기술 검증

주니퍼 네트웍스 자동 위협 탐지 및 대응

Sky Advanced Threat Prevention 및 SRX 시리즈 방화벽

Jack Poller, 시니어 애널리스트

2019 년 7 월

이 ESG 기술 검증은 주니퍼 네트웍스에서 의뢰했으며 ESG 의 라이선스하에 배포됩니다.

목차

ESG 기술 검증

ESG 기술 검증은 모든 규모 및 유형의 기업에 필요한 정보 기술 솔루션에 대한 내용을 IT 전문가에게 교육하기 위한 용도로 제작되었습니다. ESG 기술 검증 은 구매 의사결정을 내리기 전에 수행해야 하는 평가 프로세스를 대체하는 것이 아니라 이러한 최신 기술에 대한 통찰력을 제공하기 위한 목적으로 사용됩니다. ESG 의 목표는 보다 가치 있는 IT 솔루션 기능을 연구 조사하여 고객의 실제 문제를 해결하는 데 사용할 수 있는 방법을 알려주고 개선이 필요한 영역을 식별하는 것입니다. ESG 검증 팀의 전문적 제 3 자 관점은 실제 테스트뿐만 아니라 생산 환경에서 해당 제품을 사용하는 고객들과의 인터뷰를 기반으로 합니다.

소개

이 ESG 기술 검증은 주니퍼 네트웍스 Sky ATP(Advanced Threat Prevention) 및 SRX 시리즈 차세대 방화벽에 대한 평가로, 자동화된 위협 탐지 및 문제 해결의 효과와 효율성에 초점을 맞춥니다. 기술 검증 과정에서 ESG 는 엔드포인트를 멀웨어에 감염시키고 Sky ATP 를 사용하여 공격을 탐지합니다. Sky ATP 가 공격을 탐지하면 방화벽이 엔드포인트의 north-south 트래픽을 차단하고 로컬 스위치가 엔드포인트의 east-west 트래픽을 차단하여 엔드포인트를 네트워크에서 차단합니다.

배경

ESG 의 연간 기술 지출 설문 조사에 따르면 사이버 보안이 IT 의 최우선 책임 과제로 부상했으며, 응답한 조직의 40% 가량이 사이버 보안 강화가 향후 12 개월 내에 기술 부문의 지출을 주도할 최상위 요소가 될 것이라고 밝혔습니다.[1]

하지만 다양한 측면에서 사이버 보안을 강화하는 것이 쉽지만은 않습니다. ESG 조사에 따르면 오늘날 위협 탐지 및 대응이 2 년 전보다 더 어렵다고 응답한 조직이 전체의 3/4 을 넘어 76%에 달합니다. 응답자들은 위협 탐지와 대응에 있어서의 주요 과제로 위협의 양과 정교함 증가(34%), 위협 탐지/대응 워크로드 증가(17%), 공격 경로 증가(16%), 서로 다른 위협 탐지/대응 툴 증가(11%), 사이버 보안 전문인력 부족(8%) 등을 꼽았습니다.[2]

사이버 보안 강화가 향후 12 개월 내에 기술 부문에서 가장 많은 지출 요인이 될 것이라고 밝힌 응답자 비율입니다.

위협 탐지 및 대응이 2 년 전보다 오늘날 더 어렵다고 밝힌 응답자 비율입니다.

실제로 조직은 위협을 탐지하고 이에 대응하기 위해 여러 벤더의 서로 다른 여러 툴을 구축하므로 분석가가 시스템마다 일일이 로그인하여 알림을 관리하고 보호 조치를 취해야 합니다. 이러한 수작업으로 인해 탐지, 조사, 응답, 대응 프로세스가 지연되는 동시에 MTTR(mean-time-to-respond)과 공격자의 체류 시간(dwell time)이 증가할 수 있습니다.

따라서 위협 탐지 및 대응 워크플로우를 자동화하여 이러한 여러 툴의 사용과 관리를 간소화하는 솔루션, 즉 다양한 개별 툴들의 기능이 통합된 솔루션이 필요합니다. 조사 응답자의 82%는 위협 탐지/대응을 개선하는 것이 최우선 과제라고 답했고, 87%는 위협 탐지 및 대응을 개선하기 위한 공식적인 계획과 자금이 마련되어 있다고 답했습니다.[3]

[1] 출처: ESG 조사 보고서, *2019 기술 지출 의향 설문조사*, 2019 년 2 월.

[2] 출처: ESG 마스터 설문조사 결과, *위협 탐지 및 대응트렌드*, 2019 년 4 월.

[3] Ibid.

주니퍼 네트웍스 Sky Advanced Threat Prevention 및 SRX 시리즈 방화벽

주니퍼 네트웍스의 Sky Advanced Threat Prevention 은 주니퍼 네트웍스 SRX 시리즈 서비스 게이트웨이와 함께 사용 시 시너지 효과를 발휘합니다. 분산된 가상 코어 로케이션을 위한 라우팅, 스위칭, WAN 인터페이스를 통해 고성능 네트워크 보안 및 고급 위협 방어 기능을 제공합니다.

Sky Advanced Threat Prevention

SaaS 솔루션으로 실행되는 주니퍼 네트웍스의 SKY ATP(Advanced Threat Prevention)는 클라우드에서 멀웨어에 대한 실시간 정보를 사용하여 지능형 지속 위협(advanced persistent threats, APT)과 랜섬웨어 등 사이버 공격으로부터 조직을 보호합니다. Sky ATP 는 SRX 시리즈 차세대 방화벽과 통합되어 심층 패킷 검사을 실행하고 위협에 대한 인라인 차단을 제공할 수 있습니다. Sky ATP 는 사이버 공격을 탐지하고 방지하기 위해 머신 러닝, 동적 분석, 안티샌드박스 우회(anti-sandbox evasion) 기술, 정적 분석 및 안티바이러스 시그니처를 사용합니다. Sky ATP 를 구축하는 조직의 이점:

- **클라우드 기반 분석**—잠재적 위험 파일이 클라우드에 전송되어 고급 분석을 통해 정상적인지 악성인지 여부를 판단할 수 있습니다.
- **멀웨어 문제 해결**—멀웨어 탐지 결과가 SRX 시리즈 방화벽에 전달되어 공격을 차단합니다.
- **보고 및 분석**—구성 및 업데이트를 비롯한 관리를 간소화할 수 있는 Sky ATP 웹 인터페이스와 위협 및 감염된 시스템을 확인하기 위한 보고 및 분석 툴이 제공됩니다.
- **시스템 격리**—SRX 시리즈 방화벽은 Sky ATP 의 정보를 사용하여 손상된 시스템을 격리합니다.
- **통합 위협 인텔리전스**—주니퍼 네트웍스 SecIntel 위협 인텔리전스 서비스와의 실시간 통신을 통해 SRX 시리즈 방화벽에 대한 위협 정보를 공유하여 즉각적인 조치를 취할 수 있습니다. Sky ATP 는 개방형 API 를 사용하여 타사 위협 인텔리전스 피드를 모든 ATP 서브스크립션 SRX 방화벽에 배포하여 즉각적인 대응이 가능하도록 함으로써 공격 노출을 줄입니다.
- **C&C(Command-and-control) 방지**—Sky ATP 는 SRX 시리즈 방화벽과 통신하여 멀웨어의 내부망 확산을 방지하고 C&C 서버와의 통신을 차단합니다.
- **이메일 및 웹 분석과 교정**—머신 러닝 알고리즘이 이메일 및 웹 파일을 분석하여 악성 첨부 파일과 파일을 검색하고 방화벽으로 해당 파일을 차단하여 이메일이 공격 벡터로 사용되는 것을 방지합니다.
- **통합 관리**—Sky ATP 및 SRX 시리즈 방화벽은 주니퍼 네트웍스 Junos Space Security Director 에 통합 가능합니다. Junos Space Security Director 는 주니퍼 네트웍스 디바이스 및 서비스의 관리를 단일 콘솔로 통합하는 통합

애플리케이션입니다. 관리자는 Security Director 를 사용하여 스테이트풀 방화벽, 통합 위협 관리, 침입 방지, 애플리케이션 방화벽, VPN, NAT 에 대한 보안 정책 수명 주기의 모든 단계를 관리할 수 있습니다.

SRX 시리즈 서비스 게이트웨이

주니퍼 네트웍스 SRX 시리즈 서비스 게이트웨이는 차세대 방화벽으로, 클라우드, 브랜치 오피스, 중소기업 및 대기업, 대규모 데이터센터 및 서비스 프로바이더를 지원하도록 설계된 가상 또는 물리적 어플라이언스로 사용할 수 있습니다. SRX 방화벽은 다음을 위해 설계되었습니다.

- **모든 규모의 조직을 위한 보안**—SRX 방화벽은 올인원, 통합 물리적/가상 보안 네트워킹 디바이스에서 확장성이 뛰어난 섀시 기반 데이터센터 솔루션에 이르기까지 다양한 폼 팩터로 제공됩니다.
- **포괄적 위협 보호**—포괄적인 계층형 보안 서비스 제품군을 통해 알려진 위협과 알려지지 않은 위협으로부터 보호할 수 있습니다.
- **성능 및 확장성**—최대 285Gbps IMIX 방화벽, 9 천만 개의 동시 세션 및 230Gbps IPS 를 통해 최대 1Tbps 의 처리량을 지원하도록 확장할 수 있습니다.
- **안정성**—무중단 비즈니스 연속성, 보안 및 애플리케이션 가용성을 위해 서비스 내 하드웨어 및 소프트웨어 업그레이드, 이중화 구성 요소, 최대 99.9999%의 안정성을 통해 지속적인 가동 시간을 보장합니다.

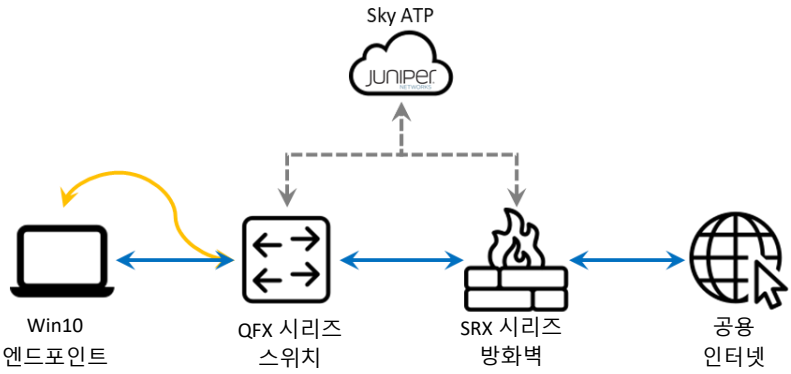
ESG 기술 검증

ESG 의 Sky Advanced Threat Prevention 및 SRX 시리즈 방화벽 평가 및 테스트에는 악성 파일을 엔드포인트에 다운로드하고 SRX 방화벽이 평가를 위해 해당 파일을 Sky ATP 로 전송했는지 확인하는 작업이 포함되었습니다. Sky ATP 가 감염된 엔드포인트 발견 시 수행하는 자동화된 탐지, 대응, 해결 과정을 중점적으로 확인하였습니다.

시작하기

테스트에 앞서, 그림 1 과 같이 테스트 베드를 제작했습니다. 먼저 Windows 10 엔드포인트를 가상 머신으로 실행했습니다. 엔드포인트는 VLAN 4025 의 주니퍼 네트웍스 가상 QFX 시리즈 스위치에 연결되었고, 이는 VLAN 3025 로의 별도 연결로 전환 가능합니다. QFX 스위치가 SRX 시리즈 가상 방화벽에, 다음으로 공용 인터넷에 연결되었습니다. QFX 스위치 및 SRX 방화벽이 Sky ATP 로 통합되었습니다.

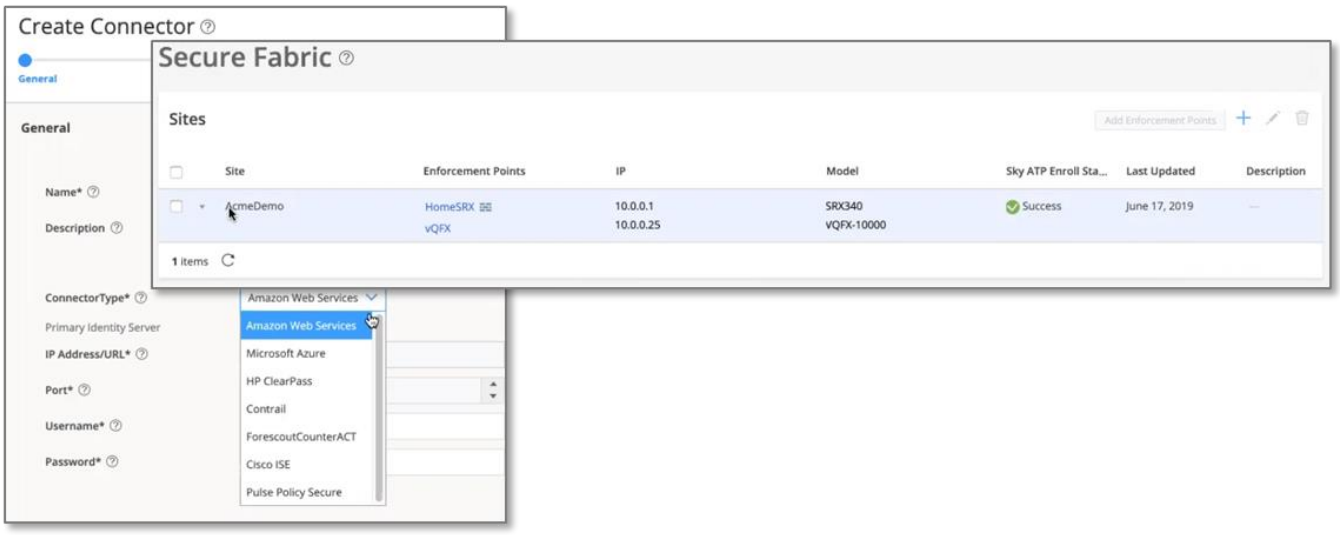
그림 1. ESG 테스트 베드



출처: Enterprise Strategy Group

주니퍼 네트웍스 Junos Space Security Director 를 통합 콘솔로 사용하여 모든 주니퍼 시스템을 관리했습니다. 그림 2 와 같이 방화벽을 관리하고 단일 보안 도메인으로 전환할 수 있는 보안 패브릭을 만들었습니다. 또한 AWS, Azure, ClearPass, Contrail, Forescout CounterACT, Cisco ISE 및 Pulse Policy Secure 와 같은 타사 서비스와 스위치에 Sky ATP 를 연결할 수 있는 커넥터 생성 기능도 검토했습니다.

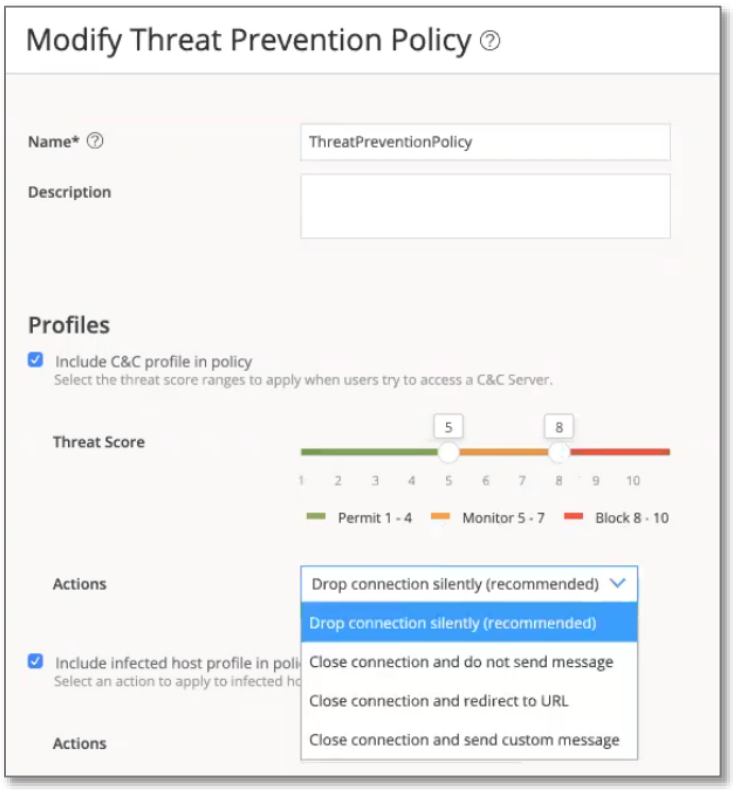
그림 2. Sky ATP 보안 패브릭 및 커넥터



출처: Enterprise Strategy Group

다음으로 Sky ATP 위협 방지 정책을 검토했습니다. 그림 3 에서와 같이, Sky ATP 는 위협 점수에 따라 사전에 결정된 조치를 설정할 수 있도록 되어 있습니다. 위협 점수가 8 이상인 모든 오브젝트에 대한 연결을 자동으로 삭제하기로 선택했습니다.

그림 3. Sky ATP 위협 방지 정책



출처: Enterprise Strategy Group

이러한 기능이 중요한 이유

사이버 보안은 복잡하고 까다롭습니다. 또한 숙련된 전문 인력이 부족하고 사용자 환경과 인터페이스가 서로 다른 여러 벤더의 멀티 포인트 툴을 조정하는 것이 복잡하여 위협 탐지 및 방어의 어려움은 가중되고 있습니다. 이러한 복잡성을 해결하기 위해 조직은 사이버 보안 인프라 및 프로세스를 단순화하는 솔루션이 필요합니다.

ESG 의 검증 결과 주니퍼 네트웍스는 구축을 단순화할 수 있었으며 보안 패브릭을 쉽게 만들 수 있었습니다. 각 디바이스에서 정책을 개별적으로 설정하는 대신 서로 다른 시스템 그룹에 대한 정책을 정의하고 설정할 수 있었습니다. 슬라이더를 사용하여 다양한 위험 수준에 대한 임계값과 대응조치를 설정하는 방식으로 손쉽게 보안 정책을 설정할 수 있었습니다.

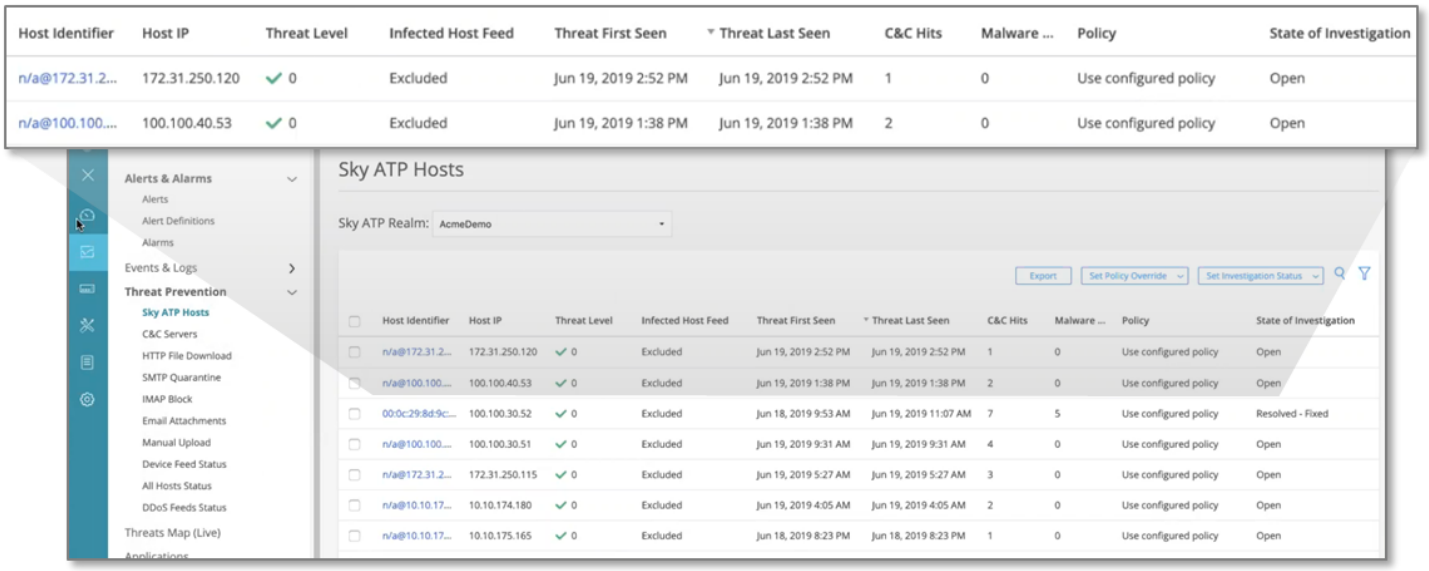
또한 ESG 는 가상 및 물리적 주니퍼 네트웍스 디바이스의 임의 그룹에 대한 정책을 정의하고 설정하여 복잡한 환경에서 보안 및 네트워크 관리를 단순화할 수 있음을 검증했습니다. Sky ATP 및 SRX 방화벽을 사용하면 보안 분석가가 툴 구성 및 관리에 소요되는 시간을 단축하여 알림에 대응하고 위협 및 공격 조사와 같은 중요한 활동에 더 많은 시간을 할애할 수 있게 됩니다.

감염, 탐지 및 대응

ESG 는 주니퍼 네트웍스에서 파일을 다운로드할 때 위협을 방지하기 위해 사용하는 프로세스를 관찰했습니다. 멀웨어를 엔드포인트로 다운로드하고 SRX 방화벽이 분석을 위해 다운로드한 파일을 Sky ATP 로 보냈습니다. Sky ATP 가 파일을 분석하여 파일이 악성 프로그램이고 호스트에 감염된 것으로 확인되면 Sky ATP 는 SRX 방화벽 및 QFX 스위치의 엔드포인트 연결을 네트워크로부터 끊도록 지시하여 north-south 트래픽(SRX 방화벽)과 east-west 트래픽(QFX 스위치)을 모두 차단했습니다.

먼저, 그림 4 와 같이 환경의 현재 상태를 검토했습니다. Sky ATP 는 테스트 Windows 10 엔드포인트를 관리 엔드포인트 목록에 포함했으며 엔드포인트(IP 주소 100.100.40.53)는 ***감염된 호스트 피드***에서 ***제외*** 되었습니다. Sky ATP 는 이 목록을 사용하여 손상된 호스트를 추적합니다.

그림 4. Sky ATP 호스트 모니터링



출처: Enterprise Strategy Group

그런 다음 가상 SRX 방화벽 및 가상 QFX 스위치에 로그인하여 구성을 통해 엔드포인트가 내부(east-west) 및 외부(north-south)와 올바르게 통신할 수 있는지 확인했습니다.

Windows 10 엔드포인트에 로그인한 후 웹 브라우저를 사용하여 멀웨어 샘플을 호스팅하는 웹 사이트로 이동하여 멀웨어가 포함된 파일 3 개를 다운로드했습니다.

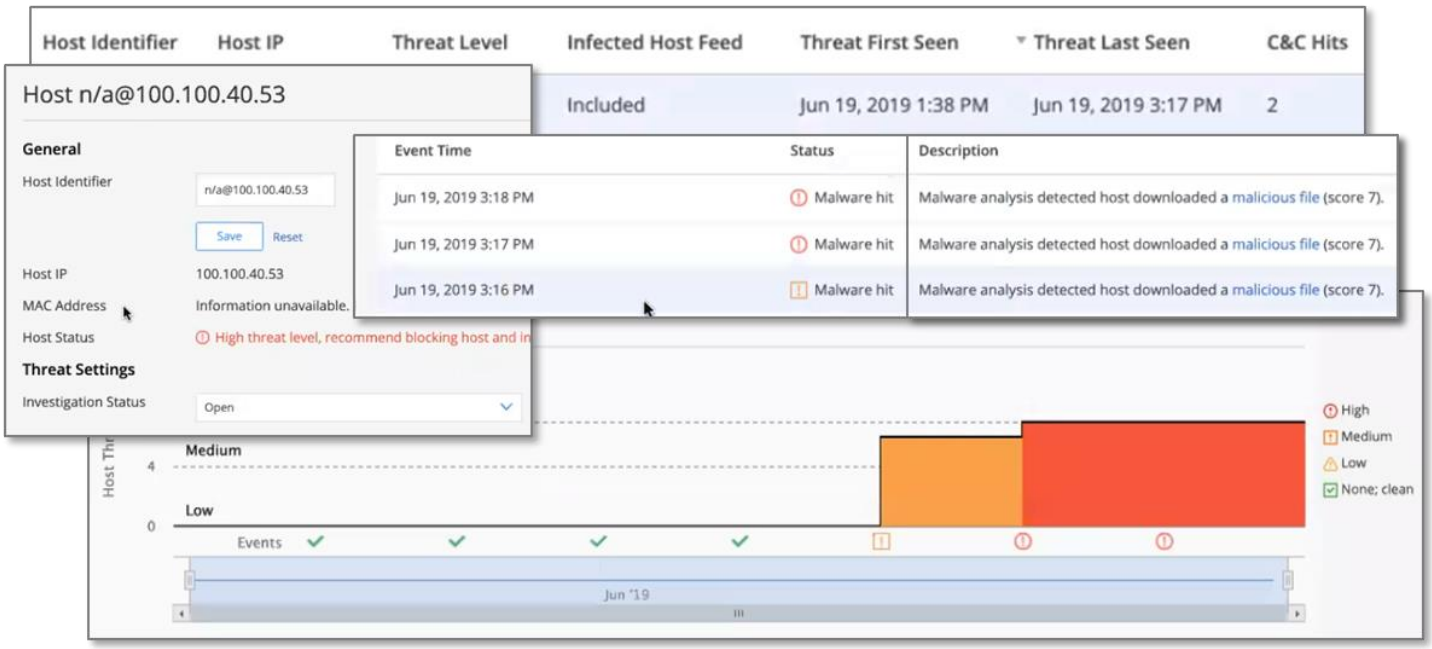
각 파일 다운로드가 끝날 때마다 SRX 방화벽은 분석을 위해 파일 복사본을 Sky ATP 로 보냈습니다. Sky ATP 는 멀웨어 데이터베이스에 대한 시그니처 비교, 머신 러닝을 통한 정적 분석, 동적 샌드박스 분석, 행동 분석 등 일련의 검사를 각 파일에 적용했습니다. 이러한 검사를 통해 Sky ATP 는 각 파일에 멀웨어가 포함되어 있음을 확인했습니다. 자동

분석 단계에서 수집된 정보를 기반으로 Sky ATP 는 각 파일에 위협 점수를 할당하고 엔드포인트에 대한 위협 점수 총계를 계산했습니다.

Sky ATP 는 위협 점수 총계와 이전에 구성된 위협 방지 정책(그림 3 참조)을 기반으로 호스트 상태를 ***높은 위협 수준***으로 설정하고, 조사 상태를 ***시작됨 상태***로 설정하며, 엔드포인트를 감염된 호스트 목록(그림 5 와 같이 ***감염된 호스트 피드***)에 추가합니다.

보안 분석가의 일반적인 워크플로에 따라 ESG 는 호스트 식별자 링크를 클릭하여 조사를 시작했습니다. 호스트 식별자 링크를 클릭하면 호스트에 감염되는 멀웨어 목록과 시간 경과에 따른 감염을 보여주는 그래프가 포함된 추가 정보가 표시됩니다. 이 정보는 조사 시작, 근본 원인 분석, 엔드포인트 치료 및 문제 해결에 유용합니다.

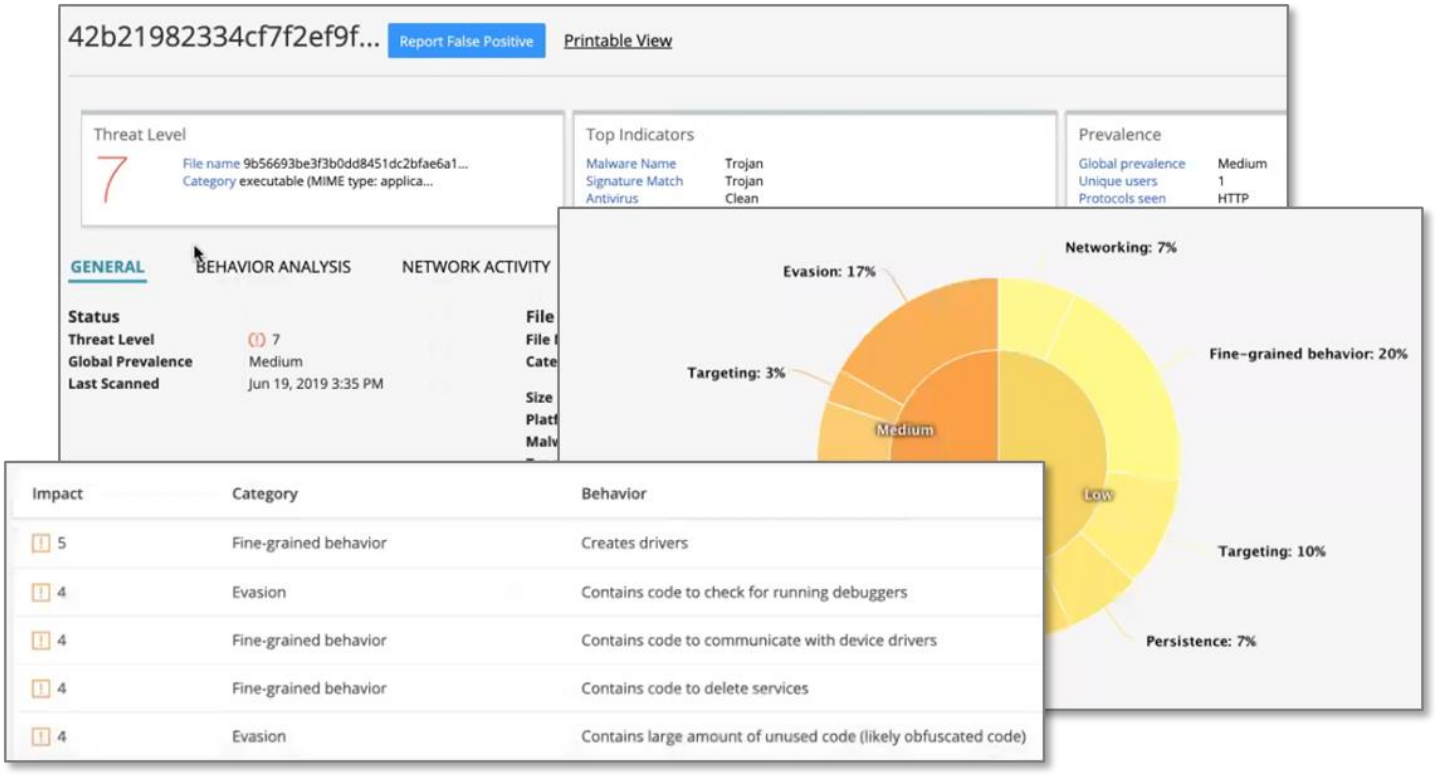
그림 5. 감염된 호스트 세부 정보



출처: Enterprise Strategy Group

다음으로 다운로드한 멀웨어의 링크를 클릭하면 그림 6. 위협 수준, 상위 지표 및 위협의 확산 정도를 포함한 요약 정보가 상단에 제공되었습니다. 요약 데이터 아래의 탭 창은 일반 정보를 제공합니다. 동작 분석 탭을 클릭하면 위험 기반 원형 차트가 나타나 위험에 따라 여러 동작을 분류합니다. 이 악성코드는 트로이 목마(Trojan)로 분류됐으며 이는 중간 위험도의 우회와 타겟팅 기법, 낮은 위험도의 네트워킹, 우회, 타겟팅, 지속성 기술 등을 포함합니다. 또한 Sky ATP 는 식별된 각 동작에 대한 세부 정보가 포함된 표를 표시했습니다. 추가 탭에서는 멀웨어의 네트워크 작업을 자세히 설명하는 테이블을 제공했습니다.

그림 6. 멀웨어 세부 정보



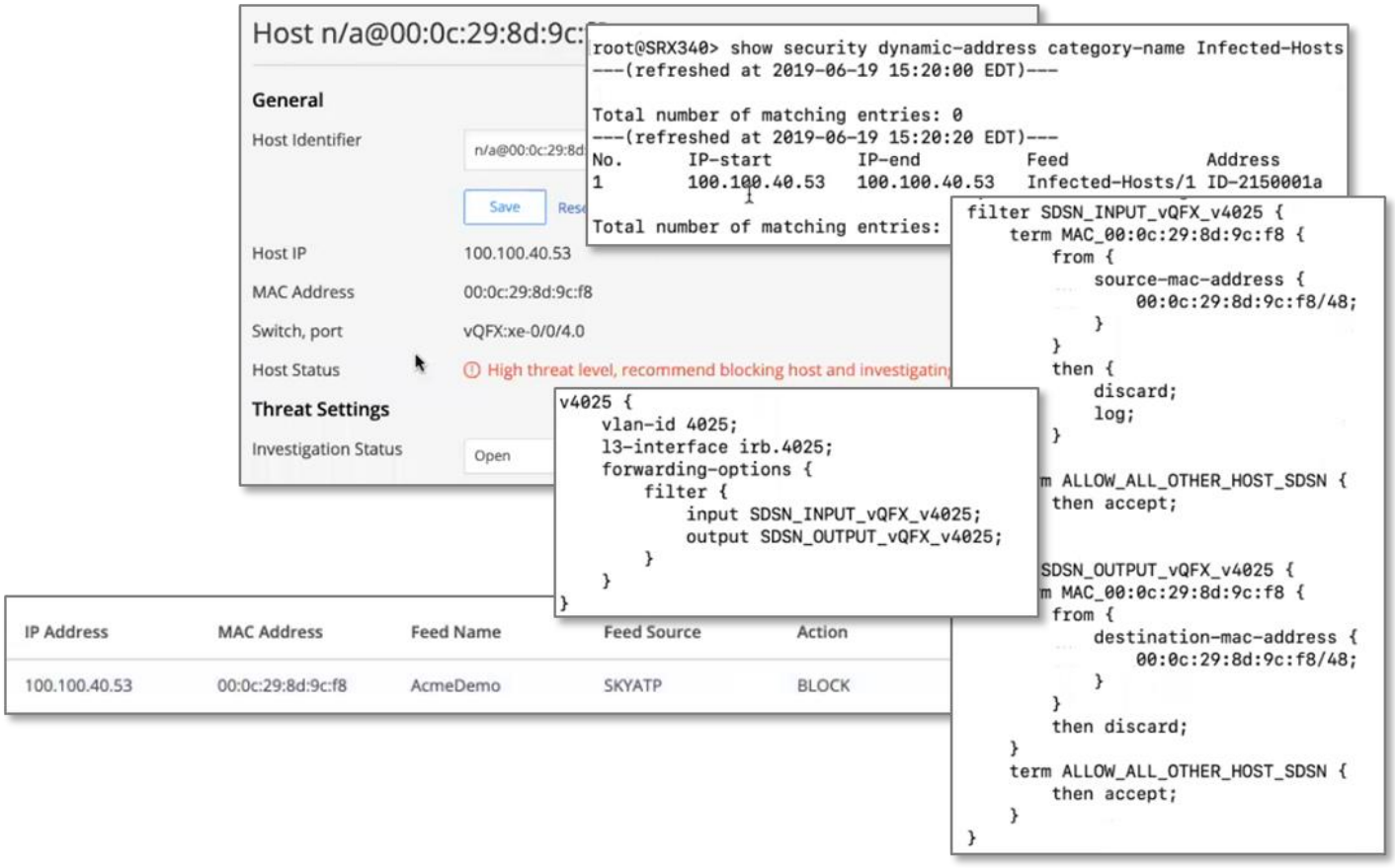
출처: Enterprise Strategy Group

파일을 다운로드한 후 5 분 이내에 엔드포인트가 네트워크에서 분리되었다고 판단했습니다. 내부 또는 외부 IP 주소의 연결이 불가능하여 Sky ATP 의 자동화된 위협 대응 방식이 검증되었습니다. 감염된 호스트 피드에 엔드포인트를 추가하자 SRX 방화벽이 엔드포인트의 north-south 통신을 차단하였습니다. 또한 엔드포인트의 DHCP 리스가 취소되고 엔드포인트의 IP 주소가 손실되었습니다.

IP 주소가 무효화되었기 때문에 그림 7 과 같이 Sky ATP 는 MAC 주소의 감염된 엔드포인트를 참조하도록 데이터베이스를 업데이트했습니다.

Sky ATP 가 모든 주니퍼 네트웍스 디바이스와 통신할 수 있도록 내장 커넥터를 사용하여 QFX 스위치에 엔드포인트 파티션을 분할하도록 지시하여 east-west 트래픽을 방지했습니다. 스위치가 필터를 생성하여 엔드포인트의 MAC 주소(00:0c:29:8d:9c:f8)와 패킷을 차단했습니다. 이 필터는 엔드포인트의 VLAN(4025)에 적용되었습니다.

그림 7. 자동화된 문제 해결



출처: Enterprise Strategy Group

엔드포인트가 네트워크에 통신할 수 없는 상태이며, 네트워크에 문제가 발생하여 장애를 겪는 사용자가 다른 이더넷 포트를 사용하려고 시도할 수 있다고 가정했습니다. ESG 에서는 가상화 서버를 사용하여 가상 네트워크를 전환하고 엔드포인트를 VLAN 4025 에서 VLAN 3025 로 이동하여 이러한 상황을 시뮬레이션했습니다. 전환하자마자 엔드포인트에 새 IP 주소가 부여되었고 내부 및 외부 모두에서 통신할 수 있었습니다.

약 5 분 후, 내부와 외부 모두에서 통신이 다시 차단되었습니다. Sky ATP 및 SRX 방화벽은 지속적으로 네트워크를 모니터링하고 MAC 주소를 통해 엔드포인트를 식별했습니다. 엔드포인트가 감염된 호스트 피드에 이미 있으므로 SRX 방화벽이 새 north-south 블록을 적용했습니다. 그리고 Sky ATP 는 QFX 스위치에 스테이트리스(Stateless) 방화벽을 업데이트하여 VLAN 3025 에 MAC 주소 블록을 적용하도록 지시했습니다.

이러한 기능이 중요한 이유

지속적인 사이버 보안 기술 부족에 직면한 조직은 광범위한 학습 곡선을 보여주는 복잡한 여러 제품에 투자할 여력이 없으므로 위협을 감지하고 예방하기 위해 상당한 노력과 수동 프로세스를 필요로 합니다.

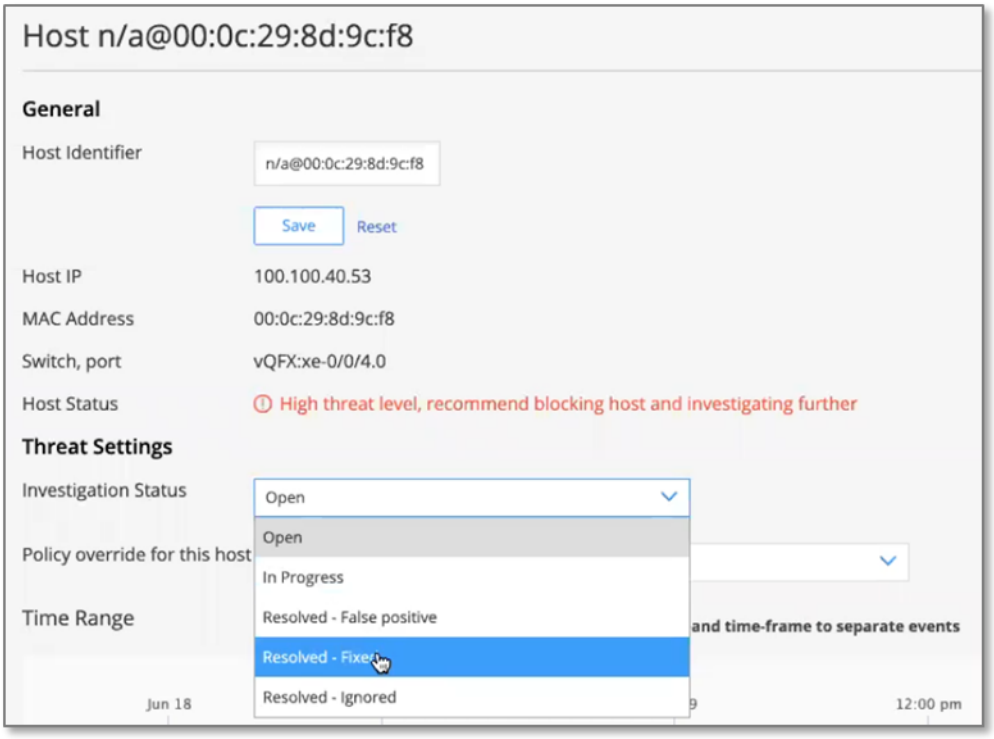
ESG 는 주니퍼 네트웍스 SRX 시리즈 방화벽이 멀웨어의 분석 및 탐지를 위해 다운로드한 파일을 Sky ATP 에 자동으로 전달했음을 확인했습니다. Sky ATP 에서 엔드포인트가 감염되었다고 확인하면 엔드포인트가 감염된 사이트 목록에 추가됩니다. 내장된 자동화 및 오케스트레이션으로 엔드포인트가 네트워크에서 분리되어 내부 및 외부 통신이 모두 차단되었습니다.

Sky ATP 및 SRX 시리즈 방화벽을 사용하면 조직이 사이버 공격을 최대한 신속하게 탐지하고 사이버 킬 체인의 진행을 중지하여 중요 자산을 보호하고 멀웨어 체류 시간을 단축할 수 있습니다.

관리 해결 및 대응

ESG 는 호스트에서 모든 멀웨어 파일을 제거하여 호스트의 바이러스를 제거하는 일반적인 보안 분석 워크플로를 시뮬레이션했습니다. 다음으로 Sky ATP 인터페이스를 사용하여 조사 상태를 변경해 문제를 종결로 표시했습니다. 호스트 모니터 섹션에서 호스트를 클릭합니다. 풀다운 메뉴를 사용하여 조사 상태에 대해 ***해결됨 – 수정됨***을 선택했습니다. 그림 8 과 같이 보안 분석가는 조사 상태를 ***시작됨***, ***진행 중***, ***해결됨 - 오탐****(false positive)*, ***해결됨 - 수정됨*** 또는 ***해결됨 - 무시***되도록 설정할 수 있습니다.

그림 8. 조사 상태 업데이트



출처: Enterprise Strategy Group

조사 상태를 '해결됨' 옵션 중 하나로 설정하면 시스템이 더 이상 감염된 상태가 아니며 네트워크에서 통신을 재개할 수 있음을 나타냅니다. Sky ATP 는 감염된 호스트 피드에서 시스템을 제거하고 SRX 방화벽과 QFX 스위치 모두 호스트에 대한 방화벽 항목을 제거합니다. 조사 상태를 해결됨 - 수정됨으로 설정한 직후에 엔드포인트가 내부 및 외부 모두에서 통신할 수 있다는 것을 발견했습니다.

이러한 기능이 중요한 이유

조직들이 점점 더 정교해지는 사이버 공격에 맞설 수 있도록, 보안 분석가들은 적시에 잠재적으로 손상된 시스템을 지속적으로 조사해야만 합니다. 통합, 자동화 및 오케스트레이션의 부족으로 인해 분석가들은 일상적인 반복 작업에 상당한 시간과 노력을 투자하고 있습니다.

ESG 는 보안 분석가가 조사를 종결된 것으로 표시하면 주니퍼 네트웍스 자동화가 모든 적절한 방화벽 및 스위치와 통신하여 네트워크 통신 블록을 제거하여 호스트가 내부 및 외부에서 통신할 수 있도록 하는 것을 확인했습니다. 따라서 분석가는 더 이상 업데이트해야 할 스위치 및 방화벽 세트를 수동으로 파악하여 각 디바이스에 로그인하고 규칙을 업데이트하고 새 구성을 저장하지 않아도 됩니다. 주니퍼 네트웍스 자동화는 보안 분석가 워크로드를 줄일 뿐만 아니라 인적 오류를 방지하는 데에도 도움이 됩니다.

거부할 수 없는 진실

사이버 보안 환경은 점점 복잡해질 뿐만 아니라 관리하기도 어려워지고 있는 추세입니다. 지적 재산, 고객 정보 및 재무 데이터의 손상 위험은 점차 증가하고 있으며, 이로 인해 금전적 처벌, 브랜드 및 회사 가치 평가에 대한 영향, 법적 조치 등 심각한 결과를 초래할 수 있습니다. 한편, 기업은 급증하는 보안 인시던트에 대해 조사하고 이에 대응해야 합니다. 새로운 시스템과 애플리케이션의 확산으로 보안 인시던트 시나리오가 늘어나고 있으며 향상된 탐지 툴이 더 많은 알림을 생성하고 있습니다. 2019 년에 사이버 보안 기술이 부족하다고 응답한 조직이 53%에 달해,[4] 2018 년의 51%보다 늘었습니다. 이에 따라 조직들은 효율성과 효과의 개선을 모색하고, 반복적인 작업 또는 수동 작업의 부담을 줄일 수 있는 자동화된 툴이나 자동화 가능한 툴로 전환하는 추세입니다.

주니퍼 네트웍스는 안티멀웨어 위협 방지를 위한 실시간 인텔리전스를 사용하여 사이버 보안을 자동화하도록 Sky ATP 를 설계했습니다. 이 SaaS 솔루션은 다양한 커넥터를 통해 SRX 시리즈 차세대 방화벽, 주니퍼 전체 제품군 및 타사 제품과 통합됩니다. Sky ATP 는 위협 인텔리전스, 안티바이러스 시그니처, 정적 및 동적 분석 및 머신 러닝과 기타 기술을 사용하여 위협을 자동으로 탐지하고 해결할 수 있습니다.

SRX 시리즈 차세대 방화벽은 분석을 위해 다운로드한 파일, 이메일 첨부 파일 및 기타 잠재적으로 악성 오브젝트를 Sky ATP 에 자동으로 전달합니다. 위협 탐지 시 SRX 방화벽은 Sky ATP, QFX 시리즈 스위치 및 기타 네트워크 디바이스와 연동되어 감염된 시스템을 네트워크에서 분리하여 자동으로 north-south 트래픽을 차단합니다. 멀웨어가 C&C 서버로 데이터를 유출하는 것을 방지하고, 자동으로 east-west 트래픽을 차단하여 내부망 확산을 방지합니다.

ESG 는 Sky ATP 가 구축, 구성 및 관리를 단순화했음을 검증했습니다. 네트워크 디바이스 모음과 같은 보안 패브릭을 정의할 수 있었습니다. 이를 통해 대규모 시스템 그룹을 제어하는 간단한 작업을 수행할 수 있었고, 이는 대규모의 복잡한 환경에 유용했습니다. 간결하고 단순한 사용자 인터페이스를 통해 보안 정책을 정의하는 작업을 가속화하고 간소화했습니다.

ESG 는 SRX 시리즈 방화벽이 악성 프로그램의 분석 및 탐지를 위해 의심스러운 오브젝트를 Sky ATP 에 자동으로 전달했음을 확인했습니다. 감염된 호스트(Sky ATP 로 분류됨)는 SRX 방화벽에 의해 네트워크에서 자동으로 연결이 끊겨 north-south 트래픽을 차단했습니다. 또한 Sky ATP 및 SRX 자동화는 QFX 스위치와 함께 작동하여 감염된 시스템을 east-west 트래픽에서 격리했습니다. 이러한 자동화는 멀웨어의 내부망 확산을 방지하고 C&C 서버와의 통신을 차단하는 데 도움이 되었습니다.

Sky ATP 는 감염된 호스트 조사 작업에 도움을 주어 감염, 근본 원인 및 수정 작업을 식별하는 데 필요한 정확한 정보를 제공합니다. 문제를 해결하고 조사를 해결한 것으로 표시하면 Sky ATP 및 SRX 방화벽이 자동으로 네트워크 연결을 복원하여 보안 분석가의 워크플로에서 또 다른 지루하고 복잡한 수동 프로세스를 제거합니다.

오류가 발생하기 쉬운 복잡한 수동 워크플로에서 벗어나 환경 전반에서 자동화 및 오케스트레이션을 활용하여 위협을 탐지하고 방지하고자 하는 조직의 경우 주니퍼 네트웍스 Sky ATP 및 SRX 시리즈 차세대 방화벽을 자세히 살펴보는 것이 좋습니다.

[4] 출처: ESG 조사 보고서, *2019 기술 지출 의향 설문조사*, 2019 년 2 월.

Enterprise Strategy Group 글로벌 IT 커뮤니티에 시장 인텔리전스와 실행 가능한 통찰력을 제공하는 IT 분석가, 연구, 검증 및 전략 회사입니다.

 www.esg-global.com

 contact@esg-global.com

 전화번호: 508.482.0188