텐츠가 최고라는 점을 거듭 입증했습니다. 지난 7년 동안 Talos는 탐지율 부문의 NSS Labs Network IPS 테스트에서 1위 자리를 유지하고 있습니다.

지능형 악성코드 차단

악성코드의 맹공으로부터 고객을 안전하게 보호하려면 혁신적이고 빠르게 발전하는 탐지 기술 및 콘텐츠가 필요합니다. 또한 엄청난 규모의 데이터를 처리하여 이를 실행 가능한 정보로 전환하려면 엄청난 양의 인텔리전스 수집, 리버스 엔지니어링 및 분석이 필요합니다. Talos는 이러한 모든 정보를 활용하여 "실제 상황에서" 나타나는 위협을 발견할 수 있도록 악성코드 차단, 침해 후 보호, 평판 서비스 및 분석 툴을 개발합니다. 이러한 기능은 호스트, 메일 게이트웨이 및 네트워크 자산을 보호하기 위한 모든 Cisco 제품에 포함되어 고객을 위협 전, 중, 후 전 단계에 걸쳐 확실히 보호합니다.

Talos는 엔드포인트, 네트워크, 클라우드 환경, 웹 및 이메일 전반의 위협을 추적하여 사이버 위협, 침입 경로 및 보안 침해의 범위에 대해 포괄적으로 이해하도록 돕습니다.

포괄적인 인텔리전스

실행 가능한 커뮤니티 중심 위협 데이터

모든 종합적인 보안 전략의 핵심 구성 요소는 견고하고 실행 가능한 인텔리전스입니다. 지난 10년 동안 Talos는 업계에서 가장 포괄적인 인텔리전스 수집 및 분석 플랫폼 중 하나를 구축해 왔습니다. ClamAV™, Snort®, Immunet™, SpamCop©, SenderBase©, Threat Grid™ 및 Talos 사용자 커뮤니티를 통해 Talos는 다른 보안 연구팀은 따라올 수 없는 중요한 인텔리전스를 얻습니다. 또한, 전 세계에 있는 사용자 및 고객과 Crete(이전의 SPARK) 프로그램을 통해 협업함으로써 Talos는 위협이 등장할 때 지역 및 언어별 위협을 탐지할 수 있습니다.

취약점 정보 액세스

Talos는 수많은 공용 및 개인 인텔리전스 피드를 매일 분석하여 새로운 위협을 찾고 실시간 정보를 바탕으로 작업하여 새로운 탐지 콘텐츠를 개발합니다. 또한, Talos는 MAPP(Microsoft Active Protection Program)와 같은 산업 파트너십을 통해 Microsoft 및 Adobe 표적 위협을 신속하고 효과적으로 처리할 수 있으며, Microsoft 패치가 이루어지는 동일한 날짜에 탐지 방법을 릴리스합니다. 이로써 고객은 새로운 패치를 테스트 및 구축하면서 동시에 네트워크 및 호스트 기반 보호를 통해 핵심 자산을 보호할 수 있습니다.

TALOS의 제로 데이 위협 차단 예시:

- **TALOS-2015-0024 – Total Commander**
- **TALOS-2015-0018 – Apple Quicktime**
- **VRT-2014-0301 – Microsoft Windows FastFAT**

실시간 악성코드 인텔리전스

Talos는 허니 팟, 샌드 박스 및 악성코드 커뮤니티의 광범위한 산업 파트너십과 더불어 전 세계 수백만 명의 사용자로부터 확보한 데이터를 모아 하루에 1,100,000개 이상의 악성 소프트웨어 샘플을 수집합니다. Talos의 지능형 분석 인프라는 이 샘플을 자동으로 분석하고 매일 탐지 콘텐츠를 신속하게 생성하여 이러한 위협을 완화합니다. 이로써 공격자가 사용자를 공격하려고 시도할 때 이러한 위협 환경에 대한 탁월한 인사이트와 뛰어난 관점을 얻을 수 있습니다.

위협 연구

PoSeidon과 같은 POS(Point of Sale) 단말기를 목표로 하는 새로운 악성코드 계열, "Kyle and Stan"과 같은 널리 퍼져 있는 맬버타이징 네트워크, 심지어 "SSHPsychos"와 같은 인터넷의 핵심 서비스에 위험을 초래하는 위협을 포함하여 어떤 위협을 식별하든지 Talos를 활용하여 공격자를 식별, 연구 및 문서화할 수 있습니다.

각각의 연구가 진행될 동안 Talos는 고객이 위협을 방어할 수 있는 여러 가지 방법을 찾습니다. Talos는 직면한 문제를 식별하고 치료할 뿐만 아니라 문제가 개별 악성코드 캠페인과 확실히 관련이 있는 경우에도 모든 공격자의 공격과 관련된 네트워크의 모든 요소를 식별한다는 점에 자부심을 느끼고 있습니다. Cisco 고객은 이러한 위협 인텔리전스를 모든 제품에 구축한 후 많은 혜택을 경험하고 있습니다.

또한 이러한 정보는 블로그, Snort 규칙, 회의 및 백서를 통해 공개적으로 공유됩니다. 가능한 한 많은 사람에게 이 정보를 제공하여 공격자에 대한 장애물을 더욱 쉽게 소개할 수 있습니다.

Talos는 전 세계 수백만 명의 사용자와 허니 팟, 샌드 박스 및 광범위한 산업 파트너십으로부터 데이터를 얻으며 하루에 110만 개 이상의 고유한 악성코드 샘플을 수집하고 있습니다.

혁신적인 탐지 기술

동적 환경을 위한 유연한 방어 기술

위협 환경은 네트워크 서비스의 버퍼 오버플로우에서 브라우저 및 파일을 표적으로 삼는 복잡한 클라이언트 측 공격으로 진화해 왔습니다. 공격이 변화함에 따라 공격을 탐지하는 데 사용되는 방어 기술도 변화해야 합니다. Talos는 오늘날의 탐지 메커니즘의 한계에 도전하는 새로운 탐지 기술을 끊임없이 찾고 있으며 동시에 미래의 위협에 신속하게 대응할 수 있도록 민첩성을 유지하고 있습니다.

위협 예측

새로운 위협에 대응하는 것과 새로운 위협으로부터 보호하는 것은 별개의 문제입니다. Talos는 고객에게 영향을 미치는 새로운 취약점과 위협을 끊임없이 찾고 있습니다. 새로운 취약점이 발견되면, Talos는 제로 데이 위협을 차단하는 규칙을 릴리스하는 한편, 영향을 받는 벤더는 패치를 개발 및 테스트합니다. 이러한 보호책을 통해 Talos 고객은 벤더의 보호를 기다리는 동안 위협을 제어할 수 있습니다.

Talos는 또한 인터넷에서 새로운 악성 웹사이트, 봇넷 C2(Comand and Control) 서버 및 기타 악성 사이트의 위치를 적극적으로 찾고 있습니다. 일단 위치를 찾아내면 해당 정보는 포괄적인 IP 블랙리스트 및 URL 필터링 피드로 분류 및 통합된 다음 고객에게 배포될 뿐만 아니라 인터넷을 더욱 안전한 장소로 만들기 위해 업계 파트너와도 공유됩니다.

신뢰할 수 있는 커뮤니티

팀 확장

상황이 힘들어질 때 의지할 수 있는 신뢰할 수 있는 장소를 확보하는 것은 효과적인 보안에 있어 필수적입니다. 보안 및 대응 팀과 신뢰할 수 있는 파트너 간의 강력한 커뮤니케이션 채널 없이는 최신 위협에 대응해 최신 상태를 유지하고 고객의 고유한 보안 문제를 해결할 수 없습니다. Talos는 Talos가 고객의 보안 팀의 추가적인 인력과 같은 역할을 해야 한다고 믿고 있습니다. Talos는 단순히 고객에게 정보를 제공하는 것이 아니라 고객의 목표와 고객이 이 목표를 달성하는 데 어떤 도움을 줄 수 있는지에 대해 건설적인 대화를 나누길 원합니다. Talos는 이를 지원하기 위해 여러 가지 프로그램을 만들었습니다.

인텔리전스 공유

AEGIS™(Awareness, Education, Guidance, and Intelligence Sharing) 프로그램은 고객의 특수한 환경에서 맞춤형 탐지 문제를 해결하는 데 도움이 되기 위해 고객 및 파트너와 상호 작용을 할 수 있도록 특별히 생성되었습니다. AEGIS는 보안 업계의 참여 구성원과 Talos 위협 인텔리전스 팀을 직접 연결하여 맞춤형 탐지 콘텐츠를 구축하고 보안 사례를 개선하고 제품 및 서비스에 대한 피드백을 수집하며 제품에 대한 고객 개선사항을 구현하는 데 도움을 줍니다. 이것은 고객 네트워크를 보호하는 데 도움이 되는 한 가지 방법에 지나지 않습니다.

Crete 프로그램은 Talos 및 고객 간의 협업 교환 프로그램으로, 실시간 시나리오 및 트래픽을 제공하며 참여 고객에게는 첨단 인텔리전스를 제공합니다.

Talos

콘텐츠	URL
Talos 웹사이트	talosintel.com
Talos 블로그	blogs.cisco.com/talos
Talos 트위터	twitter.com/talossecurity
Talos YouTube 채널	cs.co/talostube
IRC 채널	irc.freenode.net: #snort, #razorback, #clamav
ClamAV 웹사이트	clamav.net
ClamAV 블로그	blog.clamav.net
Snort 웹사이트	snort.org
Snort 블로그	blog.snort.org
Talos 규칙 자문	snort.org/talos

대화형 정보

Talos는 수많은 대화형 채널을 통해 고객과 지속적으로 관계를 유지합니다. Talos, ClamAV 및 Snort 블로그는 최신 위협 정보, 맞춤형 탐지 콘텐츠 생성 방법 및 최신 악성코드 계열에 대한 심층적인 분석에 대한 정보를 지속적으로 업데이트합니다. Talos 리소스 목록과 Talos와 상호 작용하는 방법은 아래 표를 참조하십시오.

최신 상태 유지

Talos는 인텔리전스 수집, 분석, 콘텐츠 생성, 패키지 생성 및 품질 보증, 최종 사용자 전달에 이르기까지 Cisco 탐지 및 방지에 대한 전체 체인을 책임집니다. 이 전체 프로세스 제어를 통해 Talos는 오늘날의 최신 위협에 방어하는 데 필요한 시간 프레임 내에서 업계 최고의 탐지 콘텐츠를 신속하게 제공할 수 있습니다.

결론

Talos는 네트워크를 보호하기 위한 고유하고 포괄적인 사전 대응적 접근 방식을 제공합니다. 보안 업계에서 부러워할 만한 성공 이력과 선도적 입지를 유지하고 있는 Talos 팀원은 정확성과 관련성에 대한 새로운 기준을 수립하는 우수한 품질의 고객 중심 보안 연구에 중점을 두고 있습니다.

Talos 고객이라면 이러한 기술 및 연구를 바탕으로 한 수상 경력을 지닌 제품 및 서비스를 만나볼 수 있습니다. Talos 고객이 아니더라도, Talos 연구 성과에서 제공하는 이점을 누리실 수 있습니다. 오픈 소스 모델에 대한 Talos만의 지속적인 노력과 끊임없는 연구 논문, 프레젠테이션, 블로그 게시물 등을 통해 Talos는 전체 커뮤니티가 사용할 수 있는 많은 영향을 미치는 효과적인 지식 및 툴을 만들었습니다.

업계 최고의 레코드 및 레거시를 제공합니다.