데이터 인텔리전스의 혁신을 통한 Intel의 보안 태세 전환

개요

Intel의 기술이 기여한 사회적 영향과 중요성은 과대평가하기 힘들 것입니다. 이 회사가 지닌 엔지니어링 전문성은 수십억 개의 기기와 연결된 스마트 세상 속 인프라의 보안, 성능 및 연결을 지원합니다. 이와 마찬가지로, 조직의 가장 보호받는 자산으로서 보안 데이터가 갖는 중요성도 과대평가하기 어려울 것입니다.

Intel의 IT 팀은 Splunk®와 Apache Kafka를 토대로 자사가 정보 보안에 접근하는 방식을 다음과 같은 방법으로 변화시키고 있는 새로운 사이버 인텔리전스 플랫폼을 개발했습니다.

- 데이터 분석 속도를 높이고 지능형 위협을 발견하고 이에 대응하는 시간 단축
- 공통의 언어와 작업 인터페이스로 협업 조직 지원
- 보안 운영 및 시스템 상태 같은 추가 분야에서 비즈니스 가치를 실현하는 스트림 프로세싱 및 머신 러닝 도구 제공

데이터가 전부

Intel은 PC 위주 기업에서 데이터 위주 기업으로 변모했습니다. 이 회사는 혁신적인 방법으로 신제품을 개발하고, 새로운 시장에 진출하고, 새로운 고객과 교류하고 있습니다.

Intel의 최고정보보안책임자(CISO)인 Brent Conran은 이렇게 말합니다. “데이터가 전부고, 데이터가 왕입니다. 데이터는 저희의 비즈니스를 포함한 모든 것에 힘을 부여합니다. 또한 기존 산업과 클라우드에서 태어난 산업을 변화시키고 있습니다. 데이터에서 통찰력을 얻을 수 있는 능력에 따라 비즈니스의 성패가 좌우됩니다.”

이렇게 데이터가 중요해지고 데이터에 대한 의존도가 높아지자 Intel의 정보 보안(InfoSec) 조직은 포괄적인 ‘심층 방어(defense-in-depth)’ 전략을 수립하고 유지해야 했습니다. 이들은 예방 및 감지 도구를 경계, 네트워크, 엔드포인트, 애플리케이션 및 데이터 계층을 포함한 여러 수준에서 자동화하여 Intel 환경에서 발생하는 위협의 99%를 처리했습니다.

1퍼센트 추적

지능형 위협은 더 잦아지고 더 정교해지고 있습니다. 그리고 조직의 필요를 더 이상 충족하지 않은 레거시 SIEM은 조직의 부담이 되었습니다. 레거시 SIEM을 사용할 줄 아는 전문가는 몇 명밖에 없어 더 많은 유형의 데이터가 요구되는 현실에 대응하기 위한 확장이 불가능했습니다.

산업

- 기술

Splunk 이용 사례

- 보안
- 사이버 보안 사고 대응 관리
- 보안 모니터링
- 애플리케이션 모니터링

도전과제

- 데이터 위주 비즈니스 모델로 전환하자 데이터 가치가 높아졌지만 취약성도 증가함
- 레거시 SIEM은 더 이상 용도에 맞지 않음
- 여러 단절된 데이터 사일로와 팀에서 각기 다른 데이터 분석 해석 제공

비즈니스에 미치는 영향

- 정보 보안 관리 및 통제 변화
- 정교한 위협을 며칠 또는 몇 주가 아닌 몇 분 또는 몇 시간 만에 발견
- 협력적인 통일된 사이버 보안 관리 방식 실현
- Intel의 전체 InfoSec 조직을 위해 사이버 인텔리전스 플랫폼 제공

Splunk 제품

- Splunk Enterprise
- Splunk Enterprise Security
- Splunk ITSI(IT Service Intelligence)
- VictorOps
- Splunk Mission Control

Intel InfoSec은 조직 환경에 침투하려고 시도하는 정교한 위협을 감지할 전략이 필요했는데, Intel InfoSec에서는 이를 **1퍼센트 추적**이라고 합니다. 이 전략은 Splunk와 Apache Kafka 같은 최첨단 기술을 중심으로 한 **Intel의 사이버 인텔리전스 플랫폼(CIP)**으로 이어졌습니다. 새로운 CIP 플랫폼은 Intel® Xeon® Platinum 프로세서, Intel 3D NAND SSD(Solid State Drive) 및 Intel® Optane™ SSD 기반 고성능 서버를 사용하여 하루에 12테라바이트가 넘는 데이터를 수집하고 15페타바이트의 데이터를 저장합니다. 데이터는 수백 개의 원본에서 Kafka 메시지 버스로 흐른 후 Splunk 플랫폼으로 흘러 들어가고, 여기서 사용자는 일주일에 130만 번이 넘는 검색을 수행합니다.

InfoSec 조직은 이제 Splunk의 Data-to-Everything 플랫폼과 수백 가지의 타사 도구를 사용해 컨텍스트가 풍부한 가시성과 공통 작업 인터페이스를 갖게 되어 전체 InfoSec 조직의 효력을 개선합니다. 이들은 이제 위협을 감지하고 위협에 대응하는 시간을 이전의 몇 주 또는 몇 시간에서 몇 시간 또는 몇 분으로 단축했습니다.

Intel의 사이버 인텔리전스 플랫폼(CIP) 확장

CIP의 성과는 추가 데이터 원본과 새로운 이용 사례, 더 많은 데이터 모델로 이어졌습니다. 곧 CIP가 취약점 관리, 컴플라이언스 및 집행, 리스크 관리 팀 등으로 확장됨에 따라, 인프라에는 더 많은 것이 요구되고 더욱 빠른 컴퓨팅과 스토리지가 필요해졌습니다. Intel의 보안 솔루션 설계사 및 엔지니어들은 플랫폼 성능을 극대화하기 위해 Splunk 플랫폼과 Intel 기술에 대한 더 깊은 지식이 필요했습니다.

Splunk와 Intel의 협업 팀은 최신 Intel 제품 및 기술을 사용하여 CIP의 컴퓨팅, 메모리 및 스토리지 확장 지침이 될 수 있는 공동 **기준 구성**을 개발했습니다. 이제 Splunk와 Intel은 동료 IT 기업들에게 자신의 성공 사례를 공유하면서 그들이 Splunk 및 Apache Kafka 배포를 확장하여 원시 데이터를 운영, 비즈니스 및 보안 인텔리전스로 더욱 효과적으로 전환할 수 있도록 지원하고 있습니다.

"Splunk는 잠재력을 지니고 있습니다. 그렇기 때문에 저희는 Splunk에 시간과 노력, 자원을 투자하고 있어요. Splunk가 업무 수행에 도움이 될 것이라고 생각하기 때문에 Splunk가 성공하길 바랍니다."

— Brent Conran, CISO(최고정보보안책임자), Intel

오늘과 미래를 위한 가치 제공

Intel의 InfoSec 팀은 Splunk와 Kafka의 사용 범위를 넓히고 있습니다. 애널리스트와 데이터 과학자들은 데이터를 스트림 안에서 변환, 보강, 조인, 필터링 및 운영하고 있습니다. 이들은 사고 대응, 운영 및 시스템 상태부터 워크플로 오케스트레이션 및 경고에 이르는 모든 분야에 머신 러닝 도구를 추가하기도 합니다. Intel은 Splunk와 협업하여 오늘과 미래를 위한 가치를 극대화하고 있습니다.

Conran은 다음과 같이 말합니다. "Intel InfoSec은 어느 때보다도 민첩해졌습니다. 완전히 새로운 Splunk 데이터 레이크를 도입했고, 도구를 현대화했습니다. 데이터를 적합한 곳에 투입하고 팀원들에게 새로운 기술을 가르침으로써 능력을 배가시키기도 했습니다. 저희는 머신 러닝을 이용하여 사이버 인텔리전스의 깊이와 속도를 크게 향상시키고 있습니다."

"CIP는 하루에 수십에서 수백 테라바이트의 데이터를 처리하고 임시 검색, 예약된 검색, 데이터 모델 가속 및 머신 러닝 모델을 만드는 수백 명의 사용자를 지원하도록 구축되었습니다. 성능을 대규모로 확장하려면 고성능 컴퓨팅 및 스토리지를 위해 Intel의 Xeon Scalable 프로세서와 Intel SSD에 기반한 서버가 필요했습니다. 'Intel이 안전하고 빠르게 작동'할 수 있게 만들려면 단 몇 초도 중요하니까요."

— Jac Noel, 보안 솔루션 설계사, Intel

Splunk를 무료로 다운로드 하거나 **무료 클라우드 평가판**으로 시작하십시오. Splunk 배포 모델은 클라우드, 사내 환경, 대규모 또는 소규모 팀 등 모든 환경의 요구사항을 충족합니다.

2020-Splunk-RET-Intel-101-CS