안녕하세요. 스플렁크 코리아입니다.

지난 4 월 22 일 스플렁크는 토크아이티 플랫폼에서 SIEM 글로벌 No.1 Splunk - "모니터링부터 SoC 자동화까지, Splunk SoC Suite 으로 스윗하게 해결해드립니다." 라는 제목으로 스플렁크 웨비나 방송이 진행되었습니다. 스플렁크의 주요 솔루션인 SIEM 의 특징과 사용 사례, 2020 스플렁크 SIEM 솔루션 업데이트 사항에 대해 설명드렸습니다.

4 월 22 일 토크웨비나 방송 중 진행된 실시간 Q&A 답변을 정리하여 드리니, 업무에 참고하여 도움 되시길 바랍니다

[질문] 스플렁크 제품을 모니터링 솔루션용도로 사용하는곳도 있는듯한데 어느 정도 범위까지 모니터링이 가능할까요?

[답변] Timestamp 를 가지는 시계열 이벤트 데이터라면, 데이터의 형식과 수집 프로토콜에 제약없이 수집하고 모니터링할 수 있습니다. 보안 운영 이외에도 ITOps, 비지니스 분석, 고객 분석 등 다양한 형태의 모니터링/분석 유즈케이스가 있습니다.

[질문] 스플렁크의 장점이 유연하게 대시보드 구현이 가능한 것인데, 보안의 경우 보안관제 서비스에 정형화된 부분도 직접 구현을 해야 하는 건가요? 아니면 보안에 특화된 Contents PACK 이 별도로 있는지 궁금합니다.

[답변] 알고 계신것처럼 유연하게 원하는 대시보드를 마음대로 만들수있는 장점과 더불어서 Enterprise Security 라는 프리미엄 앱을 이용하면 빌트인 되어있는 보안 업무 플로우를 활용할 수 있습니다. ES Contents Update 를 이용해서 최근 유행하는 공격에 대한 Analytic Story 를 피드 받아서 우리 환경에 적용하는 것도 가능합니다.

[질문] Splunk 에서 강화학습에 대한 분석 예는 없는지요? (가능한지요?)

[답변] Splunk 에서 머신러닝을 활용하는 방법으로는, MLTK(Machine Learning Toolkit)과 DLTK(Deep Learning Toolkit) 등의 각종 툴킷에서 제공되는 알고리즘이나 커스텀 알고리즘을 이용해서 내가 원하는 방식으로 적용하는 방법이 있고, 그 외에 머신러닝 기능이 보안 업무 플로우로 활용할 수 있도록 구현되어있는 ES 나 UBA 와 같은 완제품 형태를 활용하는 방법이 있습니다. 강화학습은 아직 완제품 형태로 제공되고 있지는 않습니다.

[질문] 스플렁크에 대량의 데이터가 저장될텐데, 라이센스 정책은 용량 대비인 가요?

[답변] 전통적으로 스플렁크 라이센스는 하루에 수집하는 데이터 총량 기준으로 책정됩니다. 최근에는 vCPU 기반으로 라이센스를 측정하는 방법 등도 추가 되었습니다.

[질문] vCPU 기반으로 라이센스를 측정 부분에 대해 상세 설명 부탁드려요.

vCPU 기반 라이센스 측정 방식은 "infrastructure-based pricing"이라는 이름으로 제공되는 새로운 라이센싱 방식입니다. 기존과 같은 1 일 수집량과 관계없이 Splunk 의 indexer, search head 등의 splunk instance 들이 사용하는 총 vCPU 개수를 기준으로 라이센스를 부과하는 방식입니다. 데이터 수집량은 엄청나게 많지만 이 데이터에 대한 검색 빈도가 낮거나 활용가치가 낮은 경우, 기존과 같은 수집량 기준 라이선싱은 상당한 부담이 될 수 있기 때문에 이러한 경우 infrastructure-based pricing 을 통해서 도입 부담을 낮출 수 있습니다. 자세한 사항은 담당 영업 대표 또는 스플렁크 코리아 대표번호(02-6007-2003)을 통해 연락주시면 상세히 답변 드리겠습니다.

[질문] 사진을 가지고도 분석가능 한가요? 혹, 사례도 있나요 ?

[답변] Splunk 텍스트로 된 데이터를 저장 분석하는 엔진으로 사진과 같은 binary 데이터는 인덱싱 범위에 포함되지 않습니다.

[질문] 모니터링의 데이터를 외부 open api 로 받아서 별도의 시스템에서 받아 조회할 수 있는 기능을 제공하나요?

[답변] Splunk 가 제공하는 REST API 및 각 언어별 SDK 를 사용하면 외부 시스템에서 Splunk 에 저장되어 있는 데이터를 연동해서 사용할 수 있습니다. REST API 와 SDK 사용에 대한 상세한 내용은 dev.splunk.com 에 자세히 안내되어 있습니다. 데이터 시각화와 분석, 알람 등이 목표라면, 스플렁크에서 제공하는 유연한 검색 언어인 SPL 및 대시보드, 앱 체계를 이용하면 빠르고 간단하게 이용하실 수 있으며, 추후 요구사항 변경에도 신속히 대응할 수 있습니다.

[질문] ES 와 UBA 의 full word 는 뭔가요?

[답변] ES 는 Enterprise Security 이며, SIEM 솔루션입니다. UBA 는 User Behavior Analysis 입니다.

[질문] Splunk 를 통해 로그를 수집하고, ML 학습이 중요한데, 학습을 위해서는 우선적으로 로그가 중요할것 같습니다. 필수적/중요 로그가 정의 되어 있나요?

[답변] UBA 는 제품이 동작하기 위해서 필수로 필요한 데이터 종류 리스트가 있고, 추가로 분석에 도움이되는 데이터 종류 리스트가 있습니다. 수집하는 데이터 소스 종류별 적용 가능한 유즈케이스가 정리되어 있습니다.

[질문] 수집된 로그에 대한 백업도 하나요? 그리고 오탐률은 어느 정도인지?

[답변] Splunk 에 데이터를 저장하는 ES(Enterprise Security)의 경우, 보통 데이터량이 많기 때문에 백업 보다는 주로 Clustering 기술을 통해서 장애 대응을 하는 경우가 많습니다. UBA 의 경우에는 원본 데이터를 저장하지 않고 탐지된 어노말리와 위협 정보만 보관하게 됩니다. UBA 제품은 단독으로 사용할 수 도 있고 ES 와 함께 사용하여 원본데이터를 이용한 사후 분석을 수행할 수 도 있습니다.

[질문] 빅데이터 기반 사고조사 분석 체계구축이 가능한가요?

[답변] 네, 맞습니다. 특히 Splunk ES (Enterprise Security)는 기업내의 다양한 보안 관련 데이터를 한곳에 수집하고 분석에 활용할 수 있기 때문에, 탐지 뿐만 아니라 자동 조치, 사고 조사까지도 하나의 플랫폼에서 수행할 수 있습니다.

[질문] 구매한 라이센스에 비해 일일 데이터 수집량이 많은 경우, 초과된 데이터 분량에 대해서는 어떻게 처리되나요?

[답변] 1 일 수집량이 보유 라이센스를 초과 하더라도 수집을 제한하지 않습니다. 모두 인덱싱 됩니다.

[질문] 스플렁크의 SIEM 플랫폼에 팬텀의 보안운영 자동화와 분석 플랫폼이 추가되었는데, SOAR 를 통해 GDPR 도 지원 가능한가요?

[답변] GDPR 은 특정제품 도입으로 충족된다기보다는 조직 전반의 보안 Practice 이기 때문에 약간 다른 측면에서 바라보아야 할 것 같습니다. Splunk 를 이용하여 GDPR Compliance 준수 여부를 모니터링 할 수 있으며 Professional Service 를 통해 GDPR 모니터링 체계 구축에 도움을 받으실 수 있습니다.

[질문] 스플렁크도 하둡처럼 수집된 데이터를 master-slave 로 구성 및 복제 할수 있나요?

[답변] 스플렁크의 클러스터링 기능을 활성화 하면 수집 데이터를 여러 노드에 자동 복제 분산할 수 있습니다.

[질문] 혹시 가능하다면, 국내에서 가장 잘 구축된 혹은 규모가 큰 레퍼런스를 알수 있을까요?

[답변] 고객사 명을 공유하기는 어렵습니다만, 국내 보안 usecase 로는 1 일 수집량 기준 8~10TB 규모의 고객이 있습니다. 해외의 경우, 1 일 300TB 이상 수집하는 고객도 많고, 최대 7PB 까지 데이터를 수집하는 고객도 있습니다.

[질문] 데이터 용량이 초기 사이징했던 것 보다 커졌을때 스플렁크 서버의 용량을 늘리는 작업은 어떤식으로 되나요? 노드를 추가하는 방식 등의 scale out 방식을 지원하나요?

[답변] 네, scale out 하실 수 있습니다. 데이터를 저장하는 인덱서 클러스터의 경우 간단히 노드를 추가하실 수 있고, 필요시 기존 데이터를 리밸런싱 할 수 있습니다. 검색 및 대시보드 기능을 제공하는 검색헤드의 경우에도 클러스터링 기능을 제공하며, 기존 클러스터에 중단 없이 노드를 추가하여 검색 성능을 확장할 수 있습니다.

[질문] 새로운 용어들이 너무 많이 쏟아져 나와서 단어만 주워 담기에도 버겁네요ㅠ

[답변] 한글화된 자료는 아니지만, 스플렁크 솔루션 용어를 확인 하실 수 있는 스플렉시콘 Splexicon page 페이지를 안내해드립니다.

[질문] 방금 시연의 피싱메일 식별기능은 Fireeye 의 eMPS 와 비교시 어떤 차별화 전략이 있나요?

[답변] eMPS 는 악성코드 방지 시스템으로, 전체적인 보안 관제 체계 상에서 하나의 보안 장비로 생각할 수 있겠습니다. 피싱 메일이 탐지되면 그에 따른 일련의 대응 작업들을 수행해야 하는데, 이 일들을 SIEM 인 Splunk ES 와 SOAR 솔루션인 Phantom 을 연계하여 자동화하여 처리할 수 있다고 보실 수 있습니다.

[질문] 내부정보유출 관점에서 Splunk 를 적용한 사례에 대해서 간단히 소개해 주실 수 있을까요?

[답변] Nasdaq 이나 Heartland 등의 고객이 UBA 를 사용하여 내부 이상징후를 탐지하고 있습니다. 일례로, 나스닥은 스플렁크 UBA 를 통해 IT 시스템에 대한 로그인 데이터와 건물 액세스 데이터 및 HR 데이터를 상호 연관시키는 방식으로 직원들이 긴 휴가 기간 동안 시스템이나 건물에 액세스에 관련 규정을 위반하는 지 여부를 확인합니다. 이외에도 나스닥은 스플렁크 UBA 를 활용하여 애널리스트들의 조사 수행 능력의 효율성 수준 또한 50%이상 향상되었다고 밝혔습니다.

[질문] 시연으로도 나올지 모르지만, 문제해결을 위해서는 로그의 시계열분석이 중요한데 어떻게 지원되는지 간략히 소개 바랍니다.

[답변] Timestamp 를 가지는 시계열 이벤트 데이터라면, 데이터의 형식과 수집 프로토콜에 제약없이 수집하고 모니터링할 수 있습니다. 이렇게 수집된 데이터가 탐지 및 분석 대응 단계에서 다양한 drill down 및 대시보드로 유기적으로 연결되어 사용될 수 있습니다. 시간이 되신다면 Splunk ES (Enterprise Security) Hands-on 워크샵 또는 Threat hunting 워크샵에 참석하셔서 보다 자세한 정보를 얻으시기를 추천드립니다.

[질문] Splunk 버전 6.5.3 에 Enterprise Security 앱버전 4.7.4 를 사용중입니다. 기존 스플렁크 제공 시나리오는 국내 보안 장비 로그로 적용 시 오탐이 많아, Correlation Search 를 별도로 만들어 notable 이벤트로 인시던트화 하여 사용 중입니다. 대시보드도 웹으로 별도로 개발 적용했습니다. UBA 와 SOAR 등을 적용하려면 Splunk 버전 이나 Enterprise Security 앱도 업데이트를 해야 하는건지요? UBA 와 SOAR 적용시에도 커스터마이징이 많이 필요할까요 ?

[답변] 안정적인 호환을 위해 업데이트를 권고 드립니다. UBA 의 경우에는 제품에 포함되어 제공되는 Security Model 을 적용하는 경우 별도의 웹 개발 커스터마이징은 필요하지 않습니다. Phantom 의 경우, 자동화된 워크플로우 구성을 위해 보유하신 보안 장비들과 연동이 필요할 수 있습니다. 잘 알려진 보안 장비의 경우에는 Splunk Phantom app store 를 통해서 재사용할 수 있는 모듈이 공유되고 있어 개발 노력을 절약할 수 있습니다.