클라우드 심층방어 DID

이용준 (극동대학교), 이기호(극동대학교)

1. 국내 · 외 사이버 공격 동향 및 사례

2022년, 사이버 공격은 랜섬웨어 조직의 활동과 가상 자산의 공격으로 요약 가능하다. 공격 그룹으로는 브라질 보건부, MS 소프트, 앤비디아 등 유수의 기업과 옥타와 같은 보안 전문 기업을 해킹한 랩서스, 코스타리카, 페루 정부기관, 캐나다 민간 군사훈련 기업 등을 대상으로 사회공학적 기법을 통해 내부 침투를 시도한 콘티와 락빗이 있다.

2023년에는 북한 해킹 조직의 글로벌한 공격이 감행되었고, 매크로 차단 정책의 영향을 받자 LNK 파일을 활용한 공격으로 전환하는 모습도 보였다. 또한, 클롭 조직의 고애니웨어 취약점을 통한 공격과 무브잇 트랜스퍼 제로데이 취약점을 활용한 공격, 러-우 전쟁과 이스라엘-하마스 갈등 등 국제 정세의 악화 속에서 사이버전이 확산되는 양상도 있었다. 2023년 말에는 웜 GPT와 프라우드 GPT 등 악의적인 목적을 가진 생성형 AI가 등장하기도 하였다.

2024년도에는 E-Sports인 리그오브레전드 LCK 스프링 시즌 경기 중 디도스 공격이 발생하여 약 7시간 동안 경기가 지연되기도 하였고, 크로노스 작전을 통해 록빗 랜섬웨어 조직을 소탕하기도 하였다. 다만, 록빗 조직은 5일만에 백업 데이터를 이용하여 다크웹 사이트를 복구하였다.

또한, CI 소프트웨어인 팀시티의 온프레미스 플랫폼에서 취약점(CVE-2024-27198, CVE-2024-27199)이 공개되기도 하였다.

사례로는 첫 번째, SEGA 보안사고 사례가 있다. SAGA 보안사고는 AWS S3 버킷에 민감파일이 저장되어 제3자가 버킷 정보를 이용한 사고이며, 버킷에는 데이터 접근이 가능한 키와 자격 증명 등이 포함되어 추가 피해가 예상되었으나 신속한 대처로 대응 프로세스 모범 사례로 꼽힌다. AWS S3 버킷 구성오류 보안 사고는 최근에도 발생하는 사고이며, 관리자 실수나 구성을 통한 문제로 사고가 야기되므로, 버킷 설정과 정상 동작 여부, 이상접근 모니터링이 필요하다.

두 번째는 캐피탈 원의 보안사고 사례이다. 퇴직한 근무자가 SSRF 취약점을 악용하여 AWS 서버를 공격해 14만 명의 사회보장번호와 8만 여개의 은행 계좌 정보를 탈취한 사건이다. 클라우드 내부 서비스는 서로 네트워크로 연결되어 SSRF 공격에 취약한 점을 이용했으며, 공격자는 익명화를 위해 토르 네트워크를 이용, 여러번의 접근 시도를 하였고 캐피탈 원은 이에 WAF 보안 정책을 설정 하였으나 잘못된 구성으로 차단되지 않았다.

세 번째는 미국 수자원 시스템 공격이다. 미 환경보호청 EPA는 미국 전역의 상하수도 시설에 대한 사이버 공격이 빈번해지고 있다며 24년 5월 20일 발표하였다. 상하수도 시설 검사 대상 중 약 70%가 사이버 위협을 방지하기 위한 기준에 미치지 못한 것으로 확인되었으며, AP통신은 웹사이트 다운이나 훼손, 시스템 운영 자체를 표적 삼는 경우가 있으니 주의해야 한다고 발표하였다.

네 번째로, 유나이티드 헬스의 자회사인 체인지 헬스케어를 랜섬허브 불법 단체가 공격하여 확보한 데이터를 공개하기 시작한 사건이다. 체인지 헬스케어는 정황상 범인들에게 몸값을 지불한 것으로 보이나, 랜섬허브 파트너 중 노치라는 조직이 데이터를 통해 몸값을 받았음에도 다시 한 번 협박하며 사태가 복잡화되었다. 랜섬웨어 조직에 대한 몸값 지불은 신뢰하지 말아야 한다는 주장이 더욱 명확하게 입증된 사례이다.

2. 클라우드 보안 위협

CSA에서 발표한 클라우드 컴퓨팅에 대한 주요 위협에서는 클라우드 환경의 보안 위협을 크게 관리 및 기술적 관점으로 분류하였다.

관리적 측면에서는 클라우드 보안 관리체계 부재와 휴먼에러의 문제가 두드러진 반면, 기술적 측면에서는 클라우드 전환에 따라 API나 공급망에서 시스템 취약점, APT 공격으로 인한 연쇄적 보안 위협이 증가하였다.

클라우드 보안 위협은 4가지 항목으로 세분화 가능하다.

그 중 첫 번째는 '보안 체계 및 전략과 관리 미흡'이다. 이는 클라우드에 맞는 보안 구조나 전략의 부재, 그리고 관리 방안의 미흡으로 인한 문제이며, 아키텍처 설계 및 데이터의 흐름이나 접근체계 구성 등 클라우드 환경에 알맞은 보안 거버넌스나 아키텍처가 부재한 경우 침해사고로 이어질 수 있음을 의미한다.

두 번째는 '클라우드의 데이터 유·노출'로, 자의적이거나 타의적인 문제로 클라우드에 저장된 데이터가 공개되는 문제이다.

클라우드에 저장된 크리덴셜 API나 민감정보가 유출되는 경우 2차 피해가 발생할 수 있으니 유의하여야 한다.

세 번째는 '인프라의 확대와 소프트웨어의 공급량 증가'인데, 위협 요소로 안전하지 않은 소프트웨어 개발과 서드파티 리소스 보안 해제, 시스템 취약점 등이 있으며, 오픈소스 취약점, 공급만 취약점, 제로데이 취약점으로 인해 위협이 발생한다.

클라우드 환경에서 소프트웨어 생명주기를 고려하지 않은 위협으로, 클라우드 안에서 운영되는 소프트웨어는 온프레미스와 마찬가지로 정적 분석과 동적 분석을 통한 위험 요소 제거 활동을 수행해야 하는데 소프트웨어 개발 패러다임과 맞물리면서 API나 패키지 등 서드파티 사용이 증가함에 따라 클라우드 환경에서도 영향을 미칠 수 있게 된다.

네 번째는 '사이버 범죄 증가'이다. 범죄조직이나 해커, APT에 의해 위협 요소가 생성되며 발생 원인은 해킹 단체와 APT 위협 증가에 있다. 앞서 살핀 위험 요소들의 악용 가능성이 높아짐에 따라 공격자들의 타깃이 변화하였으며, 사이버보안 전문 업체를 통해 대응 가능하다.

이 외에도 클라우드 보안 위협에서는 '보안체계 전략과 관리 미흡'으로 인한 위협이 존재하며 4가지로 분류가능하다.

그 중 첫 번째는 '부적절한 ID와 자격증명, 접근 및 키 관리'이다. 접근 통제에 영향을 미치는 ID나 자격증명, 키 관리 등의 미흡으로 인하여 데이터 유·노출 사고가 발생할 수 있으며, 접근 제한된 데이터에 접근이 가능해지는 경우도 발생한다. 이는 프로비저닝이나 디프로비저닝 과정에서 자원의 권한과 접근 범위를 점검하고 지속적인 모니터링을 통해 대응 가능하다.

두 번째와 세 번째는 '구성 오류와 적절하지 못한 변경 통제'이다. 부적절한 컨테이너 설정으로 자격증명 노출과 인가받지 못한 접근이 허용되는 문제로, 보안 강화를 위해 SCP, 솔루션을 적용하여 지속적인 변경 통제가 필요하다.
부적절한 클라우드 구성은 클라우드 아키텍처에 대한 낮은 이해도와 기술 성숙도 저하로 인해 발생할 수 있는 문제로, 클라우드 내 서비스 변화에 대한 모니터링과 서비스 배포 전/후 모의 침투 등 점검을 통해 부적절한 상황을 확인해야 한다.

네 번째는 '클라우드 보안 아키텍처 전략 부족'과 '잘못된 구성, 서버리스의 취약점 및 컨테이너 워크로드'이다. 이는 클라우드 보안 전략과 관리 규정의 현행화가 중요시 된다. 이는 클라우드 보안 전략과 관리 규정의 현행화가 중요시 된다.
두 개의 보안 위협은 클라우드의 복원력 및 저항성에 영향을 미칠 수 있으므로, 클라우드 서비스나 인프라 설계 시 거버넌스·컴플라이언스 등 다양한 요소를 고려해야 한다.
클라우드 보안 아키텍처 및 위협 모델링 프로세스는 CSA에서 제시하는 보안 인프라 전략을 참고하면 좋다.

클라우드 데이터 정보 유·노출은 '안전하지 않은 인터페이스나 API'와 관련되며, API의 사용량 증가와 연관되어 있다. 아카마이의 2021 보고서에 따르면 20년 대비 API 사용량은 53% 증가하였으며, 이는 보안 위협으로 이어질 가능성이 높다.

인터페이스나 API는 기능이나 보안 위협들을 식별하기 어렵기 때문에, 소프트웨어 개발 시 시큐어 코딩 적용과 SAST, DAST 등을 수행하거나 WAAP 솔루션을 적용하는 것이 좋다.

클라우드 데이터 정보 노출 및 유출 시 '우연한 클라우드 데이터 노출'의 사고는 클라우드 환경에서의 가시성의 부재와 데이터 관리의 미흡으로 인해 종종 발생하는데, 멀티나 하이브리드 클라우드로 구성된 서비스의 경우 클라우드 간 보안 가시성이 저하되면서 네트워크 보안 미흡과 설정 오류로 인한 데이터 유출 가능성이 존재한다.

따라서, 클라우드 서비스 운영을 위해서는 교육 및 정책 제시를 통해 유출로 인한 문제 최소화가 요구되며 클라우드 DLP 등을 통해 데이터의 흐름을 분석하고 데이터 유·노출 여부를 점검하는 것이 필요하다.

또한, '클라우드 저장소 데이터 유출'사고의 경우 내부 임직원 대상 피싱이나 보안 아키텍처를 대상으로 하는 공급망 공격에 의해 발생하는 경우가 잦다.
클라우드 전환이 가속됨에 따라 데이터 정보 유출 문제는 지속 증가할 것으로 전망되므로 클라우드 환경에 최적화된 데이터 유출 위협 및 사고대응 계획 수립이 필요하다.

'안전하지 않은 소프트웨어 개발'과 '시스템 취약점'은 SDLC와 관련되어 있는데, 소프트웨어 보안 강화 및 SBOM 등을 통한 소프트웨어 구성 요소의 투명성을 확보해야 한다.
SSDLC(시큐어 소프트웨어 디벨롭먼트 라이프 사이클)를 구현하기 위해서는 소프트웨어 요구사항, 분석, 설계, 구현을 거쳐 단계별 검증과 테스트를 수행해야 하며, 이 외로는 KISA의 시큐어 코딩 가이드라인을 참고할 필요가 있다.

또한, 사이버 범죄의 증가와 관련하여 스태티스타(Statista)의 발표 자료에 따르면 조직 근무체계 및 국제 정

세의 급격한 변화로 인해 사이버 공격 비중은 점차 증가하는 추세에 있음을 알 수 있다.

업무체계의 변화로 인한 원격 근무의 확산은 VPN이나 RDP 등 원격 접근 환경의 증가로 이어졌으며, 내부 시스템에 접근할 수 있는 포인트로 악용될 가능성이 높아졌고, 국가지원형(북한, 중국, 러시아 등)사이버 공격의 증가로 인하여 클라우드 피해 규모가 커지면서 범죄조직, 해커, APT로 인한 클라우드 보안 위협도도 증가하였다.

이에 따라 보안을 위한 인프라 가시성을 확보하고, 인텔리전스 분석을 통한 선제적 보안 대응 체계가 요구된다.

3. 클라우드 보안 인증제 CSAP (Cloud Security Assurance Program)

- 목적 및 근거

CSAP는 국가 및 공공기관에서 안전성 및 신뢰성이 검증된 민간 클라우드 서비스 공급을 위해 만들어진 인증 제도이다. 공정한 클라우드 서비스 보안인증제도 실시를 통해 이용자의 보안 신뢰도 상승과 클라우드 서비스 경쟁력 확보를 목표로 한다.

추진 근거는 「클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률」 제5조에 의한 「제1차 클라우드컴퓨팅 기본계획」(15.11.10. 국무회의)에 따른 클라우드 서비스 보안인증제도 시행이다.

- 인증 개요

클라우드 서비스 보안인증제도의 인증 유형은 IaaS, SaaS, DaaS이며, SaaS는 표준, 간편등급으로 나눠져 있다. 인증 등급은 상/중/하로 구분되며 평가 종류는 최초/사후/갱신 평가가 존재한다.

인증 유형 세 종류와 등급의 유효기간은 5년으로 제한된다. 최초평가는 처음으로 인증을 신청하거나 인증 범위에 중요한 변경이 있어 다시 인증을 신청할 때 실시하는 평가, 사후평가는 보안인증 취득 이후 지속적으로 보안 인증 기준을 준수하는지 확인하기 위한 평가, 갱신 평가는 보안 인증 유효기간이 만료되기 전 보안 인증 유효기간 연장을 원하는 경우 실시하는 평가이다.

IaaS, DaaS 인증은 서면/현장평가/취약점 검점 5일, 모의 침투테스트 5일, 이행점검 5일 총 15일이 소요되며, SaaS 표준등급은 이행점검 4일로 총 14일, SaaS 간편등급은 서면/현장평가/취약점 점검 4일, 모의 침투테스트 4일, 이행점검 3일로 총 11일이 소요된다.

또한, 하등급 평가는 총 14일, 하등급 SaaS는 총 11일이 소요된다.

4. 클라우드 SOC(Security Operation Center) 기술동향

클라우드 SOC는 기존에는 보안시스템 모니터링, 취약점 진단, 보안관제, 통합 보안관제 시스템이 포함된 단위 보안관제와 통합 보안관제인 ESM을 거쳐 자산 및 취약점 관리, 정보 공유 및 관제 활용, 사고 대응 관리, 빅데이터 보안 관제 시스템을 포함하는 빅데이터 SIEM, 그리고 현재는 MITRE ATT&CK 기반 분석, SOAR 기반 사고처리 자동화, AI 기반 포안관제, 네트워크(NDR)과 엔드포인트 기반 침해대응 고도화가 포함된 지능형 및 자동화 보안관제 시스템이 대세로 부상했다.

SOC에서 SIEM은 데이터를 수집, 저장, 검색, 탐지, 분석, 대응하는 것으로 로그를 통합적으로 수집하는 것을 목표로 한다. 저장 영역은 SIEM에서 수집된 로우 데이터를 빅데이터 데이터 베이스에 저장하는 것으로 빅데이터 DB 엔진을 필요로 한다.

또한, 검색 영역은 빅데이터 DB를 통해 원하는 조건을 빠르게 조회하는 것을 기본으로 한다.

- SIEM과 AI 시스템의 결합

대부분 기업의 SIEM 보안 관제 인원으로는 현재 수많은 경보 이벤트를 분석하는 것이 현실적으로 어렵다.

전체 보안 로그에서 관제인원이 수동으로 대응할 수 있는 영역은 SIEM 임계치 기반 경보 이벤트 중 1% 이내로 보고 있으며, 인공지능 기계학습을 통한 자동 분석 영역이 추가될 경우 60%, XDR 확대 필요 영역이 39%가량 되는 것으로 보고 있다.

이렇듯, 이벤트 분석과 대응을 100% 따라가기 어렵다는 것은 보안 공백이 필연적으로 발생하는 것을 의미한다.

이러한 문제점을 인공지능 시스템을 이용해 보안 관제 인원이 분석 및 대응하지 못하는 경보 이벤트에 대해 AI 학습 데이터를 기준으로 정오탐 자동 판단이 가능하다.

또한, SIEM에서는 임계치 기반의 정해진 조건으로만 탐지룰을 설정하고 있으나, 인공지능에서는 AI 알고리즘을 통해 이상행위 판단도 가능하여 실제 운영 중인 기관을 사례로 보았을 때 경보 이벤트 분석 및 대응 건 수가 30배 이상 올라간 효과를 보이고 있다.

- SIEM과 EDR/NDR의 결합

XDR의 X를 확장으로 요약했을 때 가장 대표적으로 이야기되는 보안 시스템은 엔드포인트인 EDR과 네트워크인 NDR이다. 이 솔루션은 이미 SIEM을 통해 통합적으로 보안 로그를 수집하고 있었으나, 최근 XDR 개념에서는 보안 로그 수집을 넘어 인공지능 시스템의 학습 데이터로 활용이 이루어 지고 있다.

EDR 보안 로그의 특성을 파악하여 인공지능 위협 모델에

적용하였을 때, 랜섬웨어 탐지 위협 모델과 시스템 프로세스의 이상행위 탐지 위협 모델 등으로 적용이 가능하다.

- SIEM과 SOAR의 결합

자동화 시스템인 SOAR은 반복적으로 발생하는 보안 이벤트 처리를 자동화 함으로써 인력이 투입되는 시간을 줄이고 더 많은 이벤트 처리를 가능하게 돕는다.

SOAR 구축 기업에서는 하루 1,900건의 이벤트 처리량을 8,400건으로 약 4.5배 증가 시키기도 하였다.

- XDIR을 통한 통합보안 관제 플랫폼

XDIR은 확장형 탐지 조사 대응이 가능한 기술로 eXtended(익스텐디드), Detection(디텍션), Investigation(인베스티게이션), Response(리스폰스)의 줄임말이다.

최근 보안 위협은 SIEM만 활용하기에는 어려움이 있어 MITRE ATT&CK TTP 전술 등을 활용하는 등 포괄적 관점에서 보안 운영을 시도하고 있기에, SIEM을 중심으로 XDR이나 XDIR 개념으로 통합 운영이 필요하다.

국내 SOC의 경우 SK 쉴더스, 안랩, 이글루 코퍼레이션 등 국내 유수의 보안 기업들이 운영 중에 있으며, SK 쉴더스는 유럽 1위 이동 통신사인 도이치 텔레콤의 보안 부문 자회사와 상호 협력 의향서를 체결하고 디지털 인프라 방어 체계 고도화에 협력하기로 하였다. 안랩은 클라우드 보안관제 서비스를 통해 침해대응(CERT)전문 인력이 원격으로 상시 실시간 위협을 탐지하는 운영 서비스를 제공하는 방식의 사업을 진행 중이다.

5. 글로벌기업 Cisco 클라우드 보안 사례

시스코는 심층 방어 보안에 대해 다섯 가지 과제와 대응 방안으로 나눠 설명하고 있다.

첫 번째는 암호화 트래픽에 대한 보안 대책으로 '암호화 트래픽으로부터 악의적인 공격을 감지'한 경우이다. 이때 대응 방안으로는 ETA 솔루션과 시스코가 만든 스위치, 라우터, 넷플로우 기술, 시스코 스틸스워치와 연계한 네트워크 보안 센서화를 통해 보안 위협 피해 최소화를 위한 인텔리전트 네트워크를 실행하는 것이다.

두 번째는 '악의적인 웹 사이트 접속 방지'이다.

원격 접속 사례가 늘어남에 따라 보안 리스크가 증가하고, 멀웨어 감염 등으로 악의적인 외부 사이트에 액세스를 시도할 경우 신속한 차단이 어려운 부분에 주목을 하였다. 이에 시스코는 악의적인 사이트에 대한 접속을 DNS로 차단하는 클라우드 보안 서비스 Umbrella로 내 외부를 막론하고 모든 사용자를 보호할 수 있는 기능을 대책으로 세웠다.

세 번째로는 '클라우드 보안 CASB 대응'이다. 클라우드 어플리케이션 이용 시 사용자 계정 등 틀을 넘어 공유되는 데이터를 보호하거나 어플리케이션 자체의 사기성 등에 대한 리스크 대책을 세우는 것이다.

이에 시스코 클라우드 접근 보안 중계 CASB인 시스코 클라우드 락 서비스는 클라우드 환경에서 사용자 보호, DLP, 잘못된 어플리케이션 검출 및 제어를 실현하여 대응할 수 있다.

네 번째는 '고도화된 표적형 공격 대응'으로 멀웨어와 랜섬웨어로 대표되는 표적형 공격을 말한다. 이러한 공격은 감염 경로를 확인할 수 있는 EDR 기능 뿐만 아니라 감염 후 대응이 중요하다. 또한, 네트워크 레벨과 단말 레벨의 대책을 연계 하는 것이 중요하다.

이에 대해 안티 멀웨어 솔루션인 시스코 어드밴스드 멀웨어 프로텍션(AMP)을 제공하여 네트워크, 콘텐츠, 엔드포인트, 모바일 단말 등 각각 대응 가능하도록 하는 대책을 강구하였다.

마지막으로 'IoT 봇넷을 이용한 공격 대비'이다. 각종 센서나 제조 설비, 의료기기에서 가전제품에 이르기까지 다양한 장비와 연결되므로 장비 단위의 보안에는 제약과 한계가 존재한다. 가전 제품 등을 발판으로 한 사이버 공격도 현실화되어 시스템 전체의 안전성 유지가 어렵다.

이에 세그멘테이션, 가시성과 분석, 안전한 원격 액세스 등 복수의 아키텍처를 조합한'IoT 보안 솔루션 '과 고도의 보안 서비스를 통해 네트워크 관점에서 다양한 IoT 장비를 보호하여 비즈니스를 추진할 수 있는 체제 조성을 지원하는 방안을 세웠다.

6. 글로벌기업 Cisco 클라우드 보안 방안

- 시스코 네트워킹 클라우드

시스코 네트워킹 클라우드는 안전한 자동 연결, 운영 간소화, 플랫폼 접근 방식, 통합 관리 및 정책, 포괄적인 가시성 및 인사이트, 최상급 인프라, 간소화된 소비 모델을 기본 축으로 한다.

안전한 자동 연결이란 네트워크 애플리케이션에 대한 깊이 있는 가시성과 인사이트를 바탕으로 자동화를 접목하여 어떤 위치의 워크로드로도 연결 가능하다는 것이다.

운영 간소화는 모든 클라우드를 포괄하는 단일 사용자 인터페이스에서 상관관계에 대한 가시성 및 인사이트를 제공하면서 규모의 제약 없이 클라우드 에코 시스템 전 범위를 자동화하여 운영 관련 문제를 해결하는 것이다.

플랫폼 접근 방식은 운영자 중심의 단일 플랫폼에서 모든 클라우드를 포괄하여 라이프사이클 전체 워크플로우를 통합하는 것이다.

통합 관리 및 정책이란 인텐츠 인식형 단일 패브릭을 정책에 의해 정의하고 관리하면서 애플리케이션 요구사항을 해결하는 것이다.

포괄적인 가시성과 인사이트란 운영에 관한 결정 시 인프라부터 워크로드까지 포괄적으로 조명하면서 성능, 운영, 거버넌스에 대해 고려하는 것이다.

최상급 인프라란 클라우드 네트워킹의 핵심 측면이 소프트웨어 오버레이 내에 정의되며 인프라 기능도 고려해야 하고, 하드웨어 스케일과 같은 핵심 요소는 호환 가능한 기능, 코드, 운영 모델로 일관성 있는 아키텍처 빌딩 블록을 구현하는데 도움이 된다는 것이다.

간소화된 소비 모델이란, 간편하면서도 유연한 셀프서비스 기반 온 디맨드 페이 애즈 유 고(페이고)의 소비 모델을 통해 실시간 용량 관리 및 중단 없는 경험을 제공한다는 것이다.

차별화 요소로는 멀티 및 하이브리드 클라우드 운영 모델로의 전환을 도울 수 있으며, 중단 없는 클라우드 기능 제공, 멀티클라우드 네트워킹을 더욱 수월하게 구현하고 관리하며 클라우드 인프라까지 정책 확장이 가능하다는 점이 있다.

또한, SD-WAN과 구글의 네트워크 연결성을 활용하여 브랜치 사이트, 온프레미스 데이터 센터, 구글 클라우드를 구글의 고성능 글로벌 클라우드 네트워크를 기반으로 연결할 수 있다.

- 시스코 시큐어 클라이언트

시스코 시큐어 클라이언트는 애니 커넥트 VPN과 제로 트러스트 네트워크 엑세스(ZTNA)를 사용하며, 확장 가능한 엔드 포인트 보안 에이전트 관리가 가능하다. 또한, 보안 규제 준수와 사용자 친화적인 VPN 접속이 가능하며 여러 제어 지점의 엔드 포인트를 보호할 수 있다.

또한, 페어링 기능을 통해 업무 자동화, 탐지 및 대응 복구속도 단축, 통합형 위험 기반 취약점 관리, 고급 검색 기능으로 빠른 정보 확인, MITRE ATT&CK 프레임워크에 매핑되는 수동 위협 추적, VPN에 접속하지 않아도 보호할 수 있는 기능, 악성 도메인 연결 전에 악성 도메인과 IP에 대한 요청 차단 기능을 제공한다.

장점으로 첫 번째는 애니 커넥트의 모듈식 접근 방식을 향상시키고, 새로운 시스코 시큐어 클라이언트에 완전히 통합된 모듈로 도입 가능하다.

두 번째, 단일 클라이언트에서 여러 서비스를 제공하므로 총 소유 비용이 비교적 낮다.

세 번째, 포괄적이고 지속적으로 엔드포인트 보안을 제공한다.

네 번째, 유뮤선 및 VPN 전반에 걸쳐 기업 리소스에 대한 유연한 정책 기반 액세스 확장 기능을 제공한다.

다섯 번째, 일관된 사용자 경험을 제공한다.

여섯 번째, 지능적이고 신뢰 가능한 상시 연결성을 제공한다.

일곱 번째, 통합 에이전트를 통한 이용자 편의성을 확보할 수 있다.

마지막으로 제로 트러스트 네트워크 액세스로 쉽게 전환이 가능하다.

참고문헌

[1] Cloud Security Alliance 클라우드 컴퓨팅 위협: Pandemic 11 보고서는 기존 클라우드 보안 문제가 덜 우려스러워지고 있음을 발견, CSA: https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/

[2] 2022, 데이터 비용, IBM: https://www.ibm.com/kr-ko/reports/data-breach

[3] 시간 경과에 따른 CVSS 심각도 분포, NIST: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

[4] Skyrocket in Coming Years, statista : https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

[5] SEGA Europe 클라우드 보안 조사, vpnoverview : https://vpnoverview.com/news/sega-europe-security-report/

[6] Capital One 데이터 침해 사례 연구, MIT Sloan의 사이버 보안 : https://web.mit.edu/smadnick/www/wp/2020-16.pdf

[7] IMDSv2, AWS 사용 : https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html

[8] 3CX DesktopApp 공급망 공격, 국내에서도 확인, ASEC : https://asec.ahnlab.com/ko/50965/

[9] 러시아의 개요 우크라이나의 사이버 공격 활동, Microsoft: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[10] 북한의 ScarCruft, LNK 파일 감염 체인을 통해 RokRAT 맬웨어 배포, The Hacker News: https://thehackernews.com/2023/05/north-koreas-scarcruft-deploys-rokrat.html

[11] 사회 공학, imperva: https://www.imperva.com/learn/application-security/social-engineering-attack/

저자약력

이 용 준

2020032@kdu.ac.kr

1999년 2월 : 강남대학교 전자계산학과 (공학사)
2001년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
2005년 2월 : 숭실대학교 컴퓨터학과 (공학박사)
2010년 2월~2016년 3월 : KISA 사이버침해대응본부 수석연구위원
2010년 2월~2016년 3월 : 군사안보지원사 국방보안연구소 연구권
2016년 4월~현재 : 극동대학교 해킹보안학과 교수
관심분야
사이버보안, 융합보안, 산업보안

이 기 호

kdu-kh@kdu.ac.kr

2018년 2월 : 동국대학교 국어국문학과 (문학사)
2020년 10월~2024년 3월 : 극동대학교 개인정보보호 및 정보보호 담당 직원
2024년 2월 : 극동대학교 인공지능 보안학과 (공학석사)
관심분야
사이버보안, 융합보안, 산업보안