2021년 보안 현황

클라우드 복잡성, 원격 근무, 공급망 공격에 대한 보안 책임자들의 핵심 전략을 알아보는 글로벌 연구

splunk>

팬데믹 1 주년 시점의 사후 평가: 계속되는 보안 위기

2020 년은 COVID-19 와 갑작스러운 원격 근무 전환으로 시작해서 아찔한 보안 이슈로 마무리되었습니다. 이로 인해 수백여 조직이 황급히 검토-수정 모드로 돌입했습니다. 2020 년은 모든 보안 전문가들에게 가장 중요한 해로 간주될 것입니다. 신속한 예방책을 도모하고 있지만 많은 것이 많은 것이 팬데믹 이전과 이후로 극명히 달라질 것입니다.

팬데믹으로 인한 급속한 재택 근무 도입과 그에 따라 급격하게 진행된 클라우드 기술 확대는 보안 생태계에 대한 가시성 저하, 액세스 포인트 제어 미비, 공격 표면 다양화로 이어졌습니다.

그리고 SolarWinds 해킹 사건은 공급망 공격에 대한 깊은 공포와 모든 기업 입장에서 의존할 수 밖에 없는 벤더들에 대한 실존적 질문을 불러일으켰습니다. 바로 '협력 파트너를 신뢰해야 하는가?'의 문제입니다.

2021 년 보안 현황

하지만 2021 년 과제가 낯설지는 않습니다. 바로 일관성, 비용, 복잡성입니다. 스플렁크는 미드마켓과 엔터프라이즈 조직이 당면한 주요 보안 과제와 새로운 전략을 파악하기 위해 시장조사기관 ESG (Enterprise Strategy Group) 와 함께 9 개 지역, 다양한 산업 전반의 보안 책임자 535 명을 대상으로 글로벌 설문조사를 실시했습니다. 이 조사는 팬데믹 1주년이 다가오고 SolarWinds 해킹이 공개된 지 두 달만인 2021 년 2 월에 이루어졌습니다.。

78% 의 기업이 또 다른 SolarWinds 스타일의 공급망 공격을 예상합니다.

88% 의 조직이 보안 지출을 늘리고 있습니다. **35%** 가 '대폭 증가'라고 답변했습니다.

설문조사에 참여한 보안/IT 의사결정자들이 지목한 클라우드 네이티브 (cloud-native) 보안 환경의 최우선 보안 과제는 두 가지로 압축됩니다. 응답자의 50%가 '데이터센터와 클라우드 전반의 정책 및 실행 일관성 유지', 42% 가 '다수의 보안 제어 사용에 따른 비용과 복잡성'을 가장 중요한 보안 과제로 꼽았습니다. 전체 응답자들이 공통적으로 답한 두 번째로 중요한 보안 과제는 일시적 워크로드, 새로운 소프트웨어 개발 모델, 이기종 (heterogeneous) 퍼블릭 클라우드 사용으로 인한 클라우드 복잡성입니다.

클라우드 도입 확대가 보안 투자를 증가시키는 가장 큰 요인입니다

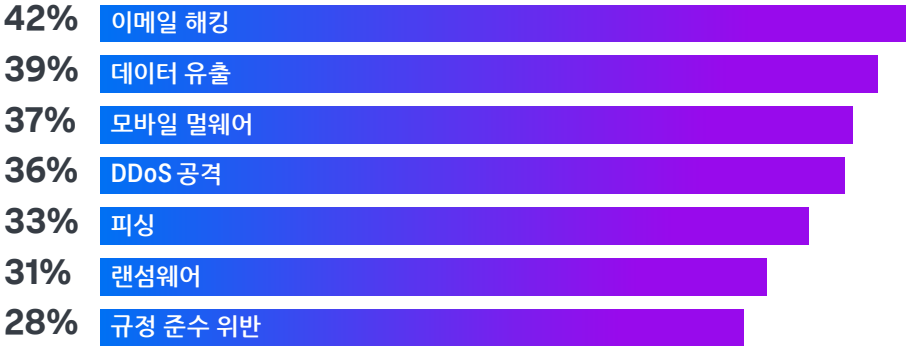
혼란스러운 상황

응답자들은 사이버 공격 증가가 팬데믹 시기인 2020 년 가장 심각한 문제였다고 답했습니다. 5개 중 4 개 조직 이상에서 업무용 이메일 해킹, 데이터 유출 등 최소한 한 번 이상 보안 사고가 발생한 것으로 나타났습니다.

이러한 사고는 후속조치에 막대한 시간과 자원이 소비되며 (응답자 42% 가 답한 피해), 생산성 저하 (36%) 와 비즈니스 시스템 장애 (35%) 로 이어졌습니다. 확실히 이러한 사고로 인해 많은 비용이 소모되고 혼란이 야기되며 파괴적인 피해가 발생합니다.

84% 의 조직이 지난 2 년 간 심각한 보안 사고 경험

응답자들이 겪은 주요 사이버 보안 사고



보안 사고로 인한 손실

응답자들이 겪은 보안 사고의 주요 영향:

보안 팀은 갑작스런 원격 근무 전환과 새롭게 확장된 경계 보호에 따른 어려움 뿐만 아니라 산업 전반을 강타한 SolarWinds 해킹과도 싸워야 했습니다. 2020 년 12 월 확인된 SolarWinds 해킹 공격으로 인해 광범위한 장애가 발생했으며, 많은 조직이 향후 공급망 공격을 막기 위한 노력을 강화했습니다. 설문 조사 응답자들은 이를 위해 보안 제어 감사 강화 (35%), 소프트웨어 업데이트 스캔 주기 단축 (30%), 침투 테스트 증대 (27%), MFA 인증 강화 (26%) 예정이라고 답했습니다. 이러한 조치는 보안을 향상시킬 수 있으나 리소스 부족 또한 심화시킵니다.

78% 의 조직이 사이버보안 팀의 역량이나 확장성과 관련하여 하나 이상의 어려움을 겪고 있다고 답했습니다. 선제적 개선이 아닌 장애 제거 활동에 매달리게 만드는 엄청난 양의 보안 경고, 수동 프로세스로 인한 문제 등이 여기에 포함됩니다. 또한 78% 가 SolarWinds 해킹과 같은 공격으로 인한 피해가 우려된다고 답했습니다. SolarWinds 공격이 끝난 것도 아니고 앞으로 다른 공급망 공격이 발생할 수 있음을 감안하면 이런 질문이 떠오릅니다.나머지 22% 는 무슨 생각을 하고 있을까요?

다음 과제는 클라우드 복잡성입니다.

이그제큐티브 하이라이트

딱 한 가지 요점만 원한다면 바로 이것입니다.
보안은 데이터 문제입니다.

데이터는 조직이 보호하는 자산입니다. 데이터는 공격자 침입 (또는 이미 내부에 있음) 사실을 알려줍니다. 데이터는 데이터가 상주하는 가상 클라우드 인프라를 정의합니다.

2021 년 과제: 클라우드 복잡성과 원격 근무 폭증

클라우드 서비스 프로바이더가 하나 뿐이라도 하이브리드 가시성은 충분히 어렵습니다. 상황은 조만간 더욱 어려워질 것입니다.

- 오늘날 클라우드 인프라 사용자 **75%** 가 멀티클라우드 환경 사용.
- **87%** 가 2년 내에 다수의 클라우드 서비스 프로바이더를 사용하게 될 것.
- **76%** 의 응답자가 원격 근무자들에 대한 보안이 더 어렵다고 답변.
- **53%** 가 팬데믹 기간 동안 공격이 증가했다고 답변.
  — **12%** 가 공격이 '크게 증가'했다고 답변.

SolarWinds 공격: 공급망 보호가 충분히 이루어지고 있을까요?

- 보안 책임자 **78%** 가 앞으로 SolarWinds 와 유사한 스타일의 공격이 증가할 것으로 우려된다고 답했습니다.
- SolarWinds 해킹 공격이 밝혀진 지 2 개월이 지난 시점에서 CISO (Chief Information Security Officer) 중 단 **47%** 만이 경영진이나 이사회에 관련 사항을 브리핑했다고 답했습니다.
- 단 **23%** 만이 네트워크 세그멘테이션을 통해 시스템과 데이터에 대한 액세스 제한을 강화했다고 답했습니다.
- 보안 팀이 과중한 업무에 시달리고 있는 것은 사실입니다. 그럼에도 불구하고 SolarWinds 상황에 대한 조용한 반응이 우려스럽습니다.

솔루션에 투자하고 있는 조직

- 거의 모든 응답자 — **88%** — 가 보안 지출이 증가할 것이라고 답했습니다.
- **35%** 가 대폭 증가할 것이라고 말했습니다.
- 기존 보안 프로세스와 기술로는 변화하는 상황에 적절히 대응할 수 없으며, 따라서 조직은 지출과 투자를 늘릴수 밖에 없습니다.
- 응답자들의 답한 보안 투자 우선 순위는 25 페이지 에서 확인하십시오.

핵심 권고사항 (P. 25 참조)

- **SOC (Security Operations Center) 현대화:**
  - 자동화 및 분석 확대
  - 제로 트러스트 모델 도입
  - 교육 및 인력 강화
- **팬데믹 종식을 위한 노력 지속:** 보안, IT, 비즈니스 담당자들 간의 긴밀하고 신속한 협업을 이어나갈 것.

데이터 시대의 과제

보안 조직은 급증하는 데이터, 확장되는 경계, 갈수록 정교해지고 증가하는 공격을 따라 잡아야하는 부담을 안고 있습니다. 이번 설문조사 결과는 상황이 계속 악화되고 있음을 확인시켜 줍니다.

COVID 로 인해 원래 있었던 문제들이 한층 심화되었습니다. 수작업 프로세스는 느리고 번거롭고 광범위합니다. 숙련된 보안 전문 인력의 부족 또한 심각한 추세입니다. 그리고 10년 전부터 계속된 트렌드인 클라우드 마이그레이션은 끊임없이 증가하는 복잡성과 속도로 인해 더욱 어려워졌습니다.

이번 조사에서 온프레미스 인프라가 클라우드 기반 인프라보다 더 자주 피해를 입지만 취약하기는 둘 다 마찬가지임이 확인되었습니다. 차이는 미비합니다. 가장 흔한 공격인 비즈니스 이메일 해킹이 온프레미스 애플리케이션 및 인프라에 영향을 미치는 시간이 44% 인데 비해 클라우드 리소스의 경우는 36%였습니다. 피싱, 모바일 멀웨어, 내부자 공격의 경우는 기껏해야 몇 퍼센트 차이입니다. 중요한 사실은 공격이 하이브리드 인프라 전반에 걸쳐 벌어지고 있다는 것입니다. 온프레미스 진입점으로 침투한 공격자가 내부 확산을 통해 클라우드 기반 애플리케이션과 데이터로 이동하거나 반대로 클라우드에 침투하여 온프레미스로 이동할 수도 있습니다. 따라서 조직은 시작 지점과 종료 지점에 관계없이 공격을 방어할 수 있도록 준비해야 합니다.

이처럼 온프레미스 리소스에서 클라우드로 공격이 급속히 확산되기 때문에 환경 전반에 대한 가시성 확보가 필요합니다. 보안 팀은 흩어진 점들을 연결할 수 있어야 합니다. 그러나 클라우드는 속도와 유연성 극대화가 관건인만큼 개발자들은 SOC 에서 제어할 수 있는 정도로 속도를 늦추고 싶어하지 않습니다.

두 명 이상의 CISO 가 특정 사례를 들어 이 점을 강조했습니다. 그들은 개발자들이 Amazon Web Services 의 Reinvent 컨퍼런스에 다녀오면 Amazon 이 발표한 클라우드 서비스 최신 기능을 당장 구현하려고 안달한다고 한탄했습니다. 하지만 보안 조직은 이런 기능이 존재하는지조차 알지 못하며, 해당 기능에 대한 적절한 제어가 미비한 경우가 대부분입니다.

재택근무 전환만을 위한 클라우드 기반 기술의 새로운 보안 요구사항은 매우 어렵습니다. 특히 조직이 위기 상황에서 빠르게 움직이고 있는 경우에는 더욱 그렇습니다.

스플렁크 CISO 인 Yassir Abousselham 은 이들의 어려움을 공감합니다. "원격 근무 셋업을 급속히 진행하는 과정에서 재택근무자들이 화상회의나 인스턴트 메시징 통신과 같은 기본 업무를 수행할 수 있도록 하기 위해 클라우드 전환이 급격히 이루어졌습니다." 그는 이렇게 말합니다. "이 때문에 많은 조직에서 보안 관행이 무너졌습니다."

Abousselham은 "클라우드 기반 애플리케이션의 도입은 싱글 사인온(single sign-on) 및 다단계 인증(MFA)을 통해 가장 안전하게 보호됩니다. 암호만으로는 계정 보안을 효과적으로 확장할 수 없기 때문입니다"라고 말합니다. " 싱글 사인온을 통해 사용자 별 단일 계정을 사용함으로써 권한 부여를 보다 세밀하게 제어하고 인증을 강화하고 일관된 모니터링을 실행할 수 있습니다."

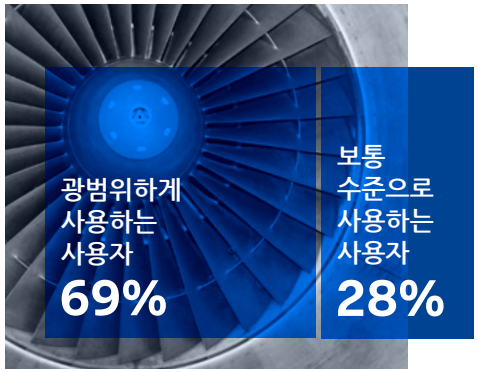
클라우드 복잡성으로 인해 요구되는 일관성

퍼블릭 클라우드 사용이 보편화됨에 따라 보안 팀은 데이터에 대한 일관된 제어와 복잡성에 대한 가시성을 확보해야 합니다. 궁극적으로 조직은 모든 아키텍처와 클라우드 서비스 프로바이더를 막론하고 어디서든 클라우드 친화적인 제어가 가능해야 합니다.

유비쿼터스 퍼블릭 클라우드

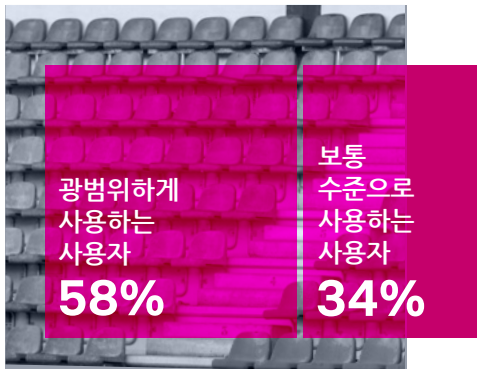
퍼블릭 클라우드 컴퓨팅을 '보통~ 광범위하게 사용'한다고 답한 조직의 비율

SaaS
Software as a Service



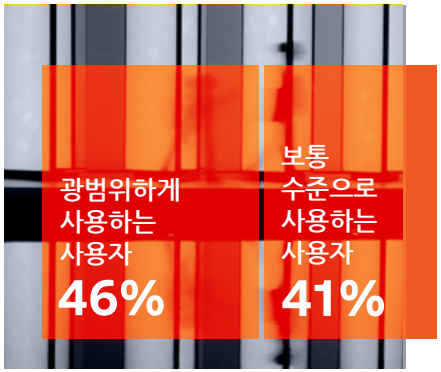
97% 총 사용자

IaaS
Infrastructure as a Service



92% 총 사용자

PaaS
Platform as a Service



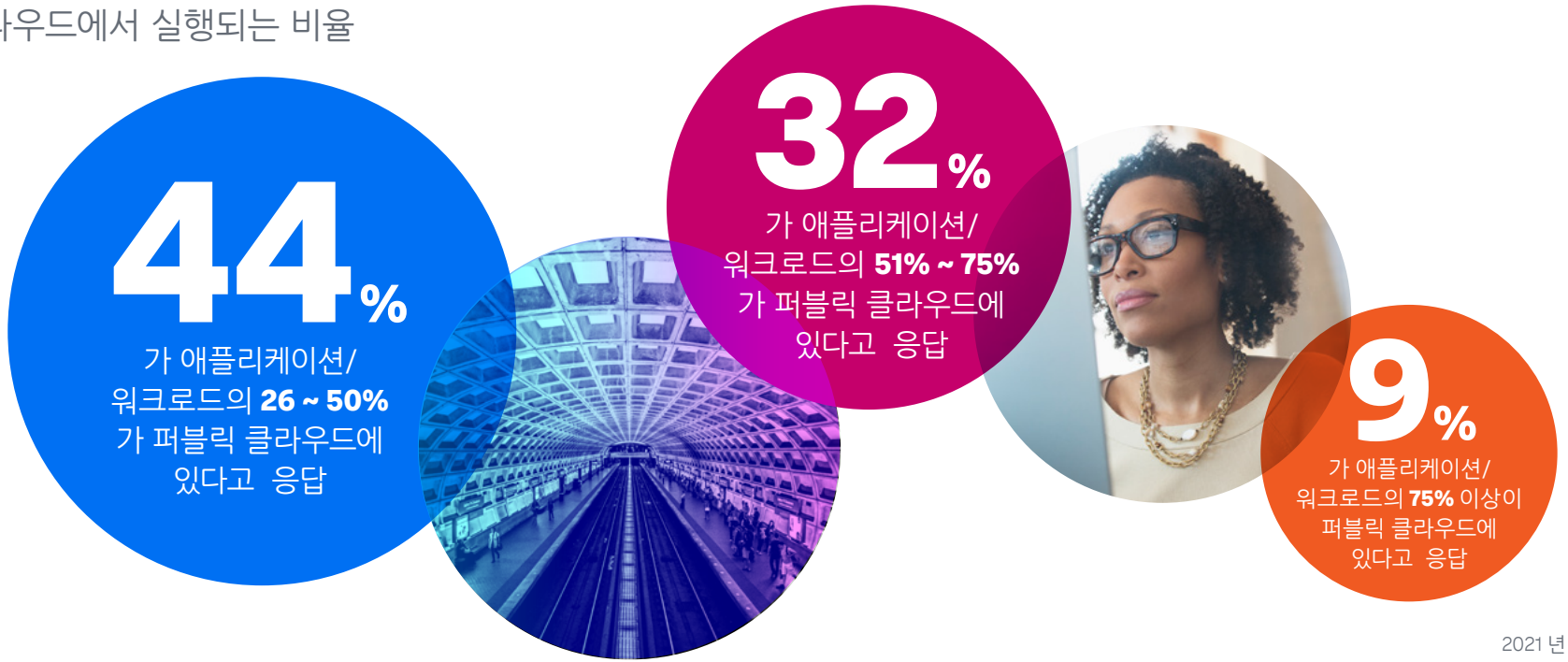
87% 총 사용자

10 개 중 거의 9개 조직이 비즈니스 크리티컬 애플리케이션의 상당 부분을 이미 퍼블릭 클라우드에서 실행하고 있습니다. 응답자의 15% 만이 클라우드에서 25% 이하를 실행한다고 답했으며, 41% 가 클라우드에서 절반 이상을 실행한다고 답했습니다. 미래의 클라우드 퍼스트 (cloud-first) 환경에 대한 조사 결과는 다음과 같습니다.

- **43%** 의 조직이 신규 애플리케이션에 대한 클라우드 퍼스트 정책을 갖고 있습니다. 단 **14%** 만이 클라우드를 예외로만 간주하는 온프레미스 정책을 갖고 있습니다.
- 클라우드 인프라 사용자의 **75%** 가 멀티클라우드이며, **87%** 가 향후 2년 내 복수의 클라우드 서비스 프로바이더를 사용할 것이라고 답했습니다.。
- 3 개 이상의 프로바이더를 사용하는 조직의 비율이 앞으로 2년 간 **29%** 에서 **53%** 로 증가할 것으로 예상됩니다.
- 응답자들은 현재 전체 워크로드의 **29%** 가 클라우드 네이티브라고 답했습니다. 그리고 2년 뒤에는 **55%** 로 거의 두 배 늘어날 것으로 예상합니다.

퍼블릭 클라우드는 필수

조직의 주요 비즈니스 애플리케이션과 워크로드가 퍼블릭 클라우드에서 실행되는 비율



클라우드 도입 관련 추세는 기존 보안 문제를 악화시킬 것입니다. 설문 조사 그룹 가운데 가장 많이 확인된 두 가지 과제는 데이터센터와 퍼블릭 클라우드 환경에서 보안 일관성을 유지하는 것 (50%), 그리고 다수의 사이버보안 제어를 사용하는 데 따른 비용과 복잡성 (42%) 이었습니다. 또 다른 문제로는 퍼블릭 클라우드 인프라에 대한 가시성 부족 (23%), 속도를 걱정하는 개발 팀과 DevOps 팀에서 보안이 제외되는 문제 (24%), 클라우드 네이티브 환경을 지원하지 않는 기존 보안 도구 (22%) 등이 있습니다.

클라우드 네이티브 애플리케이션에 대한 보안 가시성을 향상시키기 위해 조직이 최우선으로 꼽은 기본 기능은 " 규제에 위배되는 워크로드 구성 파악"(42%), "멀웨어 탐지"(33%), "소프트웨어 취약성 식별"(33%) 입니다. 그 밖의 기능으로는 서비스 계정 관련 권한 감사 (16%), 비정상 활동 모니터링 (15%), 내부 서버 및 컨테이너 워크로드 커뮤니케이션 감시 (15%) 와 같은 고급 모니터링이 있습니다.

클라우드 네이티브 아키텍처로 인한 보안 문제

응답자들이 말한 주요 과제

50%

데이터센터 및 퍼블릭 클라우드 환경에서 보안 일관성을 유지하는 데 어려움을 겪고 있음

42%

다수의 사이버 보안 제어를 사용함으로 인해 관련 비용과 복잡성이 증가

29%

퍼블릭 클라우드 인프라에 대한 가시성 부족

갈수록 더욱 힘들어지는 보안

쉽고 부담없는 일을 찾아서 IT 보안 분야에 뛰어드는 사람은 없습니다. 하지만 응답자들은 클라우드의 복잡성과 팬데믹으로 인한 혼란이 업무를 더욱 어렵게 만든다는 데 의견을 같이합니다. 클라우드는 유연성과 속도를 위해 보안 팀이 가시성과 보안 조치를 축소하도록 만듭니다. 이는 2020 년 팬데믹으로 인한 클라우드 대이동으로 더욱 심화되었습고, 보안 검토 주기가 단축되었습니다. 응답자의 49% 가 2 년 전에 비해 보안이 더 어려워졌다고 말합니다. 주요 보안 과제는 다음과 같습니다.

- 갈수록 교묘해지는 위협 환경 대응 **(48%).**
- 워크로드를 클라우드로 이전하면서 더욱 어려워진 공격 표면 (attack surface) 모니터링 **(32%).**
- 전문 인력 확보 **(28%).**

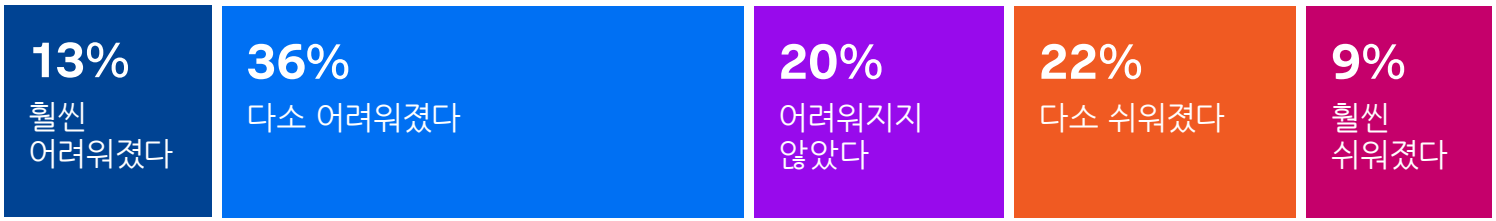
클라우드 관련 주요 이슈는 다음과 같습니다.

- 규제 위반 워크로드 파악 **(42%).**
- 멀웨어 탐지 **(33%).**
- 소프트웨어 취약성 파악 **(33%).**

너무 많은 경고는 무분별한 도구 증가로 인한 결과입니다. 보안 데이터에 대한 종합적인 뷰와 자동 이벤트 분류를 통해 사람이 개입해야 하는 경고의 수를 줄일 필요가 있습니다.

조사 결과는 보안 팀의 성공을 위해서는 어떤 것들이 필요한지 알려줍니다. 이 새로운 시대를 가장 잘 관리할 수 있는 보안 팀은 적응력이 뛰어나고 빠르게 배울 수 있어야 합니다. 자동화를 효과적으로 활용하여 기존 위협에 신속하게 대응하고, 사람이 긴급한 최신 위협에 주목할 수 있는 시간을 확보해야 합니다. 멀티 클라우드 환경을 이해하고 이를 운영하는 개발 및 운영 조직과 원활하게 협력할 수 있어야 합니다.

가중되는 보안 팀의 부담



응답자의 **49%** 가 지난 2 년 동안 보안 요구를 준수하기가 더 어려워졌다고 답변

단 **31%** 만이 쉬워졌다고 답변

SOC 에 부담을 가중시키는 원격 근무

2020 년 3 월, 많은 조직이 짧은 시간에 적절한 준비없이 사무실 운영 대부분을 재택 근무로 전환해야 했습니다. 이러한 갑작스런 혼란의 와중에 IT 팀과 보안 팀의 영웅적인 노력이 있었습니다. 더 중요한 것은 그들이 영웅적인 노력을 함께 해야 했다는 것입니다.

COVID-19 팬데믹으로 인해 보안 팀은 그 어느 때보다 비즈니스 및 IT 리더들과 긴밀하게 협업해야 했습니다. 보안이 조직의 생존에 필수요소가 되었기 때문입니다. 또한 COVID-19 팬데믹은 경영진에게 IT 보안의 가치를 강조하여 현재 대부분의 조직에서 보안 지출을 늘리려는 계획을 설명하는 데 도움이되었습니다.

팬데믹 시대의 가장 가시적인 과제는 원격 근무 전환이었습니다. 이 보고서 발표 시점에도 여전히 많은 조직이 일정 수준의 원격 근무를 계속하고 있습니다. 여러 조사에서 대부분의 조직이 전염병 이전보다 더 자유로운 원격 근무 정책을 계속할 계획임이 밝혀졌습니다. 많은 근로자들이 재택 근무 확대를 희망하기 때문입니다.

응답자들은 자사의 원격 근무 인력이 현재 COVID-19 이전보다 두 배 이상 증가 했다고 말합니다. 팬데믹 이전 원격 근무 인력의 비율이 평균 23% 였던 데 비해 2021 년 초에는 56% 까지 치솟았습니다. 출퇴근에 지친 근로자들에게는 원격 근무가 반가울 수 있으나 SOC 의 사정은 다릅니다. 원격 근무자들은 공격자에게 절호의 타겟입니다. 이 새로운 원격 근무 환경에 맞지 않는 오래된 네트워크 보안 전략과 많은 직원들이 업무 시스템 액세스에 개인 기기를 사용하는 경향 때문입니다. 개인 기기는 일반적으로 보안 수준이 낮으며 기기 공유를 통해 데이터 유출로 이어질 수 있습니다.

실제로 대부분의 응답자가 공격이 증가했다고 보고합니다.

- 응답자의 **76%** 가 원격 근무자들에 대한 보안이 더 어렵다고 말합니다.
- **53%** 가 팬데믹 기간 중 공격이 증가했다고 말합니다. **12%** 는 공격이 대폭 증가했다고 답했습니다. 。

원격 근무자 보안 과제

31%
원격 근무자 기기에서 엔드포인트 보안 소프트웨어 실행 확인

29%
원격 근무자 기기의 보안 구성 확인

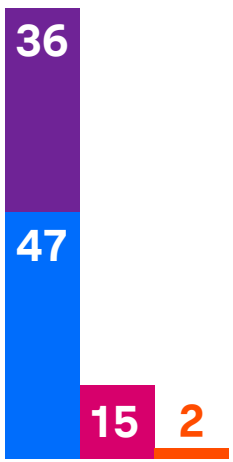
29%
클라우드 기반 앱/ 리소스에 대한 보안 액세스 제공

27%
회사 네트워크에 대한 보안 액세스 제공

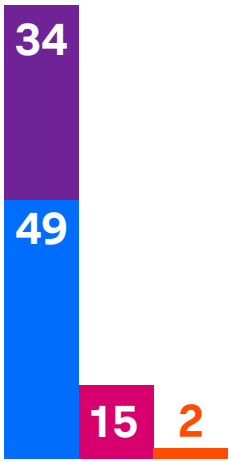
원격 근무자 보호는 어렵습니다. 보안 팀은 프로세스 자동화와 클라우드 기반 제어를 도입하고 탐지 규칙을 지속적으로 조정할 수 있는 방법을 모색하고 있습니다. 지금까지 보안 팀의 업무는 기본적인 위생 (basic hygiene), 액세스, 보안 제어 관리가 중심이었습니다. 응답자의 20% 만이 원격 근무자 트래픽 및 사용자 행동 모니터링이 2020 년 주요 과제였다고 답했습니다. 이는 이러한 기능이 궁극적으로 얼마나 안전한지에 대한 확인보다는 원격 기능을 안정적으로 가동하는 데 더 많은 노력이 투입되었음을 시사합니다.

원격 근무 대전환 초기에는 적극적인 보안/IT/비즈니스 협업으로 긍정적인 정책 변경과 프로세스 자동화 및 보안 분석 사용에 대한 관심 강화가 이루어졌습니다. 이러한 광범위한 협업은 조직 전반에서 데이터를 활용하고 공유하는 데 따른 가치를 향상시킵니다. 이는 분석 이니셔티브의 이점이기도 합니다. 그 결과가 실제로 확인되고 있습니다. 앞서가는 조직은 보안 데이터와 비보안 데이터를 결합시켜 비즈니스에 영향을 미칠 수 있는 사이버 위험을 더욱 효과적으로 식별합니다. 그런 다음 이러한 위험을 특정 비즈니스 프로세스와 관련하여 추적할 수 있습니다.

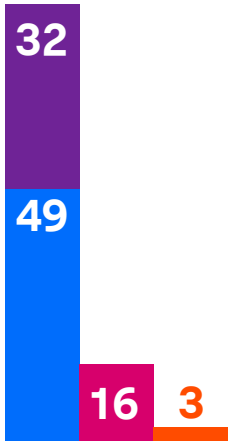
원격 근무로 인한 보안 영향



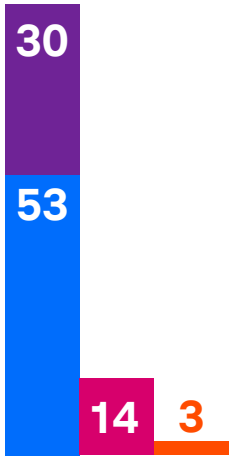
원격 근무 전환으로 IT/보안 운영 팀 간의 협업이 강화되었음



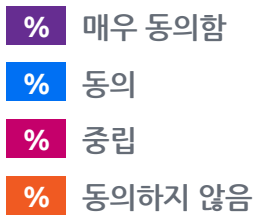
원격 근무 증가로 보안 프로세스 자동화가 향상되었음



원격 근무 트렌드로 인해 클라우드 기반 보안 기술이 증가했음



SOC 는 원격 근무 관련 리스크 해결을 위한 규칙을 계속해서 구현하고 있음



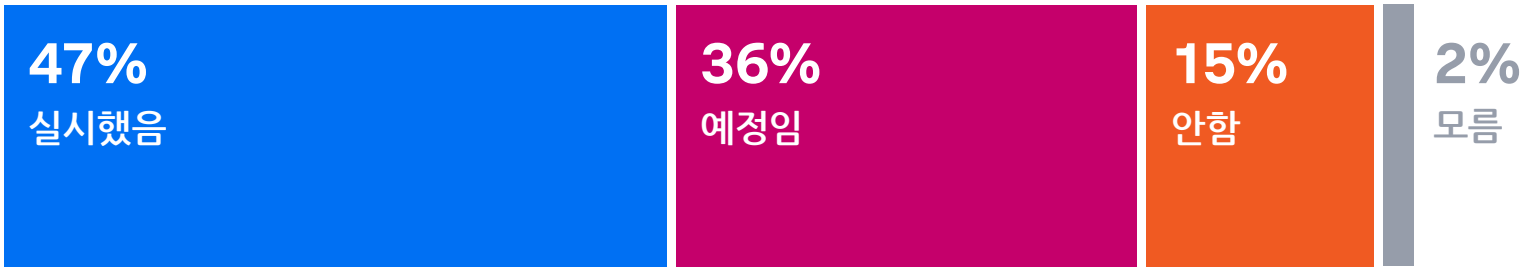
SolarWinds 공격에 대한 대응

2020 년 12 월 SolarWinds 소프트웨어 업데이트를 악용한 해킹이 전 세계적으로 최대 18,000 개 조직에 영향을 미친 사실이 드러났습니다. 이로 인해 수만 개의 조직이 관련 피해 여부를 확인해야 했습니다. 그로부터 2 개월이 지난 설문조사 시점에서 우리는 응답자들에게 이 문제에 어떻게 대응했는지 물어보았습니다. SolarWinds 해킹 사건은 모든 조직이 공급망 공격 가능성을 차단하는 방법을 재검토하도록 만들었습니다.

가장 놀라운 사실은 보안 팀이 높은 수준의 우려를 표명했음에도 불구하고 2 개월 후 CISO 중 절반도 SolarWinds 해킹과 조직의 상황에 대해 고위 경영진이나 이사회에 브리핑하지 않았다는 것입니다. 따라서 이렇게 질문할 수 밖에 없습니다. 그들은 무엇을 기다리고 있는 것일까요?

SolarWinds 해킹에 대한 이사회 논의 지연

CISO 가 임원진/이사회에 관련 브리핑을 실시한 조직의 비율 (2021 년 2 월 기준)



응답자들은 SolarWinds 공격 이후 다양한 대응을 수행했다고 답했습니다. 가장 많은 답변은 보안 제어 평가 (35%), 보안 예산 증액 (31%), 소프트웨어 업데이트 스캔 강화 (30%) 입니다. 그러나 전체 응답 조직의 약 3 분의 1 만이 이러한 조치를 각각 취했다고 답한 것을 감안할 때 보안 책임자가 이러한 심각한 위협과 향후 유사한 공격에 충분히 대응하고 있는지 확실하지 않습니다.

물론, SolarWinds 해킹 사건에 대한 구체적인 대응은 기존 보안 관행 하에서 이루어졌습니다. 예를 들어, 10 개 중 9 개 조직이 구매 고려 시 공급업체의 보안을 반복적으로 면밀하게 조사한다고 답했습니다. 또한 응답자 95% 이상이 매년 공급업체의 보안에 대한 다양한 평가를 수행한다고 보고했으며, 높은 비율로 최소 분기별 평가를 수행한다고 답했습니다.

그러나 이러한 조치들은 SolarWinds 가 거의 일 년 동안 탐지되지 않은 사실이 밝혀지기 전에 시행된 관행입니다. 문제는 추가적인 조치가 강력하게 도입되지 못했다는 점입니다.

조직마다 다른 SolarWinds 이후 보안 조치

SolarWinds 해킹 후 구체적인 조치를 취한 조직의 비율

35% 기존 보안 제어 검토

31% 사이버 보안 예산 증액

30% 소프트웨어 업데이트 스캔 작업 강화

29% 새로운 탐지 규칙 추가

27% 침투 테스트 또는 레드팀 훈련 실행

27% 공급망 보안 정책 확대 도입

26% 강력한 인증 기술 도입

26% 써드파티 위험 평가 실시

26% 사고 대응 활동 수행

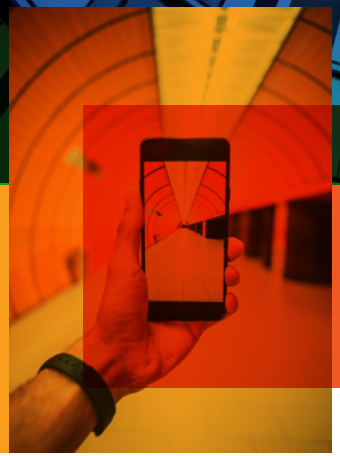
24% CISO/임원/이사회 간 회의 확대

23% 조직 네트워크 세분화

23% 벤더 위험 관리 정책 재검토

17% 인프라 소프트웨어를 차선의 보안 정책으로 교체

향후 전망



작년에는 팬데믹 위기에 따른 시급한 보안 문제에 주의를 기울여야 했습니다. 우리는 2021년 초 보안 및 IT 책임자들을 대상으로 설문 조사를 진행하면서 향후 보안 태세 개선에 대한 계획을 살펴 보았습니다.

믿기 힘든 한 해를 보낸 설문 조사 응답자들에게 향후 2 년 동안의 최우선 보안 과제를 물었습니다. 가장 많이 나온 답변은 다음과 같습니다.

- 보안 및 IT 운영 직원을 위한 보안 교육 강화 (**25%**)
- 클라우드 기반 보안 분석/운영 기술 검토 또는 구축 (**22%**)
- 보안 프로세스 자동화 및 오케스트레이션을 지원하는 도구에 투자 (**22%**)
- 보안 운영 프로세스 테스트 주기 단축 (**21%**)
- 보안 분석/운영 기술을 클라우드로 이전 (**19%**)
- 보안 분석/운영 도구를 위한 통합 소프트웨어 아키텍처 개발 가속화 (**18%**)
- 더 많은 보안 운영 인력 고용 (**18%**)

이러한 과제들을 최우선 순위로 삼는 것은 바람직합니다. "보안 분석가가 중점을 두고 있는두가지 중요 기술은" 바로 속도와 인사이트입니다. 목표는 클라우드 애플리케이션과 인프라에 대한 향상된 가시성을 확보하고 프로세스를 자동화하는 것입니다. 그리고 그 안에 있는 데이터와 인사이트에 대한 더욱 종합적이고 향상된 뷰를 제공하는 분석 도구로 이러한 모든 작업을 수행해야 합니다.

우리는 2019 년에도 매우 유사한 목록을 예상했습니다. 보안 책임자가 2021 년 현실에 맞게 전략을 조정하려면 새로운 기술에 제로 트러스트 전략이 포함되어야 합니다. 왜냐하면 전통적인 네트워크 중심의 '경계 보안' 개념으로는 더 이상 안되기 때문입니다. 팬데믹으로 인한 원격 근무 인력을 지원하기 위해 서둘러 구축된 새로운 클라우드 기술에 특히 주의를 기울여야 합니다. 그리고 보안 프로세스 테스트는 클라우드에 더 많은 데이터가 저장되고 보안 직원을 비롯한 더 많은 인력이 원격으로 근무하는 새로운 상황을 고려해야 합니다. 자세한 내용은 권고사항을 참조하십시오.

핵심 기술: 보안 분석

데이터의 두 가지 귀중한 용도는 서로 다르며 때로는 병합됩니다. Data-driven 과 Data-informed 사이에는 차이가 있습니다. 전자는 데이터를 기반으로 액션이 수행되는 것을 의미하며 자동화에 적합합니다. 피싱의 경우를 생각해 보십시오. 악성 이메일이 식별되면 보안 분석가에게 에스컬레이션할 필요 없이 수정 조치가 취해집니다. 반면 Data-informed 는 인간이 데이터를 기반으로 인사이트를 얻은 후 결정을 내리는 것을 의미합니다. 최근의 비정상적인 행동 패턴에 대응하여 전체 보안 전략을 재조정하는 경우가 여기에 해당합니다.

데이터 분석은 이 둘을 연결하여 자동화된 대응을 촉진하고 분석가와 보안 책임자에게 전략적 통찰을 제공합니다. 이번 조사를 통해 우리는 분석이 위험을 파악하고 의사 결정을 지원하기 위한 보안 체계의 창끝과 같다는 사실을 확인했습니다. 특히 분석은 위협 탐지 및 대응부터 보안 제어, 투자, 예산 책정, 자동화에 대한 결정에 이르기까지 다양한 주제에 대한 의사 결정을 지원하는 정보를 제공합니다.

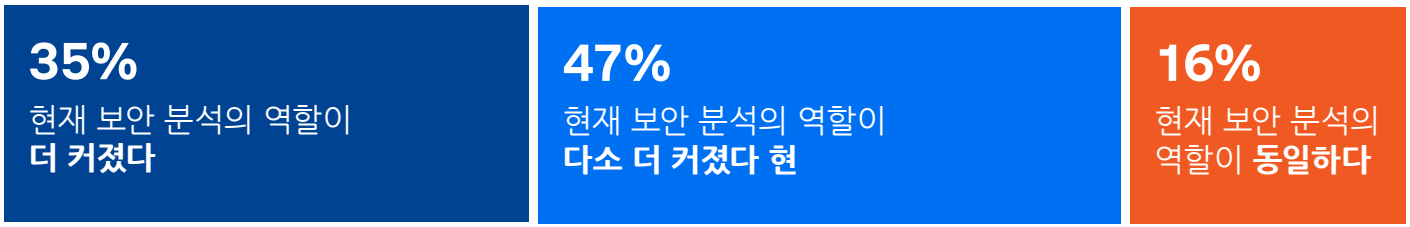
우리는 이번 조사에서 분석, 자동화 등을 지원하는 보안 분석 (security analytics) 과 머신러닝 (machine learning) 이라는 두 가지 데이터 관련 기술에 대한 관심뿐만 아니라 도입 또한 증가하고 있음을 발견했습니다.

보안 분석에는 엔터프라이즈 환경의 잠재적 위협을 탐지하는 알고리즘과 분석 프로세스가 조합되어 있습니다. 멀웨어와 기타 공격이 갈수록 빨라지고 교묘해져서 보안 분석가가 분석 도구 없이는 따라 잡기 어렵기 때문에 최근 몇 년 동안 보안 분석에 대한 수요가 증가했습니다. 조사 결과에 따르면 82% 의 조직이 보안 분석 도구가 2 년 전에 비해 오늘날 전반적인 보안 의사 결정에서 더 큰 역할을 한다고 말합니다. 이는 분석이 선택, 구성 등의 기반이 되는 하향식 보안 접근 방식이 이루어지고 있음을 나타냅니다.

응답자들에게 최신 보안 과제 해결을 위한 분석 도구의 중요성이 갈수록 커지는 이유를 물었습니다. 가장 많이 나온 답변은 다음과 같습니다.

- 규제 준수 지원 **(37%)**
- 비보안 데이터 통합 작업 증가 **(36%)**
- 의사 결정을 지원하는 최신 AI/ML 기반 도구 사용 **(36%)**
- 분석해야 할 데이터가 예전에 비해 훨씬 증가 **(36%)**
- 증가하는 위협에 대응하여 더욱 많은 분석 적용 **(34%)**

사이버 보안을 지원하는 보안 분석



응답자의 **82%** 가 보안 분석이 2년 전과 비교하여 오늘날 보안 전략에 점점 더 많은 영향을 미친다고 답했습니다.

그 밖에 답변으로 자동화 및 실시간 데이터 사용 증가에 따른 분석 기술 도입 (27%), 최근의 데이터 유출 사고로 인한 향후 분석 도구의 중요성 증가 (24%) 등이 있었습니다.

실제로 73% 의 조직이 다른 데이터 소스들을 활용하여 보안 분석을 강화하고 있습니다. 다양한 데이터와 솔루션 병합의 중요성은 보안 책임자들이 수년 전부터 알고 있던 사실입니다. 바로 모든 데이터가 보안 데이터라는 것입니다.

"스플렁크 CISO Yassir Abousselham 은 "분석 도구와 데이터 인사이트를 적극적으로 활용하는 것은 보안 분석가의 역량을 강화하는 데 도움이 된다" 면서 "단순한 피싱 이메일과 같은 일상적인 공격에 대한 대응을 자동화하여 분석가에게 주의가 필요한 다른 모든 케이스를 분류할 수 있는 기회를 제공해야 한다"고 말했습니다."

보안 분석의 영향을 가장 많이 받는 분야

45%
위협 탐지/대응

41%
위험 식별

39%
보안 제어

36%
더 많은 분석이 필요한 영역 결정

25%
투자

23%
프로세스 자동화

23%
예산 수립

22%
아웃소싱/서비스

15%
인사

핵심 기술: 머신러닝

데이터 유출은 빠르고 광범위하게 진행됩니다. 따라서 해커를 잡았을 때는 이미 늦은 경우가 많습니다. 이것이 머신러닝이 중요한 이유입니다. 인간이 할 수 있는 작업에는 한계가 있지만 컴퓨터는 막대한 양의 데이터를 효율적으로 처리합니다. 강력한 분석 요구를 지원하기 위해 조직은 머신러닝 (ML) 기술을 대거 사용하고 있으며 보안 데이터 이상의 것들을 결합하고 통합하여 의사 결정을 지원하고 가속화하는 방법을 모색하고 있습니다.

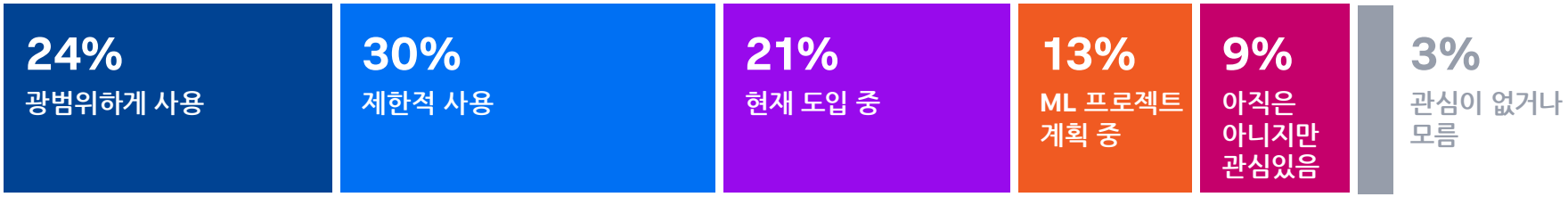
보안 침해는 몇 시간, 또는 몇 달까지 탐지되지 않을 수 있습니다. 보안 분석에서 ML 을 사용하면 분석가가 탐지 대응 (discovery and response) 시간을 가속화하고 기존 보안 데이터뿐만 아니라 조직 전체(자산, 네트워크 성능, 애플리케이션 등)의 데이터를 활용하는 데 도움이 됩니다.

이번 조사에서 확인된 결과는 다음과 같습니다.

- 보안 팀의 **54%** 가 현재 보안 분석에 머신러닝 사용.
- 전체 조직의 **43%** 가 보안 운영에 머신러닝을 추가할 계획이거나 관심을 가지고 있음.
- 주요 머신러닝 사용 사례:
  - 사이버 리스크 파악 **(39%).**
  - 위협 탐지 강화 **(37%).**
  - 주니어 레벨 분석가가 더 많은 사건을 처리할 수 있도록 지원 **(29%).**

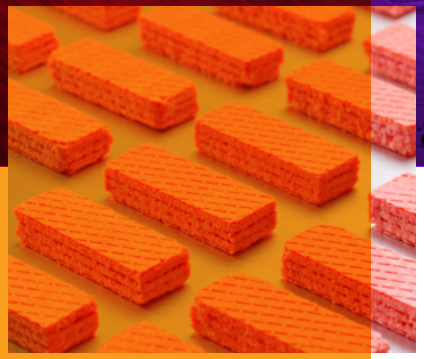
사실 우리는 머신러닝 사용이 훨씬 더 높을 것으로 예상했습니다. 실제로 그럴 수 있습니다. 그것은 많은 조직이 머신러닝 기반 제품을 사용한다는 사실을 깨닫지 못한 채 머신러닝 기반 제품을 사용하고 있기 때문입니다.

보안을 위해 머신러닝을 도입하는 조직 증가



응답자의 **88%** 가 보안을 위해 ML 을 도입 중이거나 도입 계획을 갖고 있음

보안은 결국 데이터 문제



보안 팀은 데이터 시대 (Data Age)
의 영향을 체감하고 있습니다.
급속한 클라우드 전환과 빠른 디지털
트랜스포메이션 (Digital Transformation)
의 진행이 바로 그것입니다.

이러한 변화는 COVID-19 로 인해 더욱 가속화되었으며, SolarWinds 공격이 급증하는 복잡성으로 인한 위험을 부각시켰습니다. 2020 년의 교훈은 보안 방식, 또는 보안이 어떻게 이루어져야 하는지를 근본적으로 변화시키고 있습니다.

COVID 이후 데이터 시대의 과제가 클라우드 서비스, 하이브리드 아키텍처, 공급망의 복잡성이라면 기회는 모든 데이터에 있습니다. 보안 팀은 효과적인 분석 도구를 사용하여 그 어느 때보다 많은 데이터를 연결함으로써 비정상적인 활동, 소프트웨어 및 시스템 취약성, 실시간 공격의 징후를 찾을 수 있습니다. 그리고 적절한 자동화를 통해 부족한 인적 자원의 낭비 없이 수동 프로세스에 비해 훨씬 빠르게 대부분의 문제를 처리할 수 있습니다.

설문 조사 데이터는 다음과 같은 결과를 보여줍니다.

- 거의 모든 응답자 **(88%)** 가 자사의 보안 지출이 증가할 것이라고 답변
- **35%** 는 보안 지출이 대폭 증가할 것이라고 답변
- 특히 클라우드 보안 **(41%)** 과 사이버 리스크 관리 **(32%)** 부문의 지출이 증가할 것
- 보안 중심 분석 추가 계획 **(22%)** 및 프로세스 자동화 추세**(22%)**

이번 조사에서 확인된 가장 좋은 소식은 IT와 보안 스펙트럼 전반에서 협업 수준이 높아졌다는 것입니다. 그리고 조직이 분석, 자동화, 인적 투자를 통해 클라우드 복잡성을 해결하는 데 보안 지출을 늘리고 있다는 점입니다.

데이터 시대의 과제에 대응하기 위해 IT 보안이 새로운 시대로 전환되었습니다. 응답자들은 계속해서 증가하는 과제를 해결하기가 그 어느 때보다 어렵다고 토로했으나, 보안 전문가들은 이제 미래의 성공을 위한 기반을 마련하고 있는 것으로 보입니다.

보안 지출 증액 우선순위

41% 클라우드 보안

32% 사이버 위험 관리

27% 네트워크 보안

24% 보안 운영

22% 보안 분석

21% 엔드포인트 보안

20% 데이터 프라이버시

19% 사이버 보안 직원 교육

17% 보안 테스트

15% 애플리케이션 보안

15% 인력 확보

14% 보안 서비스

12% 계정/액세스 관리

핵심 권고사항

많은 보안 책임자들이 심화되는 보안 과제에 대처하기 위한 조치를 마련하고 있습니다. 지출 증대와 기술 투자가 효과적이기 위해서는 제대로 된 전략이 뒷받침되어야 합니다. 또한 향상된 분석과 데이터 전반에 대한 명확한 뷰를 통해 클라우드 복잡성을 관리하는 것이 필수적입니다. 이번 조사 결과를 토대로 한 Splunk 의 제안의 핵심은 다음과 같습니다.

1. SOC 현대화.

보안 팀은 갈수록 진화하는 다양한 위협과 공격자들로부터 정해진 형태가 없는 전장에서 방어하고 있습니다. 보안 팀은 최첨단 지휘센터가 필요합니다. 아래 나열된 기술과 기법 중 어느 것도 단독으로 완전한 해결책이 될 수는 없습니다. 그러나 이러한 기술과 기법들을 결합하여 오늘날의 위협에 보다 효과적으로 대처할 수 있는 현대화된 SOC(security operations center) 를 구축할 수 있습니다.

제로 트러스트 (Zero Trust): 네트워크 경계가 아닌 사용자, 자산, 리소스에 중점을 둔 제로 트러스트는 보안 위험을 최소화합니다. 이 모델은 세 가지 원칙을 기반으로 합니다. 모든 사람과 모든 사물을 확인하고, 최소한의 액세스 권한을 제공하고, 침해가 발생했다고 가정합니다. 데이터 보안에 중점을 둔 제로 트러스트는 최종 사용자를 엄격하게 인증합니다. 이것은 더욱 세분화되고 분산된 보안 환경을 위해 필수적인 전략입니다.

보안 운영 프로세스 자동화: 이것은 필수입니다. 분석가가 모든 공격에 일일이 대응할 수는 없습니다. 대신 분석가는 자동화된 솔루션이 사람의 개입없이 이러한 공격을 식별하고 사람보다 빠르게 대응하도록 규칙을 작성할 수 있습니다. SOAR (Security Orchestration, Automation and Response) 과 UEBA (User and Entity Behavior Analytics) 를 통해 자동화의 이점을 실현할 수 있습니다.

최신 SIEM: 이번 조사에서 우리는 분석 투자의 결실이 최신 SIEM 임을 확인했습니다. SIEM 시스템은 네트워크 내 활동에 대한 완전한 가시성을 제공하여 실시간으로 위협에 대응할 수 있도록 해줍니다.

교육 및 인재 확보: 이것은 모든 조직이 어려움을 겪는 부분입니다. 앞서 언급한 다른 모든 기술이 더 작은 팀으로 더 많은 일을 할 수 있도록 도와 주지만, 궁극적으로 증가하는 위협에 직면한 조직은 보안 팀을 성장시켜야 합니다. 자동화와 분석을 통해 분석가의 효율성을 개선하고 작업에 사용하는 도구의 수를 줄임으로써 교육을 개선할 수 있습니다.

2. 종합적인 데이터 뷰 확보.

현대화된 SOC 에는 최고의 도구와 커스터마이즈가 포함됩니다. 그러나 이는 자칫 교육과 다양한 소스의 데이터로 사고를 파악하는 능력 측면에서 어려움을 야기할 수 있습니다. 복잡한 멀티 클라우드, 멀티 서비스 환경에서는 기존 보안 데이터뿐만 아니라 모든 데이터를 볼 수 있어야 합니다. 이러한 종합적인 엔드 투 엔드 관점은 보안 및 규제 준수뿐만 아니라 성공적인 개발 및 운영에도 중요합니다. 종합적인 데이터 뷰는 보안 팀과 IT 팀을 위한 SSOT (Single Source of Truth) 를 제공합니다.

3. 공급망 위협에 대한 접근방식 재고.

SolarWinds 해킹 사건 이후로 우리는 공급업체를 이용하여 조직의 시스템과 네트워크를 익스플로잇할 수 있는 적들을 걱정하게 되었습니다. 공급업체 감사라는 첫 번째 원칙은 생각보다 어렵습니다. 왜냐하면 '화상회의 벤더' 또는 '결제 처리 벤더'가 한 곳이라 하더라도 실제로는 외부 API 와 서비스를 통해 예닐곱 개 비즈니스 시스템으로 구성되기 때문입니다. 따라서 모든 데이터 요소와 플로우에 대한 가시성이 필요합니다. 또한 침해가 확인되었을 때 이를 차단하고 어떤 데이터가 유출되었는지 확인할 수 있도록 가장 신속하게 대응하는 방법을 알아야 합니다.

공급망 위협(및 기타 위협)에 대응하기 위해서는 네트워크 내에서 의심스러운 내부 확산 (lateral movement) 을 파악할 수 있는 기능을 강화해야 합니다. 공급 업체의 소프트웨어 패치를 통해 몰래 들어오든 탈취된 직원 계정을 사용하여 잠입하든 관계없이 먹이를 찾아 네트워크 내부를 돌아다니는 공격자를 포착할 수 있어야 합니다.

하지만 취약한 암호, 미흡한 다단계 인증 (MFA;multifactor authentication) 수단과 SSO(single sign-on) 솔루션 부재로 인해 이러한 전략에 구멍이 뚫릴 수 있습니다. 이러한 구멍을 메우기 위해서는 현대화된 SOC 와 정확하게 정의되고 면밀하게 모니터링되는 ID 정책, 강력한 실행 및 모니터링이 필요합니다.

4. 협업 이점 강조.

COVID-19 재난 대응에는 신속한 조치가 필요했으며 이로 인해 보안/IT 협업이 강화되었습니다. 보안 팀은 향후 발생할 수 있는 재난 대응을 위해 이러한 강화된 협업이라는 변화를 계속해서 가져가야 합니다. 궁극적인 목표는 조직에서 DevSecOps 를 실현하는 것입니다. 즉, 현재로서는 충분히 상호 연관되어 있지 않은 세 가지 관련 분야를 결합시키는 것입니다.

DevOps 신속한 소프트웨어 개발과 소프트웨어 및 디지털 경험의 고품질 제공을 위해 개발 팀과 운영 팀 간의 전통적인 사일로를 허물었습니다. 다음 단계는 여기에 보안을 통합하는 DevSecOps 입니다. DevSecOps 는 공동 목표와 측정, 그리고 전통적으로 사일로화 된 세 그룹 간의 마찰을 줄이는 도구 및 관행을 통해 세 가지 분야를 모두 단일 플로우로 가져옵니다. 이렇게 함으로써 보안 자동화의 기회를 제공하고 개발 프로세스 초기에 보안을 적용합니다.

조직이 이러한 철학적 변화를 완전히 수용할 준비가 되어 있지 않더라도 2020 년의 경험을 통해 IT 및 비즈니스의 모든 단계에서 통합 보안 사고의 중요성을 주장 할 수 있습니다.

누구도 정확히 알 수 없는 2021 년 이후에 대비하기 위해서는 이러한 준비가 필요할 것입니다.

산업별 주요 내용

산업 전반에서 응답 내용이 유사하게 나왔으나, 다음과 같은 몇 가지 부분에서 업종별로 독특한 동향과 데이터가 확인되었습니다.

통신/미디어

지난 2 년 동안 데이터 유출을 겪었다고 응답한 비율이 통신 회사에서 53% 로 가장 많았습니다. 이는 기술 회사 42%, 금융서비스 기업 41% 에 비해 높고, 전체 평균 39% 에 비해서도 훨씬 높은 비율입니다.

통신/미디어 회사는 보안 인력의 직무 기술 부족을 겪고 있다고 답한 비율이 44% 로 전체 평균 28% 에 비해 약 1.5배 높았습니다.

통신 회사는 DevOps 팀이 보안 팀을 우회하는 비율이 38% 로 전체 평균 24% 에 비해 높게 나타났습니다.

통신 회사는 핵심 워크로드와 애플리케이션의 75% 이상이 클라우드에서 처리된다고 응답한 비율이 23% 로 전체 평균 9% 에 비해 높습니다.

통신 회사는 원격 근무 증가로 인해 사이버 공격이 증가했다고 응답한 비율이 23% 로 기술 회사 16%, 전체 평균 12% 에 비해 높게 나타났습니다.

향후 12-24 개월 동안 보안 지출을 늘릴 것인지 묻는 질문에 통신 회사는 '그렇다, 대폭'이라고 응답한 비율이 50% 로 가장 많았습니다. 전체 평균은 35% 이며, 통신 회사와 더불어 제조업 부문만이 38% 로 평균을 상회하였습니다.

금융 서비스

금융 서비스 회사는 온프레미스 데이터센터와 퍼블릭 클라우드 환경 전반에서 보안 일관성을 유지하는 문제를 가장 적게 언급했습니다. 금융 서비스 회사의 36% 가 이 문제에 동의한 반면 전체 평균은 50% 였습니다.

금융 서비스 회사는 인력의 66% 가 원격 근무를하고 있다고 보고하여 원격 근무를 가장 적극적으로 도입하고 있는 것으로 나타났습니다. 이는 공공 부문보다 1% 높고 전체 평균 56% 에 비해 10% 높은 비율입니다.

금융 기관은 더 많고 다양한 최신 기기를 지원함으로써 보안 문제가 증가했다고 답한 비율이 가장 낮았습니다. 이렇게 답한 금융 기관의 비율은 13% 로 전체 평균 24%, 가장 높은 제조 부문 33% 와 기술 부문 28%에 비해 낮았습니다.

헬스케어

헬스케어/생명과학 분야는 보안 분석/운영을 온프레미스에서 클라우드로 이전하는 것이 보안 전략에 포함된다고 응답한 비율이 11% 로 전 산업 중 가장 낮았습니다. (전체 평균 19%, 가장 높은 산업은 금융 서비스 부문 23%)

헬스케어/생명과학 분야는 보안 운영 기술(프로세스 자동화, 보안 운영 시각화 등)에 투자할 것이라고 응답한 조직의 비율이 14%로 전 산업 가운데 가장 낮았습니다. 전체 평균은 24%, 가장 높은 분야는 기술 기업 (39%) 입니다.

제조

제조업체의 33% 가 기기 수 증가 및 다양화로 인해 어려움을 겪고 있습니다. 이는 전체 평균 (24%) 에 비해 1.4 배 높은 수치입니다.

제조업체들은 또한 전체 평균 (36%) 보다 약간 높은 비율인 42% 가 생산성 저하를 경험하고 있습니다.

제조 분야 기업들은 비보안 데이터와 보안 데이터를 통합하여 의사 결정을 지원하는 데 앞장서고 있습니다.

제조 분야에서 SaaS(software-as-a-service) 솔루션 사용 비율이 83% 로 가장 높게 나타났습니다. (전체 평균 69%)

유통

과도하게 많은 경고로 인해 어려움을 겪고 있다고 답한 비율이 유통 부문에서 전체 평균의 거의 두 배로 많았습니다 (유통 부문 36%, 전체 평균 20%).

또한 너무 많은 도구/벤더로 인해 보안 스택이 지나치게 복잡해졌다고 답한 비율도 유통 부문에서 가장 높게 나타났습니다 (유통 부문 39%, 전체 평균 25%).

공공 부문

4 개 이상의 IaaS 및 PaaS 프로바이더를 사용한다고 답한 비율이 공공 부문에서 가장 높게 나타났습니다. (공공 부문 19%, 전체 평균 8%).

이 수치는 2 년 내에 39% 로 증가할 것으로 예상되며 전체 평균 21% 를 여전히 상회할 것입니다.

공공 부문은 신규 애플리케이션에 대해 온프레미스 정책을 적용한다고 답한 비율이 전 산업 중 가장 높았습니다 (공공 부문 24%, 전체 평균 14%).

공공 부문은 과거 2 년 간 데이터 유출을 경험한 비율이 전 산업 중 가장 낮았습니다. (공공 부문 22%, 전체 평균 39%).

기술

기술 기업의 54% 가 보안 사고 후속 조치에 IT 팀의 상당한 시간을 투입하고 있는 것으로 나타났습니다 (전체 평균 42%)

또한 기술 기업들에서 내부자 공격 비율이 44% 로 높게 나타났습니다. 이는 통신/미디어 부문 47% 에 이어 두 번째로 높은 수준입니다. 전체 평균은 27% 입니다.

기술 부문은 통신/미디어 부문과 함께 공격이 가장 많이 증가한 것으로 보고되었습니다.

내부자 공격은 기술 부문 (44%) 과 통신/미디어 부문 (47%) 에서 가장 높게 나타났습니다. 전체 평균은 27% 입니다.

지역별 주요 내용

응답자들의 경험과 최신 보안 위협에 대한 대응 측면에서 지역 간 차이는 아주 미세한 수준이었습니다. 다만 몇 가지 주목할 만한 차이가 있었습니다.

아태지역 (APAC)

APAC 조직들은 클라우드 네이티브 애플리케이션 아키텍처 도입이 상대적으로 부진합니다. 아태지역 조직 중 52% 는 현재 클라우드 네이티브 환경의 비즈니스 크리티컬 워크로드가 전무한 상황입니다. 반면 이 비율이 북미 조직의 경우는 44%, 서유럽 조직의 경우는 49% 입니다. 그러나 아태지역에서 이를 따라 잡을 가능성이 높습니다. 평균적으로 아태지역 조직들은 비즈니스 크리티컬 워크로드의 56% 를 향후 24 개월 내에 클라우드 네이티브로 이전할 것으로 예상하고 있습니다(북미 57%, 서유럽 52%).

클라우드 네이티브 앱과 관련하여 APAC 응답자의 38% 가 클라우드 인프라 가시성 문제를 지적했습니다(북미 25%, 서유럽 26% 에 비해 많음). 또한 APAC 응답자 30% 가 클라우드 네이티브 애플리케이션을 지원하지 않는 도구 때문에 어려움을 겪고 있다고 답했습니다(북미 19%, 서유럽 20%).

COVID 이전에는 APAC 25%, 유럽 26% 에 북미 조직의 원격 근무 비율이 20% 로 가장 낮았습니다.

서유럽

유럽 조직의 42% 가 클라우드 네이티브 시나리오에서 멀웨어 탐지에 중점을 두는 경향이 있습니다(북미 및 APAC 의 경우 각각 32% 및 25%).

클라우드 네이티브 애플리케이션과 관련하여 북미 (52%) 와 유럽 (55%) 에서는 클라우드 전반의 일관성이 문제라고 답한 응답자들이 많았습니다 (APAC 의 경우 42%).

유럽 응답자들은 SolarWinds 와 유사한 공격에 대한 우려가 북미와 APAC 응답자들에 비해 다소 낮은 것으로 나타났습니다. (우려/매우 우려한다고 답한 응답자가 유럽은 74% 인데 비해 북미 77%, APAC 86%). 그러나 관련 예산을 증가시킬 계획이라고 답한 비율은 서유럽에서 40% 로 가장 많았습니다(북미 및 APAC 은 각각 28% 및 27%).

유럽 조직들은 실시간 데이터를 통한 자동화된 보안 프로세스를 갖춘 경우가 36% 로 다른 지역에 비해 1.6 배 많습니다 (북미 23%, APAC 23%)

북미

북미 지역이 퍼블릭 클라우드 인프라 도입에서 가장 앞선 것으로 나타났습니다. 북미 응답자의 47% 가 비즈니스 크리티컬 애플리케이션 및 워크로드의 절반 이상을 퍼블릭 클라우드에서 처리하는 반면 서유럽은 40%, APAC 는 25% 입니다.

클라우드 네이티브 앱과 관련하여 클라우드 전반의 일관성이 문제라고 답한 응답자가 북미 (52%) 와 유럽 (55%) 에서 APAC (41%) 에 비해 많았습니다.

조사 방법 및 설문 대상

이 설문 조사는 Enterprise Strategy Group 이 2021 년 2 월에 실시했습니다. 535 명의 응답자는 전 세계 9개 지역의 사이버 보안 및 IT 분야 시니어 레벨 의사 결정자로 구성되었습니다.

지역별 응답자 비율

- 북미 (미국, 캐나다): 48%
- 서유럽 (프랑스, 독일, 영국): 29%
- APAC (호주, 일본, 뉴질랜드, 싱가포르): 23%

산업별 응답자 비율

- 금융 서비스: 16%
- 제조 및 자원: 16%
- 헬스케어 및 생명 과학: 14%
- 유통: 13%
- 통신 및 미디어: 12%
- 기술: 9%
- 공공 부문: 7%
- 기타: 12%

스플렁크 보안 솔루션

Splunk Enterprise

Splunk 플랫폼은 데이터를 실질적인 비즈니스 결과로 전환하는 커스터마이즈 가능한 데이터 분석 플랫폼입니다. SaaS 및 다른 오픈소스 솔루션과 달리 Splunk Cloud 및 Splunk Enterprise 는 기존 기술 투자는 물론 IT/보안/비즈니스 시스템, 앱, 기기에서 생성된 광범위하고 방대한 데이터를 활용하여 거의 실시간으로 조사, 모니터링, 분석, 액션을 제공합니다. 자세히 보기.

Splunk Enterprise Security

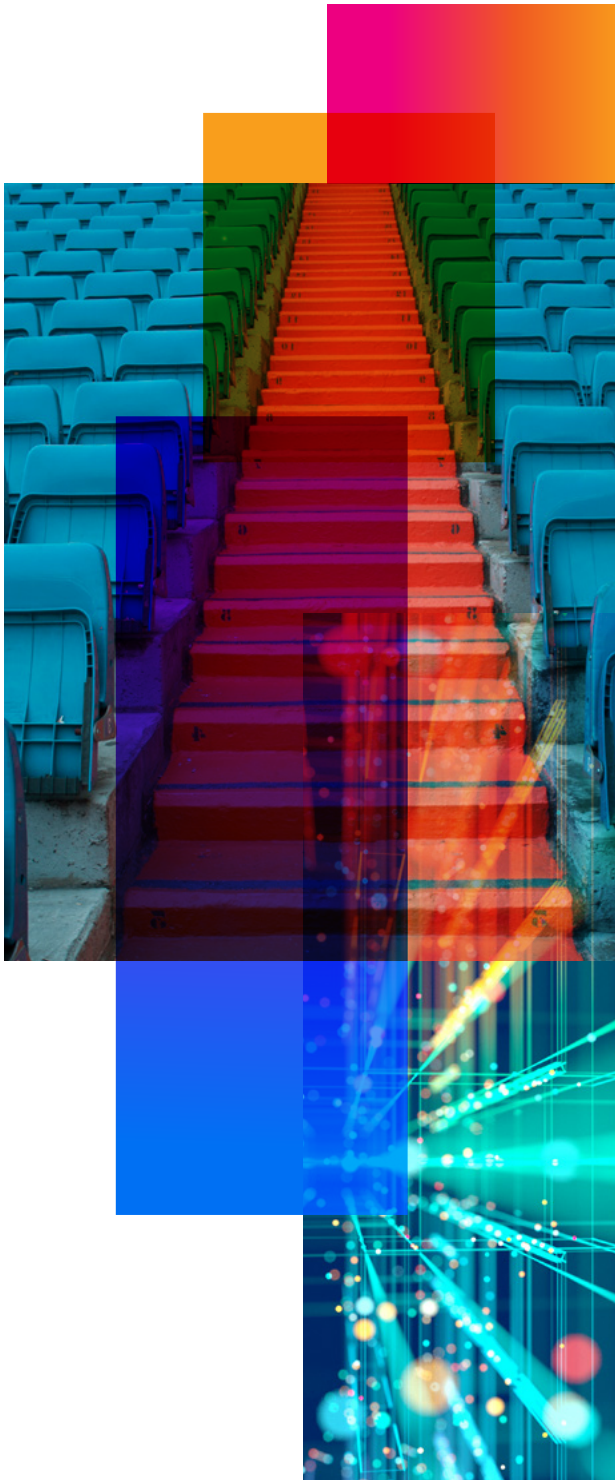
Splunk Enterprise Security(ES) 는 효율적인 위협 관리를 위해 실시간 보안 모니터링, 지능형 위협 탐지, 사고 조사 및 포렌식, 사고 대응을 제공하는 분석 기반 SIEM 솔루션입니다. Splunk ES는 보다 신속한 위협 탐지, 조사, 대응이 가능하도록 해줍니다. 자세히 보기.

Splunk User Behavior Analytics (UBA)

Splunk UBA 는 사용자, 엔드포인트 기기, 애플리케이션 전반에서 알려지지 않은 위협과 비정상적인 동작을 찾아내는 머신러닝 기반 솔루션입니다. 인력, 리소스, 시간 부족으로 인해 놓칠 수 있는 위협을 찾아냄으로써 기존 보안 팀을 보강하고 생산성을 높입니다. 자세히 보기.

Splunk Phantom

Splunk Phantom 은 세계적 수준의 SOAR (security orchestration, automation and response) 시스템입니다. Splunk Phantom 은 보안 인프라 오케스트레이션, 플레이북 자동화, 케이스 관리 기능을 결합하여 보안 팀, 프로세스, 도구를 통합합니다. 자세히 보기.z



Splunk Inc. (NASDAQ: SPLK) 는 Data-to-Everything 플랫폼을 통해 데이터를 액션으로 전환합니다. Splunk 기술은 모든 규모의 데이터를 조사, 모니터, 분석, 처리하도록 설계되었습니다. Splunk 의 강력한 플랫폼과 전문적인 데이터 활용을 통해 기업은 위험을 완화하고, 서비스 수준을 향상하고, 운영 비용을 절감하고, DevOps 협업을 강화하고, 새로운 제품 및 서비스 오퍼링을 개발할 수 있습니다.

자세히 보기

21-17605-Splunk-State of Security KR

splunk>