|  |
| --- |
|  |
| **[제 27회 해킹방지 워크샵] 보고서** |
|  |

**2023.12.13**

**제 27회 해킹방지워크샵**

일시 : 2023년 12월 7일(목)

장소 : 전경련회관 컨퍼런스센터

주최/주관 : CONCERT

특별후원 : KISA 한국인터넷진흥원

참석자 : 황훈(박정민), 김인수(양우성), 김다솔(김서영)

부록 : 해킹방지워크샵 책자

보고서 작성(분야, 담당자) :

| **분야** | **담당자** |
| --- | --- |
| Track A, Track E | 양우성 |
| Track B, Track F | 박정민 |
| Track C, Track G | 김서영 |





목차

[**Track A: 침해사고 대응 2**](#_de22hn2796ma)

[**Track B: IT Asset management 2**](#_so4uxlfubjt)

[**Track C: AI 보안 2**](#_50lgmelw95bm)

[**Track E: Case Study & Trouble Shooting 2**](#_9gseeddocm4t)

[**Track F: 클라우드 2**](#_gwjzpq4lp1hs)

[**Track G: Hot issue 3**](#_vuzyq1cns080)

# Track A: 침해사고 대응

## 1. 23년 국내 침해사고 위협에 대처하는 우리의 방어 전략

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| 한국인터넷진흥원 / 김광연 | 23년 국내 침해사고 위협에 대처하는 우리의 방어 전략 |

| **강연 내용** | 키워드 : 정보유출, 크리덴셜 스터핑  침해사고는 중소기업이 대부분(81%) 중견(9%)  이유?   1. 코로나 -> 디지털 전환   (기업) 온라인 협업 확대 -> IT 자산 증가  (생활) 비대면 클라우드 (DevOps)   1. 엔데믹 이후에도 경제 위축 2. 익명성 보장된 다크웹   기업 시스템 계정만 노린 전문 브로커 등장 (45% 증가)   1. 국제정세 사이버안보위협 증가(전쟁)   1.3 전자책 유출사고  피해업체는 출판업체와 피해보상 협의중인데 안되면 법정 싸움까지 간다.  1.4 크리덴셜 스터핑  이상탐지로 탐지가 안된다. 그래서  실제로 확인해보니까 A사와 B사 공격 ID가 99.9% 일치한다.  보통 다크웹에서 사는 줄 아는데 그게 아니라 네이버 피싱 수집 계정 등을 이용한다.  MFA -> 이용자 불편 -> 수익구조에 영향  그래서 선뜻 도입하기가 애매함.  근데 하지만 다른 기업들이 다 하면 우리도 한다는 식이 기업들 입장.  => 법적 제도 마련이 필요하다(필수적으로)  1.5 랜섬웨어   1. 제약 회사 랜섬웨어   개발서버 방치 -> IT 보안팀은 자산 존재 유무를 모름 -> 취약점 업데이트가 안됨 -> 공격자가 접근  공격자들의 최근 추세는 백업서버를 가장 먼저 감염시킨다.  ex) 새벽마다 권한상승, 권한변경이 있길래 이상해서 업체에 전화해서 확인해보니까 sysmon V15.11 취약점이 있었음. 10000포트로 접근했다.  1.6 디도스  최근 한방에 피해를 입히는 쪽으로 변경하는 추세  1.7 개인지갑 가상자산 해킹  사례) 1. broad하게 국세청 사칭 메일 배포.  2. 1번으로 얻은 정보를 가지고 협력사 사칭 메일을 발송  1.8 공급망 공격  업데이트 서버 해킹, SW취약점, 유지보수망 등을 노리는 추세  정리.  지속적 관리, 모니터링 구축  준비사항.   1. 외부 컨설팅으로 재점검하자. 2. 기업보안 강화 시 공격 주체 파악(우리를 공격하는 공격 그룹이 누구인지 아는 것이 중요) | |
| --- | --- | --- |
| **QnA** | Q1. 다크웹 모니터링을 하고 있는지?   1. 너무 많아서 하진 않는다. 근데 신고가 들어오면 한다.   Q2. C-TAS를 통해 오늘 발표한 내용의 사고들 관련 ioc, 분석 정보가 공유가 되는지?   1. 월마다 취합해서 공유하고 있다.   Q3. 크리덴셜 스터핑을 기업에서 막을 수 있는 실질적인 방법은 뭐거 있을까요? 인텔리전스를 활용하는 방법 외에 궁금합니다.   1. 로그인 페이지의 2차인증, 캡쳐를 못하는 이유가 고객이 불편하기 때문임.   기업에 접근성이 떨어지면 이익이 감소하기 때문에 기술보다 정책적으로 접근해야 한다. 일정 수의 개인정보를 처리하는 기업은 MFA 등 인증수단을 더 하게 해야 한다.  Q4. DDoS는 서비스 방해나 금전적 요구를 들어주지 않는 경우에 주로 일어나는데, 예로 들어주신 상위단계 공격으로 갈 수록 공격자가 자신의 요구사항을 주장하기가 쉽지 않을 거 같습니다. 네트워크 트래픽 규모도 커지는데 공격이 그쪽으로 진행되는 이유가 무엇일까요?   1. 보통 DDoS가 일어나는 이유는 1. 금전 목적 협박 2. 경쟁이나 개인원한같이 특정 기업이 싫어서 방해하는 목적이다. 해커들은 지속적으로 인프라를 구축해서 일시에 피해를 끼친다. 해커들이 쌓아놓은 인프라를 사전에 파악해서 막아야 한다. | |

## 2. Lazarus 그룹, 워터링 홀을 이용한 대규모 해킹 공격

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| Ahnlab / 김준석 | Lazarus 그룹, 워터링 홀을 이용한 대규모 해킹 공격 |

| **강연 내용** | 키워드 : 0-Day Exploit, Watering Hole, Supply Chain  라자루스 그룹은 북한의 해킹 그룹으로 대한민국에 가장 위협이 되는 공격 그룹이다. 가상화폐 탈취와 정보 유출을 목적으로 하고 대한민국 정부 최초로 사이버 분야 독자제재 대상으로 지정하였다.  전 세계에서 가상화폐에서 탈취된 전체 금액의 50%가 라자루스 그룹이다.  라자루스 그룹의 침투 방법은 크게 3가지로  Spear Phishing, Social Engineering, Watering Hole 이다.  워터링 홀(페이지에 자바스크립트 삽입 추정)이란  워터링 홀 목표가 되는 대상자들이 자주 방문하는 특정한 사이트에 미리 악성코드를 심어 놓고, 이들이 해당 사이트를 방문했을 때 자동적으로 컴퓨터를 감염시키는 방법이다.  안랩에서는 광고배너가 아닐까? 하는 생각으로 처음에 접근했었다.  하지만 라자루스는 보안프로그램을 통해 61개의 기관을 해킹하였다.  이때 특정한 사이트는 보통 언론사 사이트였고 어떻게 7~8개의 언론사 사이트가 당했을까 궁금해서 포렌식 등을 하려고 컨택해봤지만 언론사가 관련 파일이나 정보를 주지 않았다.  기본적으로 언론사가 단독보도를 하는 다른 언론사들을 알아야 하기 위해서 언론사가 언론사를 모니터링하는데 A언론사가 바이러스에 감염된 채로 B언론사를 모니터링하는 식으로 감염이 진행되었다.  언론사의 웹사이트를 해킹하여 워터링 홀 사이트로 악용하였고 공격자는 언론사 기업 내부로 보안 프로그램의 제로데이 취약점을 이용하여 침투했다. 언론사 침투 후 뉴스 서버를 장악하여 특정 보안 프로그램의 제로데이 취약점을 악용할 수 있는 워터리 홀 페이지를 구축하였다.  라자루스 그룹의 이번 공격 특징은 제로데이, 원데이 취약점을 악용하고 윈도우 루트킷을 사용하고 파일리스 기반의 공격이 특징이다.  라자루스 그룹이 사용한 제로데이 취약점의 도구는 금융 보안 솔루션(공동 인증서)와 자산 관리 솔루션(공급망 S/W)이다.  금융 보안 솔루션(Non-ActiveX) 의 경우 필수 프로그램으로 민간 전자서명 도입 전까지는 강제 설치 프로그램이었다.  MagicLine4NX, VestCert 이 두개의 프로그램이 중요 취약 프로그램이었고 이 두 개의 프로그램이 설치된 채로 공공기관 서비스 이용했다면 이용한 PC가 취약 환경이 되는 것이다. 만약 언론사 페이지에 들어갔다면 취약한 기업이 되었을 수 있다.  MagicLine4NX의 경우 약 39,000,000대, VestCert의 경우 dir 12,000,000대, INISAFE CrossWebEX V3의 경우 약 26,000,000대의 PC에 설치가 되어있었다.  대한민국 인구가 51,000,000인 것을 감안하면 결코 적은 숫자가 아니다.  이런 금융 보안 솔루션의 설치 시 특징은 백그라운드 자동 실행이 되는 것으로 지속성이 유지되는 특징과 특정 포트를 리스닝(사용 여부 관계 없이)하는 특징을 노렸다. 금융 보안 프로그램인 워치독 프로세스로 종료 여부를 모니터링해서 문제 발생 시 재실행시키는 프로그램이 있는데, 백신이 취약한 보안 프로그램을 종료시켜도 워치독 프로세스로 다시 취약 프로그램이 켜지는 문제도 있었다.  라자루스 그룹이 퍼트린 프로그램은 강력하지만 하나의 조건이 필요했다.  NAT가 구성된 망은 공격이 불가능하라는 것이다.(라우터와 같이 Gateway 역할을 하는 네트워크 장비가 있을 경우) 그래서 라자루스 그룹이 실제 사용한 공격 사례는 내부전파이다.  MagicLine과 같은 프로그램은 자동 업데이트가 없는 프로그램이라 보안 패치를 진행해도 수동 업데이트를 하지 않는 이상 취약점이 유효했다. 그렇기에 파급력이 높은 MagicLine의 경우 V3 백신을 통해 강제 삭제할 수 있는 보안 조치를 취했다.  이런 공격은 국내 한정으로 취약점 신고가 늦어지고 특정 국가 타겟으로는 더 좋은 먹잇감이 되는 것이다.  또한 취약 프로그램은 서버로그와 이력을 남기지 않게 안티 포렌식으로 싹 정리하고 나간다. 그래서 더 알아차리기가 어려웠다.  분석팀은 어떻게 찾았을까?  진단 모니터링 -> 악용 의심 제보 -> 포렌식 조사 -> 주요 행위(TTP) 선별 -> 주요 TTP 모니터링 -> 모니터링 알람 -> 고객사 컨택 -> 취약점 분석 -> 기관에 신고  이번 캠페인에서 확인된 S/W 취약점은 모두 RCE(Remote Code Execution) 취약점이다. | |
| --- | --- | --- |
| **QnA** | Q1. 계속 취약점이 발견되고 있는데 어떻게 대응하실 것인지  A : 공급망 공격으로 어떻게 금융보안 솔루션을 노렸는지는 모른다. 근데 해킹한 솔루션을 타고 간다.  Q2. 라자루스는 이걸 어떻게든 볼탠데, 어떻게 바뀔 것인지 짐작가는 것이 있으신지  A : 한국에서만 사용하는 취약점은 계속 노려질 것이고, 전세계적으로 사용하는 것들도 노려질 것이다. 소셜 엔지니어링 공격이나 앞에서 설명했던 여러 공격을 계속 할 것으로 생각된다. | |

## 3. 기업들의 침해사고 대응 방법, 장단점 비교

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| 플레인비트 / 이준형 | 기업들의 침해사고 대응 방법, 장단점 비교 |

| **강연 내용** | 국내 기업의 99.9%는 중소기업이고 근로자 비중은 81.3%  중소기업 침해대응 현황으로 중소기업의 랜섬웨어 피해 운영체제는 높은 순으로  윈도우10(개인포함), 윈도우서버2012 R2 Standard, Cent OS 7, Cent OS 6이다.    침해사고는 넓게 보면 인터넷에 연결되어 있는 모든 것들은 다 당할 수 있다.  피해업종은 정보통신업 - 제조업 - 도매 및 소매업 순으로 높았고  피해업종별 평균 신고 기간은 일주일 정도였다. 보통 다 스스로 뭔가 해보려고 만지다가 더 어려워지고 안되니까 신고를 하게 된다.  대응방안은 대응방안 이행률 : 39.5%  미이행 사유 : 외부 업체/ 고객사 협의 필요, 내부 사정으로 인해 추후 조치 예정, 보안 장비 구비 예정, 운영 시스템 오류 우려로 보류, 위험도 평가 진행 후 조치 예정, 서버 재설치 예정  아쉬운 침해대응  우리는 어쩔 수 없이 침해사고가 일어났다?  -> 관리, 인식, 관심의 부재로는 성립 불가 명제  우리는 보안에 쓸 돈이 없다  -> 돈으로부터 출발하는 보안, 투자의 개념이 없다면 하기 쉽지 않다.  침해사고가 일어나면 우리에게 무슨 일이 일어날까?  -> 사실, 아무 일도 일어나지 않는다(개인정보유출 침해사고 제외)  우리에게 피해는 없으니 일을 만들지 말자.  -> 직접적인 피해는 없더라도 간접적인 피해는 존재한다.  but, 중소기업들이 공격 당했던 서버가 다른 기업의 공격 인프라로 활용되는 사례가 아주 많다. 공격자들도 인프라가 없으면 공격하기 쉽지 않으니 대응하자.  가장 두려워하는 건 볼 게 없다는 것.  대응방안 중 가장 쉬운 것은 현장보존이라는 것. 폴리스라인처럼 현장보존을 위해 막아야 한다. 안티 포렌식을 하고 나오는 프로그램이라면 더더욱 어려워진다.  랜섬웨어 침해사고 - BitLocker  2016년부터 발생한 침해사고  윈도우 기본 보안 기능을 활용하다보니 탐지나 대응이 쉽지 않음.  공격자는 복구 키를 네트워크 다른 컴퓨터에 저장하거나 본인 컴퓨터로 저장함  현장 보존을 했더라면? -> 복호화 가능  현장 보존을 못했다면? -> 복호화 불가능  랜섬웨어 신고를 받고 갔는데 뭔가 이상해서 컴퓨터를 종료했다.  볼륨 섀도 복사본(특정 이벤트가 발생하면 백업해버리는 작업)을 지우는 게 요즘 랜섬웨어인데 전원을 꺼버리니까 볼륨 섀도 복사본으로 전부 복구한 적도 있다.  네트워크 구성 파악  조직의 인프라를 구성하는 기본 구성 요소  사용하는데 문제가 없으면 관심을 두지 않는 요소  네트워크 구성 요소  데이터의 제어와 흐름 정책  네트워크 연결 요소 목록  네트워크 구성도 혹은 네트워크 연결 자산 목록  로그는 침해대응의 네비게이션과 같은 역할. 록를 잃어버리면 길을 잃어버리는 것과 동일하다.  기간 만료에 의해 로그가 삭제되는 것은 당연한 일. IT자산 관점에서 당연한 일, 보안 관점에서는 당연하지 않다.  보존해야 할 대표적인 로그. 웹 로그, 데이터베이스 로그, 서비스 로그  오픈소스의 사용은 비용 절감에 효과적이지만 잘 관리되지 못하는 오픈소스는 독이 든 성배이다. 취약점을 내포하고 있는 오픈소스를 사용하면 우리 조직에 취약점을 추가하는 꼴.  오픈소스 사용 시 점검 사항으로 오픈소스 업데이트 최근 이력 존재 여부 확인, 보안 업데이트 이력도 별도로 필수 확인해야 한다.  오픈소스 취약점 목록을 보는 것도 좋다.  오픈소스 제작자가 처음엔 열심히 보안 업데이트도 해주다가 취업하고 그러면 보안 업데이트가 중단되어버린다.  침해사고 = 미사일  목적 달성을 위한 전재 과정은 대부분 비슷하지만 공격자 판단에 따라서 사고의 파급력과 양상이 달라짐. 침해 결과에 집중하는 것보다 침해 발생 원인에 집중해야 한다  보안 인식 개선  현재  우리는 피해 없으니까 괜찮다. -> 다른 곳에 피해를 주고 있을 수 있다.  사고 관련 내용은 아무도 몰라야 한다. -> 사고 관련 내용은 적극적으로 공개해야 해결하는 데 도움이 된다.  악성파일만 삭제하면 될 것 같다. -> 악성파일은 언제든 다시 생성될 수 있다.  피해 복구가 되었으니 이상의 조치는 필요없다 -> 침해 결과 해결보다 원인 해결이 중요  우리가 알아서 조치하겠다 -> 침해대응은 생각보다 복잡하다.  보안 솔루션 설치가 되어있다. -> 보안 솔루션은 완벽하지 않다.  대응방안 적용보다 중요한 일이 많다. -> 공격자는 사람 1명과 무한에 가까운 공격 기계가 존재한다.  서버 재구축하면 된다 -> 대응방안이 마련되지 않으면 서버 재구축은 불필요하다.  자원 관리 실패 사례  로그 옵션 OFF, 로그 3일 분량 저장, 로그 저장 경로 파악 불가, 시스템에 로그가 너무 많이 쌓여 로그 다운 불가 -> 정확한 원인 파악 불가  자원현황 - 유휴 서버/PC 존재, 웹 서버는 존재하지만 어디에 있는지는 모름, 자원의 사용자 파악 불가, 클라우드 자원의 생성/삭제 현황 파악 불가, 네트워크 구성도 부재 혹은 예전 버전 -> 침해 확산 범위 및 영향도 파악 불가  자원상태 - 접속 계정 정보 모름, n년전 마지막 운영체제 업데이트 -> 초동 대응 불가  기타 - 인터넷 노출 방지(중요 정보/페이지 등) -> 대응 범위의 급진적 확대  기업을 대상으로 진행되는 무료 보안 서비스 활용  한국인터넷진흥원  내 서버 돌보미, 보안 취약점 점검, SW 보안약점 진단, 중소기업 홈페이지 보안강화, 중소기업 침해사고 피해지원 서비스, 사이버 위협정보 분석공유(C-TAS), 사이버 위기대응 모의훈련, 사이버 시큐리티 훈련 플랫폼, DNS 싱크홀  한국정보보호산업협회  정보보호 컨설팅/제품 공급기업 모집, 랜섬웨어 대응지원, 한국제로트러스트위원회  침해사고 컨설팅 전문 업체 의뢰  기업의 현실적 어려움은 보안 인력 확보, 침해대응 체계 수립 및 운영, 인프라 구성 및 운영, 내부 인식 개선 = 침해사고 컨설팅 전문 업체 의뢰로 해결 가능 | |
| --- | --- | --- |
| **QnA** | Q1. 대응방안 이행률은 며칠 기준으로 확인한 것인가요  A : 보통 대응방안 보내고 나서 일주일뒤에 다시 물어보는데 그때 하고있다고 하면 그대로 확인하고 다음에 또 연락해서 물어보는 데, 총 2번 물어봐서 마지막에 물어본 것 기준으로 이행률을 했다. | |

# 

# Track B: IT Asset management

## 1. IT자산관리 패러다임의 변화

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| 토스증권 / 지정호CISO | IT자산관리 패러다임의 변화 |

| **강연 내용** | 정보보호 활동에서 첫 활동: 자산의 파악  1 .자산의 정의가 필요하다.  ‘어디까지가 자산이고 어디까지 관리 해야 하는 자산인지’   1. Infrastructure: IDC, Cloud, Server, PC, Mobile 2. Platform: DB, WAS, Docker, Kubernetes 3. Application: JS, API, Web 기반 서비스   2. NIST cybersecurity framework   1. 식별(Identify): 조직에 가장 중요한 자산과 자원이 무엇인지를 파악해야 합니다. 2. 보호(Protect): 보호 기능은 적합한 보호 장치를 개발하여 구현하고 중요 인프라를 보호하기 위한 기술적/물리적 제어를 목표해야 합니다. 3. 탐지(Detect): 탐지 기능은 조직에 사이버 공격에 관해 알리는 수단을 구현합니다. 4. 대응(Respond): 대응 기능 범주에서는 사이버 공격 및 기타 사이버 보안 이벤트에 대한 올바른 대응을 보장합니다. 5. 복구(Recover): 사이버 공격, 보안 침해, 기타 사이버 보안 이벤트가 발생할 경우에 비즈니스 연속성을 보장합니다.   3. 과거의 문제점  자산조사하는 경우 ‘자산조사 - 자산 불일치발견 - 자산현행화 - 자산반출입 기록 - 자산조사’ 이 4단계의 과정이 반복됨.  4. 자산관리를 잘하기위한 관리지침   1. 자산의4가지 분류: 서버, 네트워크, 인프라, 자산관리 2. 자산관리의 CRUD:대부분의 컴퓨터 소프트웨어가 가지는 기본적인 데이터 처리 기능인 Create(생성), Read(읽기), Update(갱신), Delete(삭제)를 묶은 개념. 3. SAC자산 목록 동기화, ANSIBLE 신규서버 취약점점검, SIEM 자산관리서버 이용 4. 서버배포와 하드닝 동시진행을 통한 안전한 상태의 운영목표 5. 금융사의 경우 임직원 수의 3배 정도 되는 PC를 운용하고있음. 이러한 환경에서 모든 PC에 대하여 운용, 보안설정, 에이전트 설치 유무를 파악   6. 최종 목표  SPLUNK를 통해 모든 리소스의 데이터를 수집한다. 모든 컴퓨터의 상태를 확인하여 자산 관리 모니터링을 진행한다.  처음 설계부터 자산 실시간 모니터링을 목표로 설계하였기에 가능하다. | |
| --- | --- | --- |
| **QnA** | Q1. 자산식별에 대한 담당을 인프라팀, 정보보안팀중 누가 담당하는가?   1. 팀마다의 관리 목적이 다름을 이해해야한다. 보안팀은 모든 리소스에 대하여 관리하는데 목적이있고, 인프라팀은 어느 서버에 어느 CPU가 달려있는지 확인하려한다. 인프라팀에게 취약점은 중요치 않다.   가장 중요한것은 원장이 똑바로 서있는것이 중요하다. 원장을 기준으로 각자 관리를 진행한다.  Q2. 하드닝 점검 주기가 어떻게 되시나요?   1. 현재는 분기마다 1번씩 진행하였으나, 매일점검을 목표로 하고있다.   Q3. 컨테이너 내용까지 확인을 진행하는가?   1. K8S등 컨테이너 자산의 현황은 파악중이지만 내부에 내용이 무엇이 있는지 확인은 어렵다. | |

## 2. ChatGPT로 공격표면 관리하기

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| 넥슨코리아 / 김동춘 실장 | ChatGPT로 공격표면 관리하기 |

| **강연 내용** | 침투하려는 외부자 입장에서 발표 진행하였음   1. 목차   1) 자산수집  2) AI적용사례  3) 마치며   1. 넥슨의 자산 수집   넥슨의 문화는 금융권과 달리 개방적인 운영을 하고있다. 해외지사의 문화적 자산관리까지 고려해야한다. 자산을 손쉽고 빠르게 조회할 수 있는 통합 검색 엔진 적용. 수 많은 자산중 외부에 직접 노출된 자산을 각별하게 관리함을 목표로한다.    <넥슨에서의 자산통합검색 화면>   1. 위협   각종 목적 또는 실수로 외부 Any open된 각종 서비스는 해커의 주요 타겟이 되어 각별한 관리가 필요함. 공격기법이 공개되고 2시간 이내 넥슨에 실제 공격 유입이 시작된다.    <실제 공격 개시이후 공격 기점별 구분>  약 1.3만개의 서비스 외부노출  자산정보수집 > Public IP추출 > IP스캐닝, All Port Scan > Protocol분석, Pattern base > Screen shot 분석   1. AI이용   AI 기반 이미지 판정 Response 패턴으로 구분되지 않는 사람이 판정해야 했던 스크린샷을 AI 기반으로 전환 => 99.95% 정확도 구현  취약점을 이용한 익스플로잇 공격 시도 또는 성공 시 평소에 발생하지 않는 이상 로그를 발생시킨다. 분석기는 대량의 로그 속에서 눈에 튀는 로그를 식별하고 이를 중심으로 분석을 시작한다.    <웹OS등 서비스에서 원시로그 수집 - GPT4로 대규모학습 - 학습데이터 기반 희소성이 높은 로그 자동 판정>  넥슨 관련 웹페이지 수백개가 하루마다 변경이됨. GPT를 통해, 즉 AI를 통해 웹사이트가 변경되는지 확인하자. 70만개의 웹페이지를 라벨링하고 AI Custom Vision을 통해 학습함.   1. 아직 남아 있는 과제   1) log4j 에 취약한 모든 자산을 알려줘  2) 적합한 조치방안 리포트를 작성해 줘  최종목표: 취약점 서칭 > 조회 > 조치 한번에 가능한 모델 개발 | |
| --- | --- | --- |
| **QnA** | Q1. AI가 학습하는데 걸리는 시간이 어떻게 되는가?   1. 70개 학습에 30분정도 소요된다.   Q2. 보안조직내에 개발 조직이 존재하는지?   1. 넥슨코리아의 CERT팀에는 개발부서가 있고 13명의 전담인원이있다. 데브옵스 11명 정책팀도 따로 존재한다. CERT팀에 관제를 제외하고 40명정도 있다.   Q3. 자산통합검색 시스템은 자체 개발인지?   1. 예 자체개발입니다.   Q4. 클라우드 관련 자산관리 툴은 무엇을 사용하는지?   1. Cloud AWS자체 제공 툴 이용   Docker Container은 공개 API를 이용한다.  Q5. Chat GPT가 학습이 되는것인가?   1. 외부 ai는 학습을 지원하지 않는다. GPT4를 다운받아 자체 학습모델로 개발했다. 타 회사의 MS나 외부 AI는 아직 시기상조이다. | |

## 3. 소프트웨어 식별증: SBOM으로 보다 스마트한 보안

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| KB국민은행 / 박종찬 대리 | 소프트웨어 식별증: SBOM으로 보다 스마트한 보안 |

| **강연 내용** | SBOM에 대하여   1. 목차   1) WHY  2) WHAT  3) HOW  4) WHERE  5) APPENDIX   1. WHY   2021년 5월 미국의 송유관 해킹사고가 발생한 이후 행정명령이 발동됨. 행정명령 내용으로는 ‘미 행정부에 납품되는 소프트웨어의 SBOM을 모두 제출하라’   1. WHAT   BOM은 주로 제조업계에서 사용된다.  예를 들어 스타뱅킹은 여러 오픈소스를 가져온다. SBOM을 통해 각 소스들의 환경설정 버전을 확인할 수 있다.  SBOM타입으로는 ISO, Cyclon DX, SPDX 3가지 타입이있다.  ISO기준은 국제적인 기준이지만 제한이 많고 사용이 적다.  Cyclon DX기준은 보안에 특화된 SBOM작성요령으로 API에 상당히 친화적이지만 유저에 친화적이지 않아 사용자가 많지는 않다.  SPDX기준은 사람이 읽기에 친화적이기에 많은 이용자가 있다.    <Cyclon DX이용한 SBOM이용>   1. HOW   소스코드와 패키지(바이너리) 기준으로 SBOM을 작성한다.  소스코드를 snippet로 보기에 상세히 알 수 있다. 한개의 오픈소스에 여러 소스코드가 있다.   1. WHERE   소프트웨어의 건강 체크 개념이다.  list open-source, find license issue, find security issue(CVE)  Cyclon DX의 CPE영향평가 이용. Supply-Chain(V3, 한컴)에도 SBOM제출을 요구함. 외부에서는 관리하지 않는것이 내부에서 발견되었다면 의심가능하다.   1. APPENDIX   오픈소스 API를 점검하는데 취약점을 발견하는 경우, 취약점 부분만 수정을 하고싶다. 버전업을 할경우 동일 API를 이용하는 다른 소프트웨어까지 수정이 필요하기에 부분적 수정 필요. 예를 들어 Spring의 경우 자바의 언어가 달라지는 수준의 버전업이 이루어지기에 버전업을 통한 해결은 어렵다. | |
| --- | --- | --- |
| **QnA** | Q1. 모든 거래처에서 SBOM을 모두 받는가?   1. 금감원 체크리스트에 SBOM을 받도록 명시되었기에 받고있다.   Q2. eks(Amazon Elastic Kubernetes Service)환경에서도 구현가능한가?   1. Docker에서 SBOM 추출은 가능하다.   Q3. 개발자와 보안담당자의 역할 분담이 어떻게 이루어지고 있는가?   1. 위험도를 낮추기 위한 디펜던시와 정상적인 작동은 개발자가 판단을 한다. 보안담당자는 가이드를 제시하는 역할이며, 그 가이드를 따를지 말지는 개발자겨 결정한다.   Q4. 개발자가 API에 대해 잘 모르고 이용하는 경우 대처할 방안이 무엇인가?   1. API사용에 대하여 포탈을 통해 철저하게 관리한다. 버전내용과 버전업의 로그를 기록하고 증적사진을 모아둔다. | |

# 

# Track C: AI 보안

## 1. 챗GPT등 인공지능이 보안 분야에 게임체인저가 될 수 있을까?

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| 이글루코퍼레이션 / 정일옥 | 챗GPT등 인공지능이 보안 분야에 게임체인저가 될 수 있을까? |

| **강연 내용** | 변화를 사전예측하는 것은 어렵다. 코로나, 팬데믹, 러시아 전쟁 등 그 어느 것도 전년도 예측되지 않았다. 아직, 사이버 팬데믹은 오지 않았지만, 이를 대비할 수 있는 것 중 하나가 AI/ML이다. 즉, 인공지능으로 예측할 수 있다. 하지만 좋은 인공지능 기능이 없이는 제로 트러스트 보안이 성공하기 어렵다.  다가올 사이버 위협 분야에서도 적대적 AI, 챗 GPT 기반의 사회공학 등이 이슈가 되고 있다.  인공지능은 다양한 보안분야(Malware Detection, 공격 단계 예측, 보안 이벤트 정 ・ 오탐 식별, 위협 헌팅 및 포렌식 등)에 이미 적용되고 있다. 하지만 아직까지 보안분야에서는 인공지능이 다음과 같은 이유로 인해 환영받지 못하고 있다.   * 데이터 부족 * 인공지능 적용을 통해 이루고자 하는 목표 미흡 * 인공지능 도입 시 인공지능 결과에 대한 신뢰 및 전문인력 부족   2년 전부터 사용했던 방법은 생성형 AI이다. 생성형 AI는 보통 기존에 많이 사용하였던 판별형(Discriminative) AI와 다르게 데이터 생성을 위한 확률분포로 사용한다. 이를 사용하면 인공지능이 보안에 잘 녹여지지 않을까 생각하였다.  생성형 AI(ex. ChatGPT)는 엄청난 확장속도를 자랑하고, 사용성이 높다. 이와 같은 장점으로 여러 사람들이 사용하고 있다. 하지만 가짜뉴스, 악용에 이용되기도 한다. 즉, 양날의 검으로 사용될 수 있기 때문에 사용 목적에 따라 사이버에 위협과 보안을 고도화할 수 있다.  이러한 상황에서 생성형 AI를 보안분야에 적용하면 게임 체인저가 될 수 있을까? Google같은 경우에는 2000년대 초반에 검색엔진을 개발하여 현재 시장점유율 90% 이상을 차지하였다. 하지만 구글 엔진에 사용되는 데이터에 대한 다음과 같은 보안 이슈가 발생하였다.   * 검색엔진으로 고객 정보 수집 * 이러한 부작용으로 고객 입장에서 정보 유출 사례   때문에 GHDB(Google Hacking Database)라는 구글 해킹에 대한 다양한 방법론들이 등장했다.  현재 생성형 AI는 보안에 어떻게 사용되고 있을까? 보안업체 체크포인트(Check Point)에 의하면 이미 다크웹 내 포럼에서 활동하는 사이버 범죄자들이 ChatGPT를 악성 공격에 활용한 사례들이 공유되고 있다.  공격자들은 ChatGPT를 통해 오픈소스 공격도구 확장, 페이로드 생성, 화이트박스 진단 등 기존보다 공격에 사용되는 도구를 만들거나, 개발하는 소요되는 시간을 단축한다.  이에 맞서는 방어자 역시 ChatGPT를 통해 취약점 진단 스크립트 제작, 로그 정규화, payload 분석 및 Rule/Query 제작, Bug Bounty 자동화 등의 방법으로 고도화된 공격에 대응하고 있다.  그렇다면 보안 분야에서는 생성형 AI를 어떻게 사용하고 있을까? 다음은 생성형 AI 활용 사례들이다.   * 빅테크 중심으로 한 단독 플랫폼 형태 * 기존 보안업체를 중심으로 독자적인 생성형 AI 모델 생성 또는 기존의 AI를 결합한 하이브리드 모델 기반의 서비스 제공 * BurpSuite 확장기능으로 LLM을 탑재한 BurfGPT를 통해 웹 어플리케이션 보안테스트   하지만 이대로 생성형 AI를 사용하기에는 위협사례가 존재한다. ChatGPT 모델이 루팅공격을 당하거나, 프롬프트가 해킹을 당하게 될 경우 사용자의 정보를 파악하는데 악용될 수 있다. 또한 LLM 서비스 제공업체가 해킹을 당하면 ChatGPT에게 물어본 데이터가 외부에 유출될 수 있다.  이러한 문제들로, 생성형 AI가 게임체인저가 되기 위해서는 몇 가지 대응전략이 필요하다.   1. 답변에 대한 신뢰성이 항상 필요하다.  * 환각(할루시네이션) 효과 등으로 인해 보안 분야의 신뢰성과 대치됨 * 때문에, 프롬프트 엔지니어링과 파인튜닝을 통해 LLM에 대한 보안성과 신뢰성 강화 * ChatGPT의 경우 Browsing, Plugins을 통해 답변에 대한 신뢰성 향상  1. 데이터 보안에 필요한 비식별화 및 적대적 AI에 대한 방안 마련이 필요하다.  * 대규모 언어모델을 사용 시 외부 연결 필요, 연결 시 이동하는 민감 데이터 유출 우려 * 서비스 되는 인공지능 모델에 대한 공격 증가(API 관련 공격 및 새로운 형태 공격 증가 우려) * 민감하고, 중요한 데이터에 대한 비식별화(변환/삭제) 조치 및 모니터링 등 대응 및 가이드 필요  1. 보안에 최적화된 sLLM 모델 개발이 필요하다.  * 보안 분야의 특성 상 내부 및 폐쇄된 환경 또는 데이터 유출 등에 대한 우려로 인해 구축형 AI를 선호한다. * 소규모 언어모델(sLLM)과 같이 특정 영역의 보안에 최적화된 모델 개발 필요  1. 양질의 학습데이터가 필요하다.  * 보안 데이터셋은 특성상 확보 어려움. 또한, 레이블 된 보안 데이터를 얻기 위해서는 시간/비용/인력 소요 * 레이블 된 데이터보안 도메인과 빅데이터, 인공지능에 대한 지식을 보유한 인력 양성 필요  1. 보안 분야에서 기존 시스템 및 데이터 연계를 고려해야 한다.  * 인공지능 기술은 대체로 기존의 보안관제 등 보안기술에 접목되어 구현되는 체계로 운영됨에 따라 기존 보안시스템과의 연계가 필수 * 사이버위협 인텔리전스 등과 연계하여 기관 내 보안 데이터 뿐 아니라 외부 기관이 보유한 위협정보를 공유, 연계할 수 있는 인공지능 체계 구축  1. 생성형 AI에 대한 보안위협에 대한 보안 가이드라인이 필요하다.  * ChatGPT 등 생성형 AI 활용보안 가이드라인 발표(국가사이버보안센터, 2023. 6), ATRAS Matrix(MITRE) * 소형 LLM에 대한 보안검증 기준 등이 필요 | |
| --- | --- | --- |
| **QnA** | Q1. LLM을 AiR의 입력 처리에도 사용한다면 자연어 형태의 입력을 받아서 처리할 수도 있을텐데 그렇게 하지 않으신 이유가 있으신가요?   1. 그냥 사용하기에는 사실 리스크가 있다. 있는 데이터를 바로 LLM 모델에 던지기에는 보안에 문제가 있기 때문에 기존의 모델에 넣는 데이터 형태로 피쳐 등을 변경하여 바꾼다.   Q2. 페이로드에 프롬프트 인젝션이 있을 경우를 배제할 수 없을텐데 이를 위한 전처리 기술이 AiR에 적용된 것이 있을까요?   1. 기본적으로 스크립트에 대한 상황이 나오게 된다. 스크립트나 인젝션이 되지 않도록 전처리 기술을 적용하고 있다.   Q3. 현재 AiR 서비스를 온라인에서 실제로 제공하고 있나요?   1. 지금 Air 서비스는 온라인에서 무료 서비스로 제공하고 있다. 안정적으로 답을 내놓는 것이 먼저이므로 이게 된다면 국내보다는 해외에서 내년 2월쯤 유로로 제공할 예정이다. | |

## 

## 2. 생성AI로 쉽게 만들어내는 BEC 공격에 대한 스마트한 방어 전략

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| SSNC / 조창석 | 생성AI로 쉽게 만들어내는 BEC 공격에 대한 스마트한 방어 전략 |

| **강연 내용** | 최근 사이버 공격에 있어서 해커들에게 가장 ROI가 높은 공격 유형은 이메일을 통한 BEC(Business Email Compromise) 공격으로 최근 3년간 크게 증가한 공격 유형이다. BEC 공격 시도도 연간 증가율이 83%이고, 소셜 엔지니어링 침해사고의 50% 이상을 차지하며, 2022년 BEC 공격 피해 금액 규모도 20억원 이상이다.  BEC 공격은 다음과 같은 공격 기법을 사용한다.   * CEO 사칭하여 긴급 송금 또는 민감한 정보 요청 * 벤더사 또는 공급업체 이메일을 침해하여 가짜 송장에 대한 결제를 요청하거나 은행 계좌 내역의 변경을 통지하여 향후 결제를 가로챔 * 직원 또는 벤더사의 계정을 탈취(ATO)하여 다른 직원이나 비즈니스 파트너에게 지불을 요청하거나 민감한 데이터를 요구 * 스레드 해킹해서 송금 또는 민감 정보를 공유하도록 속이려고 시도 * 변호사나 법률 자문자로 사칭하여 피해자에게 자금 이체나 정보 공유 강요 * 인사정보를 도용하여 인사 또는 회계부서 직원을 대상으로 세금정보와 같은 민감한 데이터를 요구   이외에도 생성AI를 활용한 사이버공격이 진화하면서, 진짜와 가짜를 구분하지 못하는 사용자들에게 AI를 이용한 공격이 점점 증가하고 있다. 이를 탐지하기 위한 기술 또한 AI를 활용할 수 있다.  다음과 같이 탐지와 방어에도 AI를 적극 활용 가능하다. 이를 통해 이메일 보안을 강화할 수 있다.   * 전송 및 수신 패턴을 프롱파일링 하기 위한 AI모델 생성 * 메시지의 어조와 감정, 스타일 분류를 사용하여 변칙적인 이메일 메시지 탐지 * 메시지의 악의적 의도 및 반복패턴 식별 * 추가 메시지 샘플을 생성하여 훈련 데이터 확장 * 실시간 업데이트 축적으로 리소스가 부족한 보안운영팀 보완   Gartner Market Guide의 이메일 보안에 대한 최신 가이드에서는 조직에 사용 중인 이메일 보안 솔류션의 기능과 효과를 재평가하고 이를 신제품과 비교하는 것이 중요하다고 한다. 즉, 새로운 공격 기법에 나오는 여러 커버리지 기술이 필요하다. | |
| --- | --- | --- |
| **QnA** | Q1. 고수준 APT 악성코드들의 경우 탐지되지 않기 위해 환경탐지, 휴먼 인터렉션 기반 로직밤 등이 적용되는 추세입니다. 이런 분석 방해 기술(트리거 기반 실행, 로직밤 등)을 무력화 하기 위한(코드 커버리지를 높이기 위한) 기존 분석기술들과 차별점이 궁금합니다.   1. 하나라도 변조되었다고 탐지하면 이는 변조된 것을 한다.   Q2. 구축 형태는 어떻게 되는지요? 클라우드? 구축형?   1. SaaS로 구성되어 있고 AWS 사용 중이다. 유럽, 미국에 이중화로 구성되어 있고, 국내 리전에 설치하는 것에 대한 검토 중이다.   Q3. 사용자한테도 악성메일이 우선은 오나요? 어떻게 보이는지 .. 아님 아얘 사용자는 악성메일 수신여부를 모르는지..?   1. 사용자에게 악성 메일이 왔다는 노티 메시지가 인박스로 가게 된다. 이를 원하면 전달 받을 수 있고 어떤 이유로 격리되었는지를 같이 전송해준다. 이 메시지는 3-5일 내 에 삭제할 수 있도록 지원한다. 첨부파일을 암호로 풀어야 하는 경우에는 사용자에게 첨부파일을 확인하기 위해 링크를 제공한다던지 인박스 메시지를 전송하는 서비스도 있다.   Q4. 탐지율이 99.5%라 했는데, 기존 솔루션 대비인지? 전반적인 공격에 대한 탐지율인건지?   1. 기존 솔루션 대비 및 전반적인 공격에 대한 탐지율에 대한 평균적인 값이다.   Q5. SoC는 어디에서 지원하고 있는가?   1. 이스라엘에서 지원하고 있고, 40명 정도의 인력이 있다. 설치의 경우에는 국내 인력이 한다. | |

## 

## 

## 

## 

## 

## 

## 

## 

## 3. AI의 속도, 정확도 및 확장성에 기반한 보안 - Microsoft Security Copilot

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| 한국마이크로소프트 / 박상준 | AI의 속도, 정확도 및 확장성에 기반한 보안 - Microsoft Security Copilot |

| **강연 내용** | 마이크로소프트는 현재 보안과 관련하여 최고의 매출규모로 성장 중이다.   * 2022년 매출규모: $20B(약 한화 26조원) * 전세계 120개 국가에서 보호하고 있는 고객수: 860K * 매일 분석하는 위협 시그널 수: 65T(65조개) * 향후 5년간 사이버보안 연구개발 투자액: $20B * 감시하고 있는 국가단위 공격, 사이버범죄 및 다른 공격자들의 수: 300 이상 * 작년에 차단한 공격 수: 70B(700억개)     [마이크로소프트 포트폴리오]  마이크로소프트는 End-to-End 구조로 이에 대한 보안을 하고 있음.   * 다음은 시큐리티, 인증 및 디바이스 관리, 규정준수 및 프라이버시 관련 솔루션 제품들이다.   + Microsoft Defender: 인프라 동적 추적   + Microsoft Sentinel: 로그 수집 및 분석   + Microsoft Endtra: 인증 관련   + Microsoft Intune: 디바이스 매니저   + Microsoft Priva: 개인정보 위험 관리   + Microsoft Purview: 데이터 거버넌스, 위험 및 규정 * 멀티 클라우드(Azure, AWS, Google Cloud Platform)를 지원한다. * 멀티 플랫폼을 지원한다.   + Android   + iOS   + Linux   + Windows   한 고객이 평균적으로 쓰는 보안 제품은 약 50-60개 된다. 이는 관리하는데 있어서 비용이 부담되고, 사용하는 방법이 제품마다 다르기 때문에 각각에 대한 학습이 필요하다. 이를 보완하기 위해 모든 영역의 보안을 포괄하는 통합 플랫폼 서비스를 제공한다.  마이크로소프트에서 제공하는 통합 플랫폼 서비스는 모든 영역의 보안을 포괄하므로 다음과 같은 장점을 갖는다.   * 다양한 보안 도구를 한눈에 쉽게 관리하고 학습할 수 있다. * 마이크로소프트 제품 및 non-Microsoft의 모든 제품에 걸쳐 동일한 데이터 모델을 적용함으로써 고객이 normalization 및 연동작업 없이도, 더 안정적인 통찰을 빠르게 얻을 수 있다. * 침해 정보, 엔티티, 및 헌팅 및 Security Copilot 등에 대해 통합된 기능과 단일 view를 제공함으로써, 공격에 대해 빠르게 대응할 수 있다. * 더 많은 데이터는 자동화, 플레이북과 AI를 통해 더 정확한 인텔리전스를 제공한다. | |
| --- | --- | --- |
| **QnA** | Q1. 데이터보호 측면에서 Purview와 EMS AIP의 차이와 각 효과는?   1. AIP는 MIP로 정보보호에 대한 부분으로 바뀐다. Purview 하위에 각 10개 정도의 제품이 있는데 이중 AIP, MIP가 포함된다. 같은 컨퍼런트라고 봐줄 수 있다.   Q2. 800개의 기업이 체험판을 쓰고 있는데, 기업별 평가는 어떤지?   1. 올해 3월부터 체험을 시작했고 200개의 기업 -> 800개의 기업으로 늘어났다. 1년에 1억 3천의 사용료를 지불하여 사용 중에 있다. 기업별 평가는 다음과 같이 크게 두가지다.  * 기존에 몇 시간 걸리던 일을 단 3분 내에 완료할 수 있었다. * 사람이 하다보면 빠트리는 일들이 있는데 그런 경우 없이 일을 모두 완료할 수 있었다. | |

# 

# 

# 

# Track E: Case Study & Trouble Shooting

## 1. 칭찬은 보안팀을 춤추게 만들고 상도 받게 만든다.

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| 두들린 / 정일권 | 칭찬은 보안팀을 춤추게 만들고 상도 받게 만든다. |

| **강연 내용** | 보안 문화 정착시키기, 더 이상 선택 사항이 아니다. 보안 문화 정착에 필요한 9가지 요소. 참여 관심 잡담 소통 격려 맞춤형 협력 설득 성취감.  정보보호의 날 행사로 입구나 엘리베이터에 포스터를 붙여 캠페인, 개발보안가이드, 보안 메시지가 담긴 선물 나눠주기 등등을 하는 등 이런 활동을 해야 한다.  정책/지침 심플하게.  결제 양식, 결재선 심플하게  아이스크림처럼 녹아드는 보안문화  칭찬.  칭찬을 아끼지 않는 모습.  칭찬문화 슬랙 문구를 딱딱하지 않고 부드럽게 만들기  칭찬하는 문화를 이용하여 보안 문화를 발전시키니 상도 받았다.    나머지는 두들린 회사 자랑하는 말 | |
| --- | --- | --- |
| **QnA** | 없음 | |

## 2. 보안왕 등극 - 높은 보안 인식과 문화를 만들기 위한 방향

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| 코인원 / 장민성 | 보안왕 등극 - 높은 보안 인식과 문화를 만들기 위한 방향 |

| **강연 내용** | 2022 내부자 위협 비용 글로벌 보고서에 따르면 내부자의 부주의 또는 과실로 인해 연간 약 660만 달러 소요.  내부자의 부주의 또는 과실 관련 위협을 줄이려면  내부자 위협 보안 솔루션을 구축 + 임직원의 높은 보안 인식 제고 = 보안 문화 정착  문화의 의미는 한 사회에서 공통적으로 나타나는 독특한 생활양식으로  보안문화를 만들기 위해서는 기업의 모든 임직원이 공통적으로 보안이라는 목적을 향해 달려가는 모습을 보여야 진정한 보안 문화라고 할 수 있다. 즉 보안 문화는 보안 부서만의 모습으로 완성될 수 없다.  코인원만의 777 보안프로그램 캠페인  매일 7시 퇴근 전, 7가지 항목을 점검하고, 매월 7일마다 검토하자  메신저를 통한 보안 캠페인 활동은 뻔하다  777보안 캠페인을 강조해서 오프라인에서도 캠페인하고 자율 권장이 아닌 자동화할 수 있는 것들은 자동화하자는 것이 목표. 그리고 잘한 크루에게 상을 줘야 한다.  의문형에서 강조형으로.  보안 캠페인 문구는 마케팅적으로 의문형으로 접근하면 관심있는 부분만 생각하게 된다. 그래서 의문형에서 강조형으로 변경.  온라인을 넘어 오프라인까지  직접적인 소통과 즉각적인 시각효과로 적극적인 참여유도.  잘 보이는 곳에 비치함으로 지속적으로 확인가능하게 한다.  보안왕 등극  보안 부서에서 보안왕같은 캠페인을 주최하다 보면 보안팀이니까 원래 보안을 강조하지.. 이런 생각을 하지만 HR부서에서 주최한다면 전사적으로 보안이 중요하다고 접근하는 구나! 라고 생각하게 된다.  보안의 게임화  자리 이석 시 PC를 잠그지 않았다면 이를 발견한 임직원으로 슬랙을 통해 특정 채널에 재미있는 메시지를 보내는 분위기.  적극적인 참여와 재미 요소  매월 둘째주 수요일은 월간보안.  매월 PC보안에 대한 경각심을 전달하고 자동 점검하여 보안성 강화.  월간 보안의 효과는 처음 366건의 보안 이슈에서 9개월 이후에는 52건으로 줄어들었다.  업무용 책상은 매일 깨끗하게.  clean Desk 감사를 통해 위규자에게는 경고를 우수 부서는 포상을 준다. | |
| --- | --- | --- |
| **QnA** | 없음 | |

## 3. ISMS 인증 여정 - 결함 및 대응에 대한 고찰

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| 자비스앤빌런즈 / 김도형 | ISMS 인증 여정 - 결함 및 대응에 대한 고찰 |

| **강연 내용** | ISMS 컨설팅 진행   * 환경 및 현황 분석 * 정보보호 관리체계 현황분석 * 취약점 점검 * 위험평가 및 보호조치 방안 수립 * 정보보호 규정 및 지침 정비   ISMS 심사준비   * ISMS 운영 명세서 준비 * ISMS 심사신청 * 예비심사 신청 * 심사 증적자료 준비   심사팀장 포함 총 5분의 심사원 참여  심사가 원활히 진행 될 수 있도록 쾌적한 심사장소 준비 필요  각 파트별 인터뷰시 별도 소규모 회의실 마련  1일차 - 서비스 소개 및 시스템 설명, 대고객 관리자 페이지 설명  2일차 - 인프라, 보안시스템, 개발보안 인터뷰  3일차 - 각 서비스별 인터뷰  4일차 - 추가 인터뷰, 결함 정리  5일차 - 확정된 결함 보고서 작성 및 종료  -> 원활한 심사 진행을 위해 내부 사전공지 필수(인터뷰 예상 대상자 지정)  -> 1일차 세부 심사일정 확정 즉시 대상자에게 일정 안내(심사 대응 자세)  -> 결함이 아닌 건에 대해서는 적극 소명, 조치 방법에 대한 확인  개인정보보호법 및 동법 시행령 개정 사항을 반영하여 인증기준 정비  - 개인정보 수집 이용, 이동형 영상정보처리기기, 가명정보 처리, 개인정보 처리 위탁, 휴면 이용자 개인정보 파기규정 삭제 등의 법 개정사항을 인증기준에 반영  (결함내용)개인정보처리방침 현행화 미흡.  개인정보처리방침에 수탁사 누락 : 개인정보보호법 제30조(개인정보 처리방침의 수립 및 공개) 미준수  -> 개인정보처리방침에 수탁사 추가 반영하여 적용  (결함내용) 일부 시스템에서 계정관리절차 미흡한 사항이 발견됨.  퇴사자 관리 계정 미흡  -> 퇴사자 발생시 인사부에서 각 시스템 계정 관리 담당자에게 즉시 공유하고 계정 삭제 완료 확인까지 즉시에 이루어지도록 프로세스화 or 계정통합관리시스템을 통한 자동화(예산필요)  (결함내용) 일부 시스템에서 계정관리절차 미흡한 사항이 발견됨  관리자 권한 과다 부여  -> 관리자 계정에 대해서 주기적인 권한부여 점검 프로세스 확립  (결함내용) 일부 시스템에서 세션 차단 미흡  관리자페이지 클로즈 시 브라우저 세션 재활용으로 재접속 가능  -> 내부시스템 접속 편의성에 의해 설정되어 있는 건으로 브라우저 세션 만료를 강제화  (결함내용)DB에 임시테이블이 존재  운영 DB에 임시 테이블이 존재  -> 운영에서 임시로 생성된 임시테이블(temp 테이블)에 대해서는 사용용도가 완료되면 즉시 삭제  (결함내용)로그 암호화 미흡  암호화가 누락된 로그 발견  -> 로그도 개인정보가 포함된 경우 암호화 필요. 생성되는 로그 중 개인정보가 포함된 로그는 암호화 처리  (결함내용) 암호화가 누락된 DB발견  DB테이블 중 암호화 누락된 컬럼 발견  -> 암호화는 했으나 우리 회사 암호화 기준에 맞지 않음. 우리 회사에 맞는 암호화 기준 수립 및 암호화 적용 (최소한의 법적요건은 지킬 것)  (결함내용) 보안성 검토 미흡  테스트단계에서 보안요구사항 적용 검토 미흡  -> QA 단계에서 보안요구사항이 반영이 잘 되었는지 확인할 수 있도록 프로세스화  (결함내용) 회사 마스킹 기준 적용 미흡  배포된 프로그램 개인정보 마스킹 정책 상이(보안성 검토 미흡)  -> 회사 개인정보 마스킹 기준 확립하고 내재화. 보안성 검토시 해당 기준에 따라 잘 적용했는지 확인  (결함내용) 접속기록 모니터링 미흡  로그 기록 모니터링 미흡  -> 특이사항 발생시 관리자에게 알람 프로세스 추가  (결함내용) 접속기록 항목 누락  개인정보처리시스템 접속기록에 필수항목 누락  -> 개인정보처리시스템 접속 로그에 필수항목 필드 추가  (결함내용) 보안시스템 정책관리 일부 미흡  불필요한 방화벽 정책 존재  -> 주기적 방화벽 정책 검토 및 불필요한 방화벽 정책 삭제. 방화벽 정책 관리 솔루션 도입(예산필요)  (결함내용) 최신 보안패치 관리 미흡  최신 보안패치가 되지 않은 프로그램 존재  -> 프로그램 버전을 현행화 목록화 하여 관리하고 자산의 중요도에 따라 계획을 수립하여 패치 적용 관리. 오픈 소프트웨어 라이선스 관리 솔루션 도입(예산필요)  (결함내용) 최신 보안패치 관리 미흡  기술지원 종료되어 패치가 지원되지 않는 OS 존재  -> 기술지원 종료 OS는 최신 OS로 전환. 즉시 적용이 어려운 경우 다른 보호대책 마련하여 적용  (결함내용) 재해복구 체계 미흡  비상대응조직 및 비상연락망 현행화 미흡  -> 비상대응조직 및 비상연락망을 항시 최신화로 유지  (결함내용) 재해복구 체계 미흡  RTO 및 RPO 기준이 중요도에 따라 분류 되지 않음.  -> 시스템 중요도에 따라 RTO(Recovery Time Objective)와 RPO(Recovery Point Objective)를 수립하고 적용  개인정보보호법 상 원칙을 중심으로 인증기준 체계 정비  - 구체적이고 세부적인 점검 사항을 기술한 인증항목(개인정보 표시제한 및 이용 시 보호조치(3.2.3)를 삭제하고, 응용프로그램 접근(2.6.3), 업무환경 보안(2.4.7), 가명정보 처리 (3.2.4) 항목 하위의 세부 점검항목으로 분산 이관  2024년 9월 15일까지 유예기간이 있는 ISMS 항목들도 존재.  ISMS-P 인증 유지를 위해서는  -> 매년 심사를 진행하더라도 결함은 나올 수밖에 없는 부분  -> 발견된 결함뿐만 아니라 통제항목 각각에 대해서도 결함이 최소화되도록 지속적으로 관리체계를 운영해야 함. | |
| --- | --- | --- |
| **QnA** | 없음 | |

# 

# 

# Track F: 클라우드

## 1. 클라우드 보안, 어디서부터 시작해야 하나?

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| Google Cloud Korea / 서진원 Security Specialist | 클라우드 보안, 어디서부터 시작해야 하나? |

| **강연 내용** | 1. 구글 클라우드 다단계 보안 통제 방안   IAM Grant, IAM Deny, VPC Service Controls & Firewalls, Org Policy, Tags, Policy Intelligence  Org Policy: 사용자가 아닌 리소스를 통제하는것 조직의 정책은 상향에서 정할 수 있고 폴더까지 적용 상위관리자가 보안정책을 지정하면 하위 사용자까지 모두가 적용된다. 조직의 정책은 프로젝트 관리자라도 건드릴 수 없다. 조직정책은 리소스이 전체 수명 주기를 지원하며 구성에대한 허용 거부하는 효과적인 가드레일을 설계한다. 정책을 확인한 후에만 리소스배포가 가능하고 규칙 위반과 효과적인 정책에 역행하는 리소스를 탐지한다.   1. 조직 정책 형식   1) Built-in Policies: Easy to enforce pre-defined policies for GCP resource configurations based on best practices and red team findings 110+ built-in constraints of boolean and list types.  2) Custom can create and manage their own tailored constraints   1. 구글 클라우드의 Recommend기능   사용자가 할당된 업무에 비해 너무 많은 권한이 주어져있는지 파악 가능함. 3개월 동안 사용자 계정을 분석하여 사용하지 않는 기능이지만 권한이 허락된 것에 대하여 권한 삭제를 Recommend기능이 있음 | |
| --- | --- | --- |
| **QnA** | Q1. 미국의 클라우드 환경과 우리나라 클라우드 환경에 대해서 비교해 달라   1. 미국의 경우 국방부도 클라우드 서비스를 도입하려한다. 우리보다는 앞선 환경이 조성되어 있다. 민감한 발언이기에 조심스럽지만 우리나라 공공기관 클라우드 안전성평가는 인프라기반의 보안정책이다. 미국의 공공기관은 클라우드 안전성평가에 인프라 보다는 데이터 중요도에 집중해야한다.   Q2. 클라우드 환경에서 컨테이너 이미지의 보안정책과 관리방법이 궁금하다.   1. 골든이미지(골든 이미지는 OS 영역을 포함해 필수 패키지가 설치된 일종의 표준 이미지 개념)를 내부적으로 관리하고 오브젝트 컨테이너에 올린다. 소스코드부터 배포하는 과정까지의 SDS solution이 매우 강력하다. | |

## 2. AWS환경의 침해사고 식별과 시나리오기반 대응 방안 사례 공유

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| Amazon Web Services / 한현상 Manager | AWS환경의 침해사고 식별과 시나리오기반 대응 방안 사례 공유 |

| **강연 내용** | 1. 목차   1) AWS 사고대응  2) AWS 사고 식별  3) AWS 사고 대응의 자동화 아키텍처  4) Q&A   1. AWS Professional Service의 목표   1) 고객의 비즈니스 아웃컴을 구축하기 위한 빌더  2) 효율적인 확장성을 위해 설계된 올바른 베스트 프랙티스 기반 구축  3) 실제 제공하고 있는 200개 이상의 오퍼링  4) 모범사례 / 고객의 전환 가속화 레거시 플랫폼의 현대화 지원  5) 프로서브&파트너와 협력을 통하여 고객의 전환을 지원  6) 보안, 규정 준수, 가용성 보장   1. AWS 환경의 사고영역   1) 서비스 영역: AWS 계정, IAM권한, S3버킷, 빌링  2) 인프라 영역: VPC리소스, EC2 데이터와 프로세스, 컨테이너, 연결성 리소스  3) 어플리케이션 영역: 애플리케이션 코드, 서비스 또는 인프라에 배포된 소프트웨어   1. AWS 환경에 대한 사고대응 주요 차이점   1) 공유 책임 모델기반 보안 영역 이해  2) 빠르게 변화되는 클라우드 환경  3) 클라우드 서비스 영역  4) 데이터 액세스  5) 인프라 프로비저닝을 위한 API  6) 자동화   1. AWS 사고 대응의 자동화 아키텍처   사고대응 자동화 프로세스  1) 격리 단계 - SECURITY GROUP 변경을 통한 네트워크 격리    2) 대응 단계 - 라이브 상태에서의 메모리 덤프 수행  3) 분석 단계 - 스냅샷에 대한 상세 분석 자동화 수행  4) 종료 단계- 사고대응 자동화 완료 & 사고 인스턴스 종료 및 신규 인스턴스 복원   1. Summary   1) AWS IR 영역의 이해: 인프라, 서비스, 어플리케이션  2) 이해관계자 협업: 각 팀별 협업 담당자의 R&R이해, 사고 대응의 프로세스 정립과 공유  3) 자동화: AWS Security 고도화는 자동화, 자동화의 구성 이후 보안 담당자의 추가 시나리오 고려  4) IR서비스 활용: 위협을 탐지하거나, 잠재 위협을 평가할 수 있는 서비스 활용  5) 보안 담당자의 대응 커버리지 확대: 사람, 프로세스, 기술을 고려 | |
| --- | --- | --- |
| **QnA** | QnA 시간 관계상 생략 | |

## 

## 3. NCSOFT의 Public Cloud 보안통제 및 모니터링 사례

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| NCSOFT / 이정현 팀장 | NCSOFT의 Public Cloud 보안통제 및 모니터링 사례 |

| **강연 내용** | 1. Agenda   1) Public Cloud 공동 책임 모델  2) Public Cloud의 보안, 인증 및 규정 준수 서비스  3) GCP/AWS 보안 모니터링 서비스 소개  4) 다중 계정을 사용하는 이유  5) 다중 계정 환경에서의 보안 고려사항  6) AWS 보안 서비스 도입 배경 / 주요 검토사항  7) NCSOFT Mint 아키텍쳐 소개/운영  8) NCSOFT Mint 도입 과정 및 결과  9) 추가활용 계획   1. 공동 책임 모델   고객과 AWS공동 책임모델을 가져야함     1. 다중 계정 환경   여러 팀, 다중 어플리케이션, 빌링, 격리와 보안  => 성장에 따라 지속적인 운영에 영향을 주지 않으면서 환경을 안전하게 확장 가능  다중 계정 환경에서의 보안 고려사항: 중앙집중적인 사용자 관리, 신규 계정에 대한 보안 기본 구성 설정, API 사용 및 리소스 설정 사항 보관, 보안 취약점, 위반 사항에 대한 점검   1. MINT 운영   템플릿 대시보드를 사용하여, 쉽고 빠르게 대시보드 구성 가능  알람 기능으로 AWS SNS, Chime, Email 으로 탐지 이벤트 전달  S3 버켓, GuardDuty 탐지내역 확인 가능  AWS WAF를 사용하고 있다면 AWS AWF로그를 통합하여 구성 가능하다.   1. NCSOFT Mint 도입 결과   AWS환경의 보안 현황에 대한 통합 가시성 확보  빠르게 대용량 이벤트 로그를 모니터링 대시보드 구성  AWS 보안 서비스가 신규로 추가될 시, 손쉽게 통합 가능 | |
| --- | --- | --- |
| **QnA** | Q1. 각 계정에서 발행하는 보안 관련 비용은 어떻게 처리되나요?   1. AWS클라우드 인프라를 관리하는 팀이 비용에 대해서 정리한다. 오픈서치등을 이용하면 가격이 발생된다. 보안팀에서도 어느정도는 비용처리하지만, 그 이상은 비용청구를 한다. 오픈서치 한달에 100기가 정도 무료인데, 이벤트가 많아 용량증설 등의 비용이 발생하는 경우가 있다.   Q2. 보안 취약점 및 위반 사항에 대한 점검의 경우 AWS서비스 자체에 의존하나요 혹은 신규 패턴 등을 추가, 수정하여 사용하시나요?   1. 커스텀을 통해 하나의 서비스로 구성하는데 AWS의 GuardDuty등에 의존하고 있다. 클라우드에 AWS뿐만이 아닌 클라우드 자체적인 솔루션이 있지만 네이티브 서비스가 아니기에 통합하지는 않지만, 자체개발 솔루션 환용 계획은 있다. 기본적으로 AWS이용하지만 다른 탐지는 써드파티 솔루션을 이용한다.   Q3. Mint로 인해 효과가 구체적으로 무엇인지?   1. 우선적으로 가시성이 좋아짐. 해킹을 실제 방지한 사례는 없다. 만약 실제 해킹이 발생하는 경우에는 AWS사고대응을 그대로 Mint에서도 그대로 적용될 것이다. 모의해킹만 이루어 지고 있다. | |

# 

# Track G: Hot issue

## 1. 현재 사이버 보안의 가장 중요한 변화 - SASE 활용을 통한 보안 도전 과제 해결 방안

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| Netskope / Eli Jang | 현재 사이버 보안의 가장 중요한 변화  - SASE 활용을 통한 보안 도전 과제 해결 방안 |

| **강연 내용** | 최근 화제가 되고 있는 이슈는 다음과 같다.   1. 하드웨어 중심의 복잡한 네트워크 보안으로부터의 탈피 2. 기존 VPN을 대체하여 완벽하고 안전한 사용자 경험 제공 3. 솔루션 벤더를 줄임으로써 비용 절감 달성 4. 제로 트러스트 아키텍처 채용으로 공격 대상 영역 축소 5. 리스크와 복잡성을 증가시키지 않고 하이브리드 워크 지원 6. DC를 중심으로 한 Perimeter 중심의 NW에서 인터넷 브레이크아웃로 전환   클라우드와 DX에 의한 인터넷 통신에서 다음과 같은 엔드포인트들의 변화들이 발생하고 있다. 이로 인해 다양한 엔드포인트들을 어떻게 제어하는지가 이슈로 남아있다.   * 60% 이상의 통신이 SaaS/Cloud이다. * 쉐도우 IT에 대해 파악되고 있지 않다. * 50% 이상의 위협이 클라우드를 사용하고 있기 때문에 Cloud가 공격 타겟이 되고 있다. * 95%의 통신이 암호화를 사용하고 있으므로 이러한 암호화 통신을 보지 않으면 위협에 노출될 수 있다.     네트워크와 보안을 통합한 것이 SASE다. SASE(보안 액세스 서비스 엣지)는 WAN 엣지 서비스 + 보안 서비스 엣지(SSE)로, 모든 네트워크 최적화 및 보안 서비스를 제공한다. | |
| --- | --- | --- |
| **QnA** | Q1. 기존 보안 솔루션 구성 대비하여 연간 비용이 얼마나 감소 되나요?  Q2. 꼭 Agent 방식으로 구성해야 하나요? 만약 Agent-less 방식을 사용하게 되면 다른 보안 기능인 ZTNA, DLP, 회사의 이메일 등과 같은 서비스는 임직원이 어떻게 제공 받을 수 있을까요?  답변은 시간 관계상 생략. | |

## 2. 하이브리드 환경에서 통합 아이덴티티 구현을 통한 IT 현대화

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| Okta Identity Korea / 장희재 | 하이브리드 환경에서 통합 아이덴티티 구현을 통한 IT 현대화 |

| **강연 내용** | 모든 IT Admin의 현실은 하이브리드 IT다. 온프레미스 환경만 사용하는 회사나 클라우드만 사용하는 회사는 없다.  하이브리드 IT 환경에서 아이덴티티 관리의 딜레마   * 통합 인증(SSO): 웹 표준 vs. 기존 방식   + 웹 표준 기반의 통합 인증 연동   사용자 교육, 관리, …을 진행하기 위해서는 하나의 솔루션만으로 힘들기 때문에 여러 솔루션을 사용해야 한다.   * + 기존 방식의 통합 인증 연동   가장 일반적으로 사용하는 솔루션은 자사에서 기존에 가지고 있는 온프레미스 SSO 시스템이다.   * + 인증 수단별 인증 신뢰도   인증 수단 중에서 패스워드가 가장 취약한 것으로 알려져있다. 사용자를 아무리 교육해도 개인적으로 동일한 패스워드를 사용하면 취약할 수 밖에 없음.   * 2차 인증(MFA): 보안 강화 vs. 사용자 편의성   + End 입장에서는 사용자 편의성에 문제가 있을 수 있음 -> 이를 어떻게 해결할 수 있을지? * 계정 관리 자동화   + 사용자를 만들어주는 관리로, 사용자 계정 관리 및 라이프사이클 관리까지   + 입사, 퇴사, 부사 변경 행위가 일어날 때 각 회사의 비즈니스 프로세스에 대해 아이덴티티 솔루션을 어떻게 적용할 수 있는지   온프레미스에서는 DB에서만 관리하면 되었지만, 다양한 서비스를 사용하게 되면서 SaaS 솔루션들을 사용함에 따라 각각의 별도 아이덴티티를 만들고 관리하는 것이 필요하다.  여러 클라우드 솔루션을 통합해서 하나의 솔루션으로 쓸 수 있도록 만드는 것이 Okta의 솔루션 개발 목적이다. | |
| --- | --- | --- |
| **QnA** | 없음. | |

## 3. K8s 환경에서의 제로트러스트 마이크로 세그멘테이션(가시성과 보안정책 실행)

| **기업명 / 강연자** | **강연 주제** |
| --- | --- |
| Akamai Technologies / 신기욱 | K8s 환경에서의 제로트러스트 마이크로 세그멘테이션(가시성과 보안정책 실행) |

| **강연 내용** | 애플리케이션을 어디서 구동을 시키는가가 중요한 문제로 잡히게 되었다. 쿠버네티스 환경과 같은 새로운 인프라 환경으로 변화하는 환경에는 보안 문제가 없는지 변화에 대해 검토하는 것이 필요하다.  쿠버네티스 환경으로 대부분 이동해가고 있다. 컨테이너 및 쿠버네티스에 대한 가장 큰 우려사항은 보안이다. 사용자들 중 한번 이상의 보안 사고를 경험했거나, 보안 투자가 충분치 않다는 등의 의견이 있다.  현재 쿠버네티스의 사용에는 다음과 같은 어려움이 있다.   1. 가시성의 어려움  * 기존에 있는 네트워크 툴로 보는것이 어려움. * 어떤 트래픽들이 어떻게 움직이는 지 상황을 파악하는 것이 어렵다.  1. 정책  * 쿠버네티스의 룰로는 native policy 기능 사용이 어렵다. * 소규모 -> 대규모에서는 정책 관리가 불가능하다.   [Gartner의 위험 기반 워크로드 보호 제어 계층 구조]  Modern Workload에서 가시성과 마이크로세그멘테이션은 방화벽과 함께 최신 워크로드를 보호하기 위한 핵심 요구사항이다.  이때 Segmentation이란 분할 기법으로 전형적인 Lateral Movement다. 만약 Segmentation이 없다면 실제 보안사고가 일어나면서 다른 네임스페이스로 건너가서 문제가 발생한다던지 등의 사고가 점차 퍼지게 된다. Segmentation Rule이 있어야 사고가 퍼지지 않는다. 즉, 사고의 측면 이동을 차단하는 것이다. | |
| --- | --- | --- |
| **QnA** | 없음. | |

## 

## 