MANDIANT
NOW PART OF Google Cloud

위협 인텔리전스에 대한 글로벌 관점

본 ' 위협 인텔리전스에 대한 글로벌 관점 ' 보고서에서 알 수 있듯이 , 보안 팀은 고위 경영진이 위협의 본질을 완전히 파악하고 있지 못하다는 점을 우려하고 있습니다 . 이는 공격자와 공격 전술에 대한 인사이트 없이 중요한 사이버 보안 관련 의사 결정이 내려지고 있음을 의미합니다 .

Sandra Joyce

Google Cloud
Mandiant Intelligence
부문 부사장

이 보고서는 조직이 글로벌 사이버 보안 위협 환경을 탐색하는 방법에 대한 인사이트를 처음으로 제공합니다 . 조사 결과는 1,000 명 이상의 직원을 보유한 조직에서 보안 결정을 내리는 1,350 명의 비즈니스 및 IT 리더를 대상으로 진행한 광범위한 인터뷰를 바탕으로 합니다 . 응답자는 3 개 지역의 13 개국에 위치한 금융 서비스 , 의료 , 정부기관을 비롯한 18 개 부문에 종사하고 있습니다 .

응답 내용의 품질과 글로벌 범위는 대규모 조직의 사이버 보안 의사 결정권자가 위협 인텔리전스를 보는 시각과 운영 방법에 대한 스냅샷을 제공합니다 .

조사 결과

응답 내용을 바탕으로 팀이 위협 인텔리전스를 중요하게 여기고 여러 출처로부터 정보를 얻지만 종종 정보를 전사 영역에 효과적으로 적용하는 데 어려움을 겪는다는 초기 가설을 확인할 수 있었습니다 .

세계 최대 기업의 보안 팀들은 조직 전반에 걸친 의사 소통에 대해 상당한 부담감을 느낄 뿐만 아니라 어려움까지 겪고 있습니다 . 그리고 보안 팀은 공격자에 대한 더 나은 정보의 필요성을 분명히 이해하고 있지만 , 대부분은 누가 , 왜 조직을 공격하는 지를 완전히 이해하지 못한 채 의사 결정을 내립니다 . 이러한 가시성 격차로 방어 체계가 의도한 목표를 달성하지 못할 수 있습니다 .

96% 조직에서 사용 중인 위협 인텔리전스의 품질에 만족한다는 응답자 비율

47% 보안 조직 전체에 위협 인텔리전스를 효과적으로 적용하는 것이 가장 큰 과제 중 하나라고 언급한 응답자 비율

67% 고위 경영진이 조직에 대한 사이버 위협을 과소평가한다고 생각하는 응답자 비율

96% 보안 의사 결정권자는 어떤 사이버 공격자가 조직을 표적으로 삼을 수 있는지 이해하는 것이 중요하다고 생각하는 응답자 비율

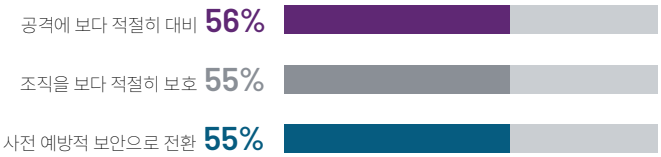
79% 적어도 대부분의 경우 공격자에 대한 정보 없이 의사 결정을 내린다고 답한 응답자 비율

실무자의 위협 인식 및 보안 자신감

이 보고서는 조직이 사이버 공격에 대처하는 높은 수준의 자신감과 보안 팀이 공격자와 공격 전술 , 기술 및 절차 (TTP) 에 대한 포괄적인 정보 없이 의사 결정을 내리는 경향 사이에 전 세계적으로 큰 격차가 있음을 보여줍니다 .

또한 보안 의사 결정권자의 상당수 (96%) 가 조직을 표적으로 삼을 수 있는 사이버 공격자를 파악하는 것이 중요하다고 믿고 있음을 보여줍니다 .

보안 의사 결정권자로서 귀사를 표적으로 삼고 있는 사이버 공격자를 파악하는 것이 왜 중요하다고 생각하십니까 ?

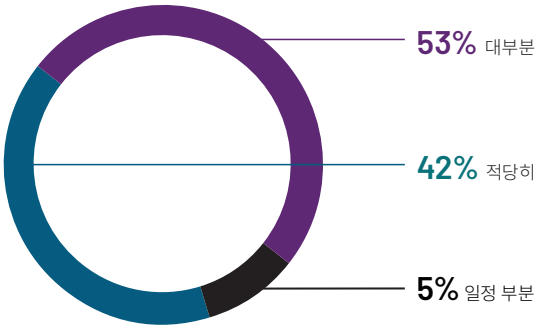


사이버 공격자에 대한 정보 획득의 중요성에 대해 거의 보편적으로 이해하고 있고 96% 의 응답자가 위협 인텔리전스의 품질에 만족한다고 언급했음에도 불구하고 , 응답자의 79% 는 조직을 표적으로 삼을 수 있는 공격자에 대한 인사이트 없이 , 사이버 공격에 대한 대부분의 의사 결정을 내린다고 말했습니다 . 35% 만이 조직이 다양한 위협 그룹과 TTP 에 대해 종합적으로 이해하고 있다고 답했습니다 .

또한 사이버 보안 의사 결정권자의 67% 는 고위 경영진이 여전히 조직에 가해지는 사이버 위협을 과소평가하고 있다고 믿고 있으며 , 3 분의 2 이상 (68%) 이 위협 환경에 대한 조직의 이해도를 높여야 한다는 데 동의했습니다 .

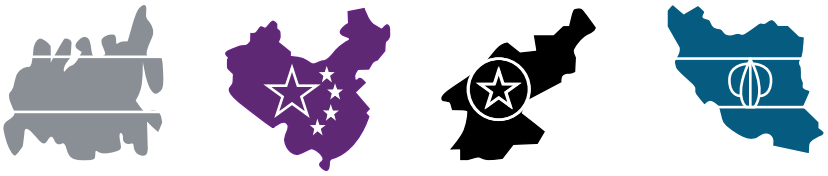
이러한 우려에도 불구하고 의사 결정권자들 사이에서는 조직이 보안 위협을 억제할 수 있다는 자신감이 높습니다 . 거의 모든 응답자 (95%) 가 조직에서 보통에서 매우 효과적인 수준의 사이버 보안 프로그램을 보유하고 있음을 고위 경영진에게 증명할 수 있다고 답했습니다 .

조직에 효과적인 사이버 보안 프로그램이 있음을 고위 경영진 (예 : 이사회 또는 최고 경영진) 에게 어느 정도 증명할 수 있다고 생각하십니까 ?



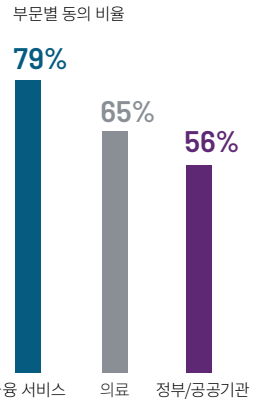
많은 보안 의사 결정권자가 조직이 금전적 동기가 있는 공격자 (91%) 나 핵티비스트 공격자 (89%), 국가 차원의 공격자 (83%) 로 인해 발생하는 심각한 사이버 보안 공격으로부터 스스로를 방어할 준비가 되어 있다고 확신하고 있습니다 .

국가 차원의 공격이 발생할 경우 , 다음 중 귀사에서 완벽하게 방어할 수 없을 것이라고 생각하는 국가는 어디입니까 ?



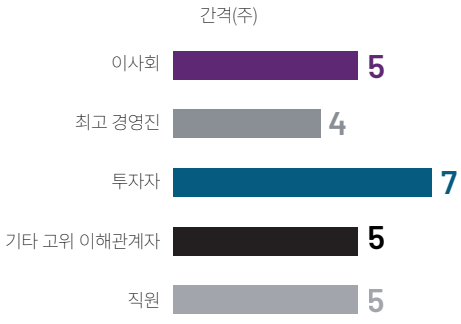
러시아 57% 중국 53% 북한 52% 이란 44%

동의하십니까 , 동의하지 않으십니까 ? 우리 조직은 위협 환경에 대한 이해를 개선해야 합니다 .



공격자에 대한 정보 부족에 대한 한 가지 가능한 설명은 보안 의사 결정권자와 광범위한 조직 간의 의사 소통이 드물다는 것입니다 . 응답자들은 이사회 , 최고 경영진 , 기타 고위 이해관계자 등 보안 팀 이외의 그룹과 함께하는 사이버 보안 관련 논의는 평균적으로 4~5 주에 한 번밖에 진행되지 않는다고 밝혔습니다 . 투자자들과의 논의 빈도는 평균 7 주에 한 번으로 더 낮습니다 .

귀하의 부서에서 다음 그룹과 사이버 보안에 대해 얼마나 자주 논의합니까 (모든 지역 평균)?

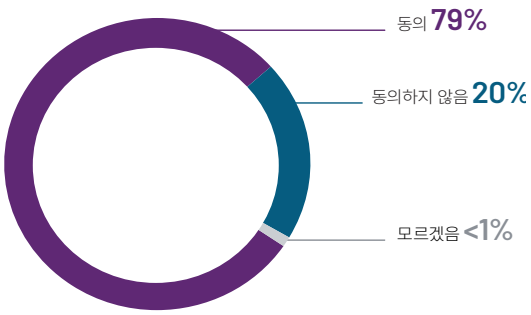


인텔리전스 운영 및 관련 리스크 문제

위협 인텔리전스의 중요성은 모두 잘 이해하고 있습니다 . 대다수의 응답자가 중요하다고 생각하는 식별 대상은 공격자 (85%), 공격자가 사용하는 툴 및 기술 (88%), 공격자의 동기 (87%) 였습니다 . 상세한 위협 인텔리전스의 중요성에 대해 공감하고 있음에도 불구하고 보안 팀은 이를 따르지 않는 것으로 확인되었습니다 . 34% 만이 사이버 보안 방어 및 운영을 테스트할 때 항상 잠재적인 공격의 출처를 고려한다고 말했습니다 .

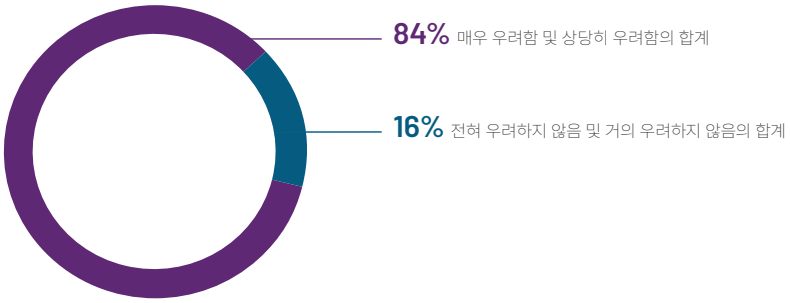
보안 팀은 또한 위협을 식별하고 조치를 취하는 데 필요한 시간을 할애하지 않습니다 . 응답자의 상당수 (79%) 는 조직이 사이버 보안 내에서 중요한 동향을 식별하는 데 더 많은 시간과 에너지를 집중할 수도 있지만 , 거의 모든 응답자 (98%) 가 최신 위협 인텔리전스에 기반해 보다 빠르게 사이버 보안 전략을 바꿔 나가야 한다고 말했습니다 .

동의하십니까 , 동의하지 않으십니까 ? 우리 조직은 중요한 사이버 보안 동향에 더 많은 시간과 에너지를 집중할 수도 있습니다 .



보다 실행 가능한 위협 인텔리전스를 확보하기 위해 보안 팀은 매일 방대한 양의 데이터를 처리해야 합니다 . 응답자의 대다수 (84%) 는 직면한 경고 및 데이터의 수로 인해 위협이나 사고를 놓치지는 않을까 우려한다고 말했습니다 . 이러한 정보 과부하는 직원의 복지에도 영향을 미칩니다 . 보안 팀의 3 분의 2 이상 (69%) 이 업무 부담이 과하다는 것을 인정했습니다 .

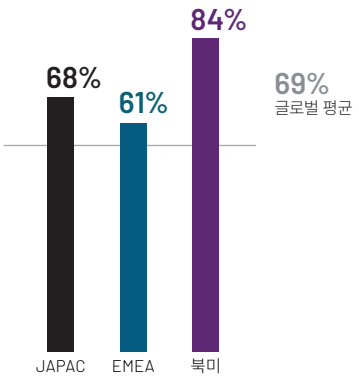
직면한 경고 및 데이터의 양으로 인해 조직에서 실제 위협 / 사고를 놓칠 수 있다는 우려 수준은 어느 정도입니까 ?



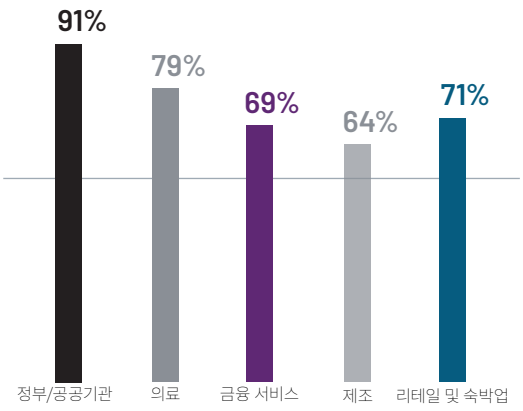
위협 인텔리전스와 관련된 데이터 및 경고의 양 때문에 번아웃될 위험이 가장 큰 응답자는 북미 지역의 응답자였습니다 . 산업 분야 중에서는 정부 응답자들이 가장 업무 부담이 과하다고 느끼는 것으로 밝혀졌습니다 .

처리해야 하는 데이터 및 / 또는 경고의 양이 증가함에 따라 IT 보안 직원에게 가중되는 업무 부담은 어느 정도 수준입니까 ?

지역별 응답에는 '다소' 및 '완전히' 과한 업무 부담이 섞여 있음



산업 분야별 응답에는 '다소' 및 '완전히' 과한 업무 부담이 섞여 있음

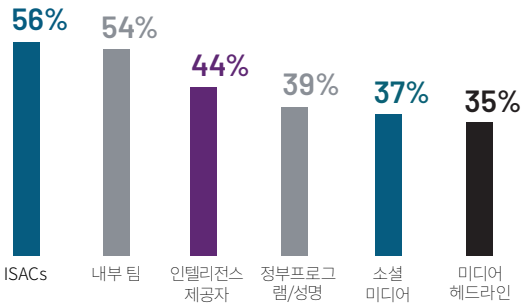


정보 과부하는 거의 모든 조직의 문제로 명확하게 파악되었지만 응답자의 거의 절반 (47%) 은 조직 전체에 인텔리전스를 효과적으로 적용하는 것이 위협 인텔리전스를 사용할 때 직면하는 가장 과제 중 하나라고 답했으며 , 38% 는 이 정보를 가지고 취해할 조치를 아는 것이 또 다른 과제라고 밝혔습니다 . 절반 이상 (53%) 은 사이버 보안 분야의 글로벌 인재 부족이 최신 트렌드를 사전에 파악하고 대응하는 역량에 위협이 된다고 말했고 , 42% 는 끊임없이 진화하는 위협의 본질을 지적했습니다 .

팀은 수집한 위협 인텔리전스를 활용하여 운영하는 데 어려움을 겪고 있지만 광범위한 출처에서 인텔리전스를 계속 수집하고 있습니다 .

귀하의 조직은 위협 환경을 최신 상태로 유지하기 위해 어떤 출처를 사용합니까 ?

글로벌 응답



보안 팀에서 수집한 정보는 해당 팀 내에만 보관되거나 전사적으로 광범위하게 공유되지 않는 경우가 많습니다 . 응답자의 61% 는 위협 인텔리전스를 IT 팀과 공유하여 인프라 및 애플리케이션 취약성을 해결하거나 IT 보안 리더와 공유하여 보안 작업의 우선순위를 설정한다고 말했습니다 . 훨씬 적은 비율 (38%) 이 위험 인식을 위해 다른 직원들과 인텔리전스를 공유했습니다 .

사이버 위협 인텔리전스를 효과적으로 운용하고 투자 가치를 극대화하려면 다음을 수행해야 합니다 .

신뢰할 수 있고 시의적절하며 실행 가능한지 확인하기 위해 사용하는 데이터 평가

신뢰할 수 있는 위협 인텔리전스 프로그램은 견고한 기반 위에 구축되어야 합니다 . 이러한 속성은 필수적인 출발점입니다 .

조직 및 산업에 특정한 실제 위협 이해

공격자 , 공격 동기 , 전술 , 기술 및 절차 (TTP) 에 대해 명확하게 파악하여 적절한 방어 태세를 갖추십시오 .

이해관계자와 소통

고위 경영진과 이사회 수준까지 관련 인텔리전스 (전술적 , 운영적 또는 전략적) 를 적절한 이해관계자 그룹에 정기적으로 제공하는 절차를 마련하여 최적의 보안 및 비즈니스 결정을 내릴 수 있도록 합니다 .

정말 중요한 문제 해결을 위한 리소스 우선순위 설정

인텔리전스를 활용하여 현재 조직에서 가장 집중적으로 대응해야 할 위협이 무엇인지 파악하십시오 . 취약성과 노출을 평가하고 , 중요도에 따라 위험 등급을 부여한 다음 , 올바른 순서로 문제를 해결하십시오 .

방어 태세 점검

식별한 공격자의 일반적인 공격 전술에 대한 조직의 대응 역량을 사전에 테스트하십시오 . 이러한 특정 그룹에 대한 보호 상태를 검증하고 시간을 두고 프로그램의 개선 사항을 측정하십시오 .

조치 실행

보안 시스템 및 프로세스 전반에서 위협 인텔리전스를 활용하여 잠재적인 위협으로부터 사전에 보호하십시오 .

맺음말

빠르게 진화하는 위협 환경에서 조직은 금전적 이득을 노리는 악의적인 사이버 범죄자뿐만 아니라 경제적 혼란 , 스파이 활동 및 중요 인프라를 표적으로 삼으려는 국가 차원의 공격으로부터 조직을 방어해야 합니다 .

이러한 맥락에서 의사 결정권자는 위협 인텔리전스를 사용하여 문제가 발생하기 전에 위협을 예상하고 이를 더 효과적으로 처리할 수 있습니다 . 실제로 , 대다수의 보안 의사 결정권자는 위협 인텔리전스의 중요성을 이해하고 있으며 위협 인텔리전스가 있을 때 더 나은 결정을 내릴 수 있습니다 .

위협 인텔리전스가 가져올 수 있는 가치에 대해 거의 만장일치로 공감함에도 불구하고 보안 팀은 이를 위협에 안정적으로 적용하지 못하고 있습니다 . 보안 결정의 절반 이상이 잠재적인 공격자에 대한 위협 인텔리전스 없이 이루어집니다 .

보안 팀은 팀이 처리해야 하는 데이터에 대처하기 위해 고군분투하고 있으며 , 때로는 충분히 숙련된 인력이 부족하고 보유한 정보로 무엇을 해야 할지 항상 알지 못하기 때문에 실제 위협을 놓치고 있다고 생각합니다 . 공격자에 대한 인텔리전스를 더 잘 처리할 수 있을 때까지 조직은 계속해서 증가하는 파괴적이고 파멸적인 사이버 공격에 취약한 상태로 남아 있을 것입니다 .

설문조사 방법 : Mandiant 의 의뢰로 2022 년 8 월에서 9 월 사이에 글로벌 시장 조사 회사인 Vanson Bourne 에서 " 위협 인텔리전스에 대한 글로벌 관점 " 이라는 설문조사를 실시했습니다 . EMEA, 북미 및 JAPAC 에서 직원 수가 1,000 명 이상인 조직의 IT 보안 의사 결정권자 1,350 명으로부터 피드백을 받았습니다 .

자세한 정보 : www.mandiant.kr

Mandiant

서울특별시 강남구 테헤란로 518 섬유센터빌딩
13 층 101 호

02-6959-4017
korea@mandiant.com

Mandiant 소개

Mandiant 는 역동적 사이버 방어 , 위협 인텔리전스 및 침해 사고 대응 서비스 분야에서 인정 받고 있는 리더로서 , 수십 년간 사이버 보안의 최일선에서 쌓아온 경험을 확장하여 조직이 사이버 위협에 맞서 대응 태세를 갖출 수 있도록 지원합니다 . Mandiant 는 이제 Google Cloud 의 자회사가 되었습니다 .

MANDIANT
NOW PART OF Google Cloud

EXT-RT-KO-KR-000482-01