CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

아젠다

*아젠다는 주최측 사정에 따라 변경될 수 있습니다.

시간	세션 주제		
09:00- 10:00	등록		
10:00-10:10	환영사		
10:10-10:40	기조연설: Trend Micro 클라우드 위험이 곧 비즈니스 위험입니다.		
10:40-11:10	기조연설: 아마존웹서비스 보안담당자를 위한 GenAI 보안 전략		
11:10-11:30	전시부스 관람		
11:30-12:00	기조연설: 한국인터넷진흥원(KISA) 사이버침해대응본부 침해대응단 최근 침해사고 동향 및 대응방안		
12:00-12:30	기조연설: 메가존클라우드 개방형 보안 체계(OCSF)를 통한 Amazon Security Lake 보안 이벤트 대시보드 구현 방안		
12:30-13:30	점심식사		
	트랙 1	**트랙 2**	**트랙 3**
13:30 - 14:00	트렌드마이크로 클라우드 공격 표면 위험 관리 및 네이티브 애플리케이션 보안	LG CNS '23년 사이버보안 3가지 주요 이슈와 대응 방안	아카마이 API보안에 대한 이해와 방안
14:00 - 14:30	퀘스트소프트웨어 하이브리드 AD환경에서의 침해 진단, 탐지부터 복구까지 한번에 이해하기	트렌드마이크로 Unified Cyber Security Platform: EDR, XDR 및 Attack Surface Risk Management의 상호 보완적 통합 전략	진앤현 시큐리티 위험관리 프로세스 자동화 방안
14:30 - 15:00	SK쉴더스 Cloud 보안 트렌드 – CNAPP (Cloud Native Application Protection Platform)	스플렁크 멀티 클라우드 환경의 통합 보안 관제 및 자동화 전략	오픈텍스트 오픈소스 라이브러리 방화벽을 통한 취약점 탐지/수정 한계성 극복
15:00 - 15:30	전시 부스 관람		
15:30 - 16:00	태니엄 운영의 완벽을 완성하는 Tanium의 위력	트렌드마이크로 제로 트러스트를 통한 보안 환경 지속성- 단계별 제로 트러스트 적용 모델 가이드	라드웨어 대규모 애플리케이션 디도스 공격과 대응 방법
16:00-16:30	사이버아크 클라우드 보안은 아이덴티티관리부터 시작합니다	소프트캠프 경계 없는 업무 환경에서 문서 보안 오케스트레이션 - 제로 트러스트 모델의 적용	스카이하이 시큐리티 ChatGPT와 같은 Shadow IT에 대한 가시성 확보 및 제어 방안
16:30	맺음말 | 경품추첨		

CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

아젠다 - 기조연설

*아젠다는 주최측 사정에 따라 변경될 수 있습니다.

시간	세션 주제	세션 소개
09:00- 10:00	등록	
10:00-10:10	환영사	
10:10-10:40	기조연설: Trend Micro 클라우드 위험이 곧 비즈니스 위험입니다.	오랫동안 클라우드 보안은 기업 보안과 별개였지만, 최신 위협으로부터 조직을 성공적으로 방어하려면 사일로를 제거하고 클라우드 보안을 포함하여 전체 위험 표면을 하나로 관리해야 합니다. 새로운 위협에 대해 살펴보고, 보안에 대한 결합된 접근 방식을 통해 향후 위협에 대한 탄력성을 어떻게 높일 수 있는지 소개합니다.
10:40-11:10	기조연설: 아마존웹서비스 보안담당자를 위한 GenAI 보안 전략	GenAI 서비스를 위한 Foundation Model(이하 "FM") 을 Fine Tuning 하거나 새로운 FM 을 개발하려고 하는 경우, 조직에서는 방대한 데이터에 대한 안전한 처리가 엄수되어야 합니다. 그리고 이를 위해서는 AI 관련 서비스 개발 환경을 효율성을 유지하면서도 안전하게 구성할 수 있는 방안이 전제되어야 합니다. 이번 세션에서는 AWS 환경에서 데이터 엔지니어와 데이터 분석가의 업무 효율을 저해하지 않으면서 보다 안전하게 데이터를 처리하고 새로운 GenAI 기반 서비스를 개발/런칭할 수 있는지 보안담당자의 관점에서 살펴보도록 하겠습니다.
11:10-11:30	전시부스 관람	
11:30-12:00	기조연설: 한국인터넷진흥원(KISA) 사이버침해대응본부 침해대응단 최근 침해사고 동향 및 대응방안	최근 국내에서 발생하는 주요 침해사고 사례를 통하여 사이버 공격 유형을 살펴보고, 그에 따른 대응 방안을 제시합니다. 더불어 급속히 확산되고 있는 클라우드 환경에서의 주요 침해사고 사례를 살펴보고 클라우드 이용기업이 이러한 공격위협에 어떻게 대응해야할지 방안을 제시하고자 합니다.
12:00-12:30	기조연설: 메가존클라우드 개방형 보안 체계(OCSF)를 통한 Amazon Security Lake 보안 이벤트 대시보드 구현 방안	Amazon Security Lake(ASL)는 클라우드와 온프레미스에서 발생하는 다양한 보안 로그와 이벤트 등의 소스 데이터를 개방형 사이버보안 표준 체계인 OCSF(Open Cybersecurity Scheme Framework)를 통해 정규화하고 중앙화하여 보안 가시성을 높이고 위협에 대응할 수 있는 환경을 구축할 수 있게 해줍니다. 메가존클라우드는 ASL의 국내 첫 공인 서비스 파트너로서, 고가의 SIEM을 도입하기 어려운 고객사들을 위해 ASL 환경을 설계하고 AWS 네이티브 보안 서비스와 Trend Micro를 포함한 다양한 3rd Party 보안 ISV 솔루션들을 ASL에 연결해 보안위협 탐지체계를 구축하도록 지원합니다.

CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

아젠다 – 트랙 1

시간	세션 주제	세션 소개
13:30 - 14:00	트렌드마이크로 클라우드 공격 표면 위험 관리 및 네이티브 애플리케이션 보안	클라우드 자산이 증가하고 클라우드 플랫폼 및 서비스가 다양해지면서 사용자 요구사항에 필요한 개발/운영 툴을 사용하는데 있어 보안 위협 요소들 또한 다양하고 공격 표면이 증가하고 있습니다. 트렌드마이크로에서는 클라우드 자산 가시성을 통한 위험 관리를 용이하게 하고 클라우드 워크로드와 네이티브 애플리케이션, 리소스를 보호하는 솔루션을 통해 탐지되는 위협들에 대한 위험성 평가와 상관관계 분석을 통한 공격 경위 및 흐름을 파악하여 최적의 관리 및 대응을 제공해 드리고 있습니다.
14:00 - 14:30	퀘스트소프트웨어 하이브리드 AD환경에서의 침해 진단, 탐지부터 복구까지 한번에 이해하기	M365환경은 대부분 하이브리드 환경으로 구성되어 있습니다. 이러한 하이브리드 환경은 온프레미스와 클라우드 환경이 연결되어 있어 보다 높은 수준의 온프레미스 환경 보안과 클라우드에 특화된 보안을 필요로 하게 됩니다. 퀘스트에서는 하이브리드 AD환경에서 고려되어야 할 핵심적인 보안을 소개하고 퀘스트의 솔루션을 통해서 어떻게 이러한 보안위협들을 진단하여 사전에 위협을 제거하고, 실시간으로 탐지하여 대응할 수 있는지 소개해 드립니다. 또한 위협 발생후에 비즈니스 연속성 측면에서 빠르고 정확한 복구 체계 구축을 위한 솔루션도 함께 소개합니다.
14:30 - 15:00	SK쉴더스 Cloud 보안 트렌드 – CNAPP (Cloud Native Application Protection Platform)	최근 Cloud 위협 동향과 Cloud 보안의 복잡성에 대해 설명하고 Cloud 환경에서 가시성을 확보하고, 통합적인 보안을 제공할 수 있는 'CNAPP (Cloud Native Application Protection Platform)'의 핵심적인 내용을 소개합니다.
15:00 - 15:30	전시 부스 관람	
15:30 - 16:00	태니엄 운영의 완벽을 완성하는 Tanium의 위력	클라우드 환경 내에서 기본적으로 필요한 가시성 확보 제어 및 문제 해결 등을 태니엄으로 해결 할 수 있는 방안을 제시 합니다.
16:00-16:30	사이버아크 클라우드 보안은 아이덴티티관리부터 시작합니다	클라우드 콘솔, 워크로드 등 멀티 클라우드와 하이브리드 환경에서 아이덴티티 보안을 통해 관리와 감사를 효율적으로 처리하는 방법을 제시합니다.
16:30	맺음말 | 경품추첨	

CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

아젠다 – 트랙 2

시간	세션 주제	세션 소개
13:30 - 14:00	LG CNS '23년 사이버보안 3가지 주요 이슈와 대응 방안	올해 사이버보안의 주요 이슈 세가지들을 하나씩 다뤄보고 그에 대한 대응 방안을 소개합니다. 1.Chat GPT와 같은 생성형 AI와 관련된 보안사고와 이를 안전하게 활용하기 위한 방안 2.2023 RSA의 키워드였던 강력한 인증/권한관리체계와 XDR의 등장배경과 앞으로의 활용 방안 3.공급망 보안의 등장 배경과 DevSecOps 체계 중요성
14:00 - 14:30	트렌드마이크로 Unified Cyber Security Platform: EDR, XDR 및 Attack Surface Risk Management의 상호 보완적 통합 전략	사이버 보안 분야는 계속해서 복잡해지고 있으며, 조직은 통합된 방식으로 다양한 위협들에 대응해야 합니다. EDR과 XDR은 각각 엔드포인트 및 확장된 네트워크에서의 위협 탐지 및 대응을 중심으로 하며, Attack Surface Risk Management(ASRM)는 조직의 공격 표면을 식별하고 위험을 최소화하는데 초점을 맞춥니다. EDR과 XDR이 대응을 자세를 취한다면 ASRM은 예방의 측면을 맡게 됩니다. 이러한 기술들을 통합함으로써, 조직은 단일화된 플랫폼에서 보다 효과적이고 일관된 방식으로 위협을 예방하고 대응할 수 있게 됩니다. EDR, XDR, ASRM의 융합과 상호 보완적인 전략을 통해 SOC 운영 효율의 향상으로 이어질 수 있는 방안을 알아봅니다.
14:30 - 15:00	스플렁크 멀티 클라우드 환경의 통합 보안 관제 및 자동화 전략	기업의 업무 환경이 멀티 클라우드와 다양한 SaaS 서비스 활용으로 급변함에 따라, 통합 보안 관제의 범위는 다양한 클라우드 환경을 포함해야 합니다. 더불어, 단일 환경에서 사이버 위협을 탐지, 분석, 대응할 수 있는 능력이 필요합니다. 스플렁크는 멀티 클라우드 환경에서 이러한 요구사항을 충족시키기 위해 상관 분석 룰 컨텐츠, 자동 대응 플레이북, 그리고 연동 앱을 즉시 활용할 수 있게 제공합니다.

*아젠다는 주최측 사정에 따라 변경될 수 있습니다.

CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

아젠다 – 트랙 2

시간	세션 주제	세션 소개
15:00 - 15:30	전시 부스 관람	
15:30 - 16:00	트렌드마이크로 제로 트러스트를 통한 보안 환경 지속성- 단계별 제로 트러스트 적용 모델 가이드	보안은 환경은 빠르게 변화하고 있습니다. 기존의 기업 관문/경계 보호는 더 이상 충분하지 않습니다. 또한 복잡한 IT 환경에서의 주요 보안 취약점이 빠르게 나타나고 있으며 클라우드 등 사이버 자산 전반에 대한 보안 태세가 부족합니다. 즉 기존의 전통적인 보안 모델에서 제로 트러스트 방법 모델로 전환하여 빠른 대응이 필요합니다. 새로운 보안 환경에 맞는 접근 제어 기본 구조를 혁신하고 상황에 맞는 접근 제어 정책 적용이 필요합니다. 추가적으로 ASRM과 연계하여 공격 표면 관리 – 접근 제어 – 위협 감소 – 지속적인 모니터링의 4단계 통하여 더 넓은 가시성과 분석 정보 통합의 지속성이 이루어져야 합니다.
16:00-16:30	소프트캠프 경계 없는 업무 환경에서 문서 보안 오케스트레이션 - 제로 트러스트 모델의 적용	하이브리드 워크 환경에 맞추어 새로운 문서 보안 대응 전략이 필요합니다. 사무실과 고정 근무시간을 벗어난 하이브리드 워크 환경에서는 업무 공간의 경계가 사라짐으로, 기존의 보안은 변화된 업무 환경에 맞추어 새로운 보안 방안이 요구됩니다. 소프트캠프는 업무가 수행되는 모든 장소와 모든 저장위치(On-Premise, Cloud) 그리고 다양한 디바이스에서 문서 중심의 보안/관리를 위한 Security 365를 소개합니다. Security 365는 업무환경의 변화에 따른 Document Centric Security 대응 전략과 문서보안을 위한 Zero Trust Security 프레임워크 적용 방안을 제시합니다. 추가로 사외 및 재택근무 등 하이브리드 업무를 위한 Remote Browser 격리 기술을 통해서 외부 위협 대응 방안을 소개합니다.
16:30	맺음말 | 경품추첨	

*아젠다는 주최측 사정에 따라 변경될 수 있습니다.

CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

아젠다 – 트랙 3

시간	세션 주제	세션 소개
13:30 - 14:00	아카마이 API보안에 대한 이해와 방안	IT환경과 기업 비즈니스의 변화로 인해 API 사용이 크게 증가하였습니다. 비즈니스의 확장으로 기업간의 협업과 모바일 환경에서의 서비스 증가는 API 활용을 더욱 크게 만들고 있습니다. 그러나 기업은 자신들이 얼마나 많은 API를 사용하는지 또 사용중인 API중 취약한 API는 없는지를 명확하게 식별하지 못합니다. 더 중요한 문제는 인증을 통해 안전하다고 간주하는 API가 내부에서 얼마나남용되는지를 식별하기란 여간 어려운 문제가 아닙니다. 조직에서 사용하는 모든 API를 식별하고 증가되고 있는 API 공격을 전문화된 기술로 빠르고 정확하게 탐지해야 합니다. 어떻게 조직의 모든 API에 대한 기시성을 제공받고, 취약하고 남용되는 API에 대해서 대응할 수 있는 방법을 소개 드립니다.
14:00 - 14:30	진앤현 시큐리티 위험관리 프로세스 자동화 방안	다양한 사이버 보안 위협과 함께 클라우드 보안 사고의 위험도 증가하고 있습니다. 클라우드 보안에서 가장 중요한 요소를 커버하는 것이 바로 지속적인 CSPM(Cloud Security Posture Management ; 클라우드 보안 상태 관리)입니다. CSPM을 통해 클라우드 보안 업무를 자동화하여 업무의 효율성을 높이고 지속적으로 안전한 클라우드 보안 상태를 유지하기 위해 앞으로는 자율 보안 체계 구축이 필요합니다. 이에 따라 통합 위험관리 플랫폼인 진앤현시큐리티의 SECUMOM 솔루션을 통한 위험관리 프로세스 자동화 방안을 소개합니다.

*아젠다는 주최측 사정에 따라 변경될 수 있습니다.

CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

아젠다 – 트랙 3

시간	세션 주제	세션 소개
14:30 - 15:00	오픈텍스트 오픈소스 라이브러리 방화벽을 통한 취약점 탐지/수정 한계성 극복	애플리케이션 1개에 400여개의 오픈소스 라이브러리가 사용되고 있으며, 이를 통해 소프트웨어 개발에 소요되는 시간과 비용을 획기적으로 줄일 수 있습니다. 그러나 매년 오픈소스 관련된 취약점은 수천 개씩 발견되고 있고, 이를 해결하기 위한 탐지부터 수정까지는 현실적으로 많은 노력과 시간이 소요되고 있습니다. 이번 세션에서는 취약점 대응의 한계성에 대한 사례를 소개하고, 조금 더 쉽게 오픈소스 보안관리를 위한 방법에 대해 설명드릴 것입니다.
15:00 - 15:30	전시 부스 관람	
15:30 - 16:00	라드웨어	디도스 공격은 이제 새로운 형태의 사이버 공격은 아닙니다. 하지만 국내 및 해외 언론을 통해 접하는 디도스 공격은 사이버 전쟁의 선봉장처럼 대규모 트래픽으로 국가나 기업의 서비스를 마비 시키기도 하고, 종교나 정치적인 이념이 다른 상대를 공격하는 하나의 사이버 무기가 되기도 합니다. 최근 보다 정교하고 진화하고 있는 대규모 애플리케이션 디도스 공격에 대해 분석하고 다양한 공격 사례와 더불어 라드웨어 디도스 방어 솔루션을 설명 드릴 것 입니다.
16:00-16:30	스카이하이 시큐리티 ChatGPT와 같은 Shadow IT에 대한 가시성 확보 및 제어 방안	보안담당자가 사용을 승인하지 않았지만 실제로 사용되어 보안 위협이 증가시키는 ChatGPT와 같은 클라우드 서비스 Shadow IT에 대한 관심이 어느때 보다도 커지고 있습니다. Shadow IT는 기업에서 관리해야 할 취약성의 영역입니다. 실제로 사용되는 위험한 클라우드 서비스 사용 현황 파악이 보안의 취약점을 관리하는 첫번째 방안입니다. 또한 사용자 인식을 통해 가시성을 확보하고, 필요에 따라 접근 제어 및 업로드/다운로드를 제어할 필요가 있습니다. Skyhigh SSE 솔루션을 통해 M365 뿐만이 아닌Shadow IT 대한 보안 대처 방안을 확인하십시오.
16:30	맺음말 | 경품추첨	

*아젠다는 주최측 사정에 따라 변경될 수 있습니다.