splunk> turn data into doing™

Splunk 의 SaaS 구축 이점

[질문] 경쟁사들은 보안 또는 특정 분야의 서비스만 제공하지만 스플렁크는 **모든** 영역을 종합적으로 서비스한다고 들었는데, 위협을 실시간 분석 및 분석 내용을 시각화/ 대시보드화가 가능한지요? 이런 작업을 수행할 때 기존 H/W 장비에 영향을 미치지는 않은지요?
[답변] 네. 오늘의 주제인 클라우드 보안, 특히 멀티클라우드 환경을 대응하는 부분은 기존의 레가시 SIEM 솔루션으로는 많은 한계가 있습니다. 스플렁크는 탁월한 유연성으로 이러한 환경변화에 아주 빠르게 대응해가고 있습니다. 기존 서비스 장비나 보안 H/W 장비의 성능에 영향을 주지않고 스플렁크에 수집된 빅데이터를 분석하여 보안 대응 업무 및 분석 업무를 수행하실 수 있습니다.

[질문] 조사, 실시간 모니터링 작업이 다른 애플리케이션의 Performance 에 영향을 주는 정도는 어떤가요, **타사 솔루션 대비** 경쟁력이 있을까요?
[답변] 스플렁크는 클라우드 환경이든 온프레미스 환경이든 관계없이 대용량 데이터를 Splunk 의 인덱서 서버에 저장하여 탐지 및 분석 업무를 수행하는 구조입니다. 대상 애플리케이션의 성능에는 영향을 주지 않고 다양한 분석을 수행하실 수 있습니다.

[질문] SIEM 은 예전부터 있던 보안 정보 및 이벤트 관리 솔루션으로 알고 있습니다. 가장 중요한 건 내,외부위협탐지가 실시간으로 다양해지고, 관련 데이터를 처리에 문제가 많아 사실 **범용성**이 매우 좁았다고 생각됩니다. 위협 탐지에 대한 성능이 많이 개선되었을까요?
[답변] 기존 SIEM 은 보안이벤트를 관리하기 위한 목적으로 대용량의 데이터를 다루기에는 한계가 분명합니다. Splunk 는 빅데이터 플랫폼에서 대량의 데이터를 처리하기에 적합합니다. 진보된 위협 공격을 탐지하기 위해서는 보안이벤트 뿐만 아니라 비보안 로그(DNS, OS Event, Network Flow 등)의 분석이 함께 수반되어야 합니다. 스플렁크가 가진 유연성과 확장성으로 성능을 개선할 수 있습니다.

[질문] 기존 온프라미스 시스템의 년 수 경과로 개편 업그레이드를 검토 중입니다. 기업의 **보안핵심업무를 SaaS 로 구축**함이 어떻게 가능하게 보장해주는지 와 클라우드가 기존 **온프라미스 대비 투자효과는** 어떻게 되는 가요?
[답변] 네, 말씀하신것처럼 Splunk Cloud 라고 하는 SaaS 서비스를 이용하여 SIEM 을 구성하실 수 있습니다. SaaS 환경에서의 SIEM 이 가능하게 하기 위하여, 스플렁크에서는 SOC2 등 다양한 보안 **인증**을 받고 있습니다. 해당 페이지의 19. CSA proof of compliance 부분을 참고하시기 바랍니다. 클라우드가 기존 온프라미스 대비 효과로 대표적인 것은, 운영 비용 절감 및 관제 업무에 집중할 수 있다는 점이 대표적일 것 같습니다.

[질문] Splunk 를 멀티 클라우드에 적용할 경우에 장점을 알려주세요. AWS 쓰고 있는데 추천해 주실 수 있는 클라우드가 있나요? 보안 이슈는 없나요?
[답변] 멀티클라우드 사용시 가장 큰 이슈 중 하나가 가시성 확보가 어렵다는 문제입니다. Splunk 를 사용하면 멀티클라우드의 보안위협과 워크로드의 상태를 단일 플랫폼에서, 손쉽게 확인할 수 있습니다. 클라우드 제공업체(CSP) 선정 시, 사용하게 될 IaaS, PaaS 등의 서비스에 회사가 가지고 있는 컴플라이언스를 적용하기위한 보안적 서비스가 적용가능한지 확인하는 것이 필수 입니다. 예) MFA(다중인증)

[질문] 기존 인프라에 용도별 보안 장비들을 Splunk 의 SIEM 이나, Splunk Security Essential 앱이나 Splunk Contents Update 앱, Splunk UBA 으로 기존 인프라 전체를 통합 관리할 수 있는 것인가요? 3 가지를 다 구매하려면 **비용**이 많이 들 것 같은데 좋은 방안을 부탁드립니다.
[답변] Splunk SIEM 인 Splunk Enterprise Security 부터 고려하시는 것이 좋을 것 같습니다. Splunk Security Essential 앱이나, Splunk ES Contents Update 앱은 무료로 제공되는 앱입니다. Splunk UBA 는 SIEM 을 구축한 이후에

ML 을 이용한 탐지에 관심이 있는 고객들만 고려하는 솔루션으로, 먼저 SIEM 도입 이후에 검토하시어도 괜찮을 것 같습니다.

[질문] Splunk 를 온프레미스에서 클라우드(단일,멀티,하이브리드)에 도입하기 위한 사전 작업과 관리 운영에서의 유의할 점에 대해 문의합니다. 클라우드에서 온프레미스로 **다시 전환**할 경우에도 어떤 유의할 점들이 있을지요?
[답변] Splunk 는 Cloud 로 마이그레이션 하는 데 유용한 툴을 제공하고 있습니다. 또한 성공적인 클라우드 마이그레이션을 위한 문서들을 제공하고 있습니다. 내용을 참고하시기 바랍니다.

[질문] Cloud 서비스 사업자들이 이종 장비와 이종 플랫폼을 사용하고 또 업그레이드를 지속적으로 하는데 이에 대한 **빠른 대응**이 가능한가요? 최소 대응 시간이 필요할텐데 어느 정도 예상하시나요?
[답변] CSP 와의 파트너쉽 등을 통해 빠른 대응이 가능할 것으로 보이며 대응 시간을 예상하기는 어렵습니다. 다만 Cloud 서비스의 업그레이드와 별개로 데이터를 가져오는 서비스 자체의 변동은 거의 없으므로 Splunk 와 연계하여 데이터를 분석하는 업무에는 영향이 거의 없을 것으로 예상됩니다.

[질문] 혹시 **국내 클라우드** 예를 들면, KT 클라우드도 지원이 가능한가요?
[답변] 어느 클라우드이든 관계없이 호스트의 보안 데이터를 수집하고 CIM 으로 표준화 하면 Splunk ES 에 연동하여 사용하실 수 있습니다. 다만 AWS, Azure, GCP 등의 경우에는 각 클라우드가 제공하는 데이터 제공 방식 별로 연동 모듈이 이미 만들어져 있습니다만, KT 클라우드는 아직 연동 모듈이 준비되지 않고 있습니다

머신 러닝/AI

[질문] 요즘 보안/관제에 AI 기술이 많이 사용되고 있는 것으로 알고 있는데 **AI** 가 사용되고 있나요? 어떤 부분에서 사용되고 있는지?
[답변] Splunk 의 SIEM 솔루션인 Enterprise Security 에서는 대표적으로 탐지 룰에 사용되는 임계치를 machine learning 기법을 이용하여 서버 별, user 별 자동으로 설정되도록 하는 기법이 있습니다. 또한 ML 을 적용할 수 있는 다양한 시나리오들을 Splunk Security Essential 앱이나 Splunk Contents Update 앱을 통하여 지속적으로 업데이트하여 제공됩니다. 또, 머신 러닝 기반으로 만들어진 Splunk UBA 라는 제품은 룰 기반이 아닌 머신러닝기반의 이상행위 탐지가 가능한 솔루션입니다.

[질문] Splunk 로 수집한 데이터들을 외부 오픈소스 **ML 플랫폼**이나 외부 데이터분석 클라우드 서비스와 연계할 수도 있을까요?
[답변] 네 당연히 가능합니다. Splunk 가 제공하는 다양한 API 들을 이용해서 데이터 레벨의 연계가 가능하고, 외부 플랫폼이 제공하는 로직을 custom command 등으로 만들어서 Splunk 내에서 사용하실 수도 있습니다.

[질문] Splunk 에서의 **오탐을 방지하는** 기술과 오탐율을 낮추기 위한 방안은 어떤 것일지요?
[답변] Rule 을 어떻게 만드는지, 어떻게 운영 하는지에 따라 오탐의 양상은 상당히 다를 수 있다고 생각됩니다. 오탐을 줄이기위한 하나의 방법으로, 통계 및 ML 기법을 활용하여 dynamic thresholding 기법을 적용하시는 고객도 있습니다. 특정 방법이 모든 경우의 오탐을 줄여줄 수 있다기 보다는 지속적은 탐지룰의 튜닝이 전제되어야 할 부분이라 생각됩니다.

레퍼런스

[질문] Splunk 를 최적화하여 적용한 전자상거래 업체 **레퍼런스**가 있는지 문의 드립니다.

[답변] 다양한 전자 상거래 고객을 보유하고 있습니다. 최근 국내의 top tier 전자상거래 C 업체 또한 클라우드에서 운영되는 자사의 서비스 인프라를 보안 위협으로부터 보호하기 위하여 Splunk 를 도입하였습니다.

[질문] Splunk 온프레미스 국내 적용 사례 중 특히 **금융권 적용 케이스**에 대한 구체적인 소개 부탁 드립니다.
[답변] 스플렁크는 은행, 보험, 증권 등 다양한 레퍼런스를 보유하고 있으며 FDS(이상거래 탐지 시스템) 및 내부 정보 유출 방지, 비지니스 분석, IT 모니터링 등 다양한 용도로 활용되고 있습니다.

기타

[질문] 많은 공공기관이나 **금융기업**들이 망분리를 운영하고 있습니다. 인터넷이 연결 안되는 **폐쇄망**이나 사설망에서도 구성이 가능한가요?
[답변] 네 망분리 환경에서 SIEM 을 운용해야 하는 전세계의 많은 금융권, 정부부처, 군 고객분들이 Splunk 를 SIEM 으로 활용하시고 있습니다. 다만, 이경우에는 클라우드가 아니고 온프레미스로 설치하여 활용하십니다.

[질문] Splunk 에서는 구체적으로 어떤 다양한 **이중인증**으로 인증 보안을 지원하는지 설명 부탁드립니다.
[답변] Splunk Enterprise Security 웹 로그인 시 Duo Security, RSA 이중인증 솔루션과 연동됩니다. 해당 문서를 참고하시기 바랍니다.

[질문] 스플렁크 솔루션을 온프레미스로 설치하는 경우 특정 **장비 Spec** 이 따로 정해져 있나요?
[답변] 네, 맞습니다. 추천 장비 스펙이 있습니다. 일반적으로는 해당 페이지에서 추천하고 있는 minimum requirement 스펙을 충족하면 되는데, SIEM 구성환경은 고객별로 상이하여 고객 상황에 따라서 저희 컨설턴트가 적절한 사양을 추천 드리고 있습니다.

[질문] **팬텀**에서 지원하는 국산 보안솔루션 리스트들이 있을까요?
[답변] 해당 페이지를 확인하시면 지원되는 전체 장비 리스트를 보실 수 있습니다. 외산 장비들과는 다르게, 국산 보안 장비들의 경우에는 아직까지는 프로젝트 내에서 상황에 맞게 연동을 구현하는 경우가 많습니다. 대부분의 국산장비들이 아직 API 를 공개하지 않는 경우가 많고, 버전이 올라가는 경우 API 의 일관성이 유지되지 않는 등의 문제가 여전히 상존하고 있습니다. 앞으로 국산 보안 장비 시장의 문화도 조금 더 성숙해지기를 기대하고 있습니다.