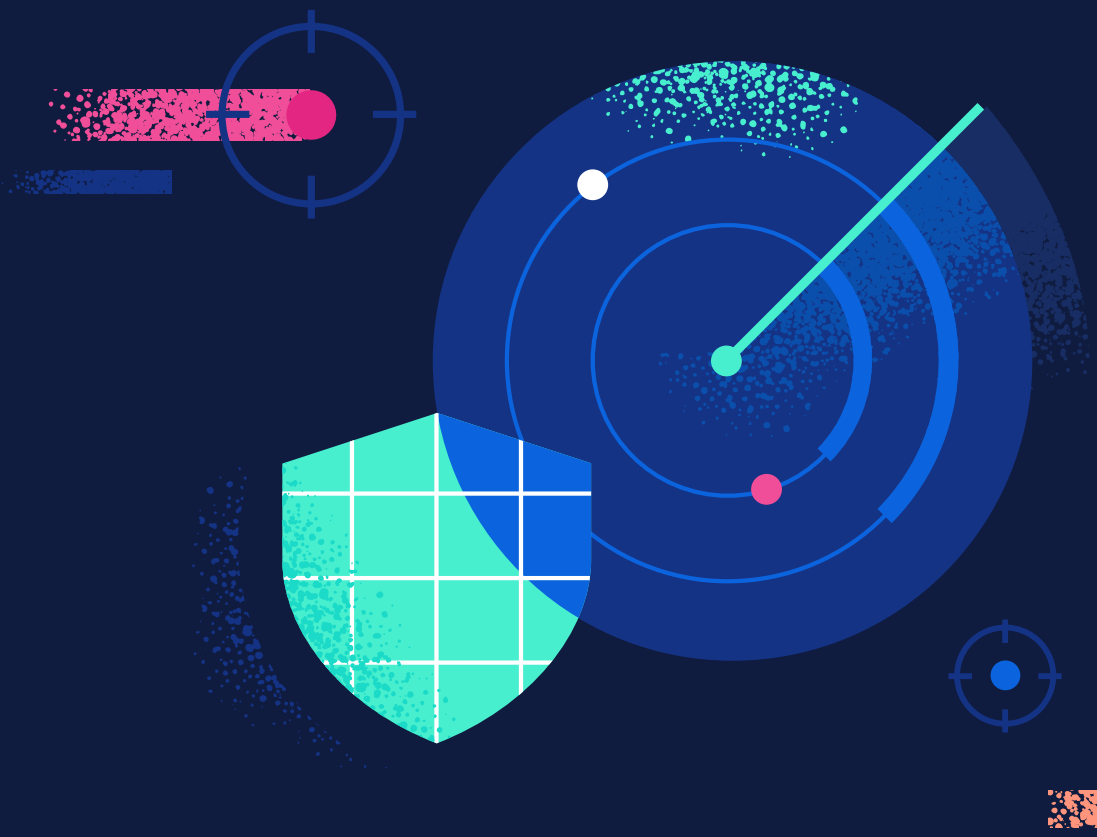

elastic | The Search AI Company

2025년 SIEM 구매자 가이드

다음 SIEM 선택 시 주요 고려 사항

보안 운영을 현대화하여 탐지, 조사, 대응 촉진

AI의 부상, 클라우드 서비스의 성장, 데이터 기반 의사 결정의 필요성과 같은 추세가 기업 혁신을 주도하고 있습니다. 이러한 역학 관계는 기존의 방어 체계를 약화시키고 사이버 기술 격차를 심화시키고 있습니다.

SOC는 어떻게 적응해야 할까요?

그 어느 때보다 중요한 최신 SIEM

보안 운영 팀은 임무 달성에 핵심적인 역할을 합니다. 효율성을 향상시키는 최신 SIEM 기능으로 보안 운영 팀이 뛰어난 역량을 발휘할 수 있도록 지원하세요.

유연한 배포: 쉽게 확장되고 멀티 클라우드, 하이브리드 및 온프레미스 아키텍처를 지원하는 SIEM으로 민첩성을 유지하세요.

인사이트와 지침: 분석가에게 관련 컨텍스트, AI 기반 권장 사항, 기본 제공 플레이북을 제공하여 더 스마트하고 빠른 의사 결정을 내릴 수 있도록 지원하세요.

완벽한 가시성: 사각지대를 제거하고 효율적으로 보관된 아카이브를 즉시 분석할 수 있는 SIEM을 통해 전체 공격 표면을 통합적으로 파악하세요.

자동화: 수동 워크플로우를 자동화하여 체류 시간을 줄이고 팀 생산성과 사기를 향상시키세요.

고급 분석: 탐지, 조사, 대응을 가속화하는 최첨단 분석으로 기존 방법을 뛰어넘으세요.

확장된 보호: 기본 엔드포인트 및 클라우드 보안 기술을 배포하거나 서드파티 기술을 통합하여 방어를 강화하세요.

고유한 요구 사항 고려

SIEM을 교체하시든, 처음부터 시작하시든, 잘 찾아오셨습니다. 다음 SIEM을 선택하려면 조직의 우선 순위, 팀의 기술 및 프로세스, 공격 표면에 대한 적합한 방어 수단을 고려하세요.

주요 고려 사항과 관련 SIEM 지침을 계속 읽어보세요.

조직

다음 SIEM이 조직의 필요에 맞게 능숙하게 조정되는지 확인하세요.

주요 고려 사항	SIEM 지침
보유하고 있는 가장 가치 있는 자산은 무엇인가?— 그리고 그 자산을 원하는 사람은 누구인가?	귀하의 조직에 인출될 수 있는 금융 자산이 있나요? 경쟁사가 알고 싶어할 만한 영업 비밀이 있나요? 랜섬웨어에 감염될 수 있는 시스템이 있나요? 판매 가능한 PII가 있나요? 공격자가 방해할 수 있는 중요 인프라가 있나요? 위협 환경이 조직의 노출 영역 — 및 위험 성향 —과 어떻게 교차하는지 이해하는 것은 우선 순위를 설정하는 데 필수적입니다. 위험 매트릭스와 전반적인 전략이 SIEM 투자를 어떻게 이끌어야 하는지 고려하세요.
SOC가 액셀러레이터인가, 아니면 차단자인가?	보안 운영 팀은 공격자를 차단하는 동시에 주요 이니셔티브를 지원해야 합니다. 두 가지를 모두 달성하려면 개방적이고 투명한 SIEM의 민첩성이 필요합니다. 폐쇄형 보안 제품에는 워크플로우를 자동화하는 통합 기능과 비즈니스와 함께 발전할 수 있는 유연성이 부족한 경우가 많습니다. 즉, 프로세스가 중단되고 도구가 너무 커지며 분석가의 속도가 느려집니다. 민첩성을 유지하려면 다음과 같은 제약 조건에 주의하세요. • NIH 증후군(서드파티가 개발한 기술이나 연구 성과는 인정하지 않는 배타적 조직 문화) • 최신 기술과의 제한된 통합 • 유연성 없는 라이선싱(예: 사용 사례별, 바이트별) • 비공개 코드 새로운 사용 사례로 확장할 수 있는 다양성을 제공하는 솔루션으로 혁신을 실현하세요. 라이선싱을 통해 필요의 변화에 맞춰 확장 및 축소하고 새로운 기능을 채택할 수 있는지 확인하세요. 신속한 로드맵 발전, 활발한 사용자 커뮤니티, 미래의 엔터프라이즈 기술과의 광범위한 상호 운용성에 대한 기록을 찾아보세요.
공급업체 종속에 대해 염려하고 있는가?	공급업체 종속은 좌절의 원인이 됩니다. 이상적으로는 무료 티어를 포함하여 유연한 라이선스를 제공하는 솔루션을 선택하면 조직이 제어권을 유지하는 데 도움이 됩니다. 제품 상호 운용성은 공급업체 종속을 방지하는 중요한 보루입니다. 이는 SIEM 뿐만 아니라 위협 인텔리전스 피드 및 플랫폼, AI 기술, SOAR 기능과 같은 인접 기능에도 해당됩니다. 따라서 다른 솔루션들과 잘 작동하는 솔루션만 선택하세요. 클라우드 인프라는 잠재적인 종속을 초래하는 또 다른 경로입니다. SIEM 배포 옵션은 다양하며, IaaS 공급업체 옵션이 제한되어 있고 하이브리드 및 멀티 클라우드 아키텍처에 대한 지원이 제대로 이루어지지 않습니다. 다음 SIEM이 진화하는 디지털 복원력 및 규정 준수 요구 사항을 충족할 수 있는 옵션을 제공하는지 확인하세요.

elastic

팀 및 프로세스

분석가가 긍정적인 영향을 미칠 수 있도록 역량을 강화하세요.

주요 고려 사항	SIEM 지침
SOC가 인재를 유치하고 유지하는가?	조직의 70%는 인력 문제로 인한 위험이 증가하고 있으며, 특히 AI/ML 및 클라우드 보안 분야에서 여전히 숙련된 실무자가 부족합니다[1]. 분석가는 일반적으로 18개월마다 역할을 변경하며, 이를 채우고 확대하는 데 6~12개월이 걸립니다[1]. 팀의 기술을 개발하고 AI로 보강하여 실무자가 새로운 방식으로 기여할 수 있도록 역량을 강화하세요. 최신 SIEM은 직관적인 UI에 관련 컨텍스트, 인사이트 및 지침을 표시하여 새로운 분석가 학습 곡선을 낮추고 숙련된 인력이 더 많은 성과를 달성하도록 지원합니다. 사용자 기반이 크고 성장하고 있으며 제품 모멘텀도 강력한 SIEM을 선택하여 채용 풀을 확장하세요. 분석가 번아웃의 주요 원인인 과도한 인지 부하로 인한 스트레스를 해결하여 유지율을 높이세요. 다음 행에 자세히 설명된 대로 분석가가 빠르고 정확한 의사 결정을 내릴 수 있도록 지원하세요.
팀이 얼마나 원활하게 위협에 대응할 수 있는가?	조직에는 실무자와 보조를 맞출 수 있는 SIEM이 필요합니다. 안타깝게도 대부분의 보안 팀은 여전히 여러 가지 다양한 도구와 데이터 세트를 사용해야 합니다. 단절된 워크플로우를 연결하고 간소화하려면 SIEM은 다음을 수행해야 합니다. • 모든 관련 데이터에 대한 단일 창을 통해 컨텍스트 전환 최소화 • 대량 데이터 리하이드레이션 없이 모든 데이터 티어(예: 핫, 콜드, 프로즌)에 대한 즉각적이고 통합된 검색 지원 • 실행 가능한 플레이북과 AI 지원으로 실무자 안내 • 경보 분류와 같은 일상적이고 지루한 작업 자동화 • 위험에 따라 조사 및 대응 노력의 우선 순위 지정 • Elastic 및 서드파티 보안 도구를 위한 사례 관리, RBAC, 워크플로우 커넥터를 통한 협업 촉진
표준 운영 절차를 어떻게 구현하는가?	성숙한 SOC는 공격 차단, 증거 수집, 보고와 같은 주요 프로세스에 대한 세부 절차를 통해 운영됩니다. SIEM은 팀이 이러한 관행을 플레이북에 성문화하고 점진적으로 자동화할 수 있는 경로를 제공하도록 지원해야 합니다. 프로세스를 처음부터 운영하려면 시간과 전문 지식이 필요하므로 전문가가 작성한 조사 지침과 AI 기반 지원을 제공하는 SIEM을 찾으세요. 협업을 촉진하고 관련 아티팩트(예: 경보, 데이터, 메모)를 중앙 집중화하기 위해 솔루션은 성숙한 사례 관리 기능도 제공해야 합니다.

1. ISACA, 2023

elastic

생성형 AI를 어떻게 활용할 계획인가?	다음과 같이 AI를 효과적이고 안전하게 사용할 수 있는 플랫폼을 찾아보세요. **모델에 구애받지 않음:** 여러 주요 모델과 모델 제공업체 간을 선택하고 전환할 수 있는 솔루션을 선택하여 비용, 속도, 정확성 및 개인 정보 보호에 대한 통제권을 확보하세요. **검색 증강 생성(RAG):** 공용 대규모 언어 모델(LLM)을 갖춘 SIEM을 선택하면 개인 저장소에서 수집된 관련 컨텍스트(예: 경보, 자산 중요도, 사용자 위험 점수)로 사용자 프롬프트를 즉각적이고 안전하게 보강하는 RAG를 사용하여 팀을 위해 훈련된 것처럼 작동합니다. **포괄적인 가시성:** 공격 표면 전체에서 컨텍스트에 액세스하면 특히 복잡한 멀티 벡터 공격 시나리오에 대한 LLM 생성 응답의 정확성이 향상됩니다. **확장성:** 생성형 AI 기능이 프로덕션 수준의 데이터 볼륨과 복잡한 쿼리를 통해 실제 환경의 요구 사항을 충족하도록 확장되는지 확인합니다. **세분화된 개인 정보 보호 제어:** 민감한 데이터가 실수로 공개되는 것을 방지하려면 문서 및 필드 수준 제어를 통해 기본적으로 그리고 필요에 따라 민감한 데이터를 익명화하거나 수정하는 기능을 확인하세요.
자동화 계획은 무엇인가?	레거시 제품은 독점 코드, 제한된 API 및 기타 상호 운용성 장벽으로 인해 자동화를 방해합니다. 에코시스템의 도구와 원활하게 연결할 수 있도록 내부에서부터 자동화를 위해 설계된 SIEM을 선택하세요. 기본 및 서드파티 기술에 대한 API 우선 전략, 공개 코드, 반자동 및 완전 자동화된 대응 작업을 찾아보세요. 이러한 기능은 데이터 공유, 워크플로우 오케스트레이션 및 자동화된 대응을 촉진하여 프로그램 효율성을 강화합니다. 또한 많은 프로그램은 기본적으로 개발된 기능, 볼트온 기능 또는 통합 기능을 통해 SIEM이 지원하는 보안 오케스트레이션, 자동화 및 대응(SOAR) 기능을 고려해야 합니다. 경험에 따르면, 대부분의 조직은 기본 제공된 SOAR 기능의 핵심 세트와 서드파티 SOAR 플랫폼(예: Tines, Swimlane, Torq, ServiceNow SecOps, TheHive)과의 심층적인 통합 목록을 모두 제공하는 솔루션을 통해 최상의 서비스를 제공받습니다. 이 접근 방식을 사용하면 적합하다고 판단되는 SOAR 기능을 채택한 다음 원하는 시스템으로 발전시킬 수 있습니다.
실무자가 다른 팀과 어떻게 협력하는가?	사고, 특히 더 넓은 비즈니스에 영향을 미치는 사고를 조사하고 대응하려면 IT 및 법무팀과 같은 인접 팀과 협력해야 하는 경우가 많습니다. 협업을 간소화하기 위해 SIEM은 사고 및 작업 관리 도구(예: Jira, ServiceNow ITSM)와 원활하게 연동되어야 합니다. 안전하고 규정을 준수하는 데이터 공유를 촉진하려면 관리자가 여러 다른 사용자가 액세스할 수 있는 데이터 원본과 개별 필드를 지정할 수 있도록 세분화된 역할 기반 액세스 제어(RBAC)를 제공해야 합니다. 또한 SIEM을 옵저버빌리티 도구와 통합함으로써 보안 팀은 인프라 및 애플리케이션 성능에 대한 인사이트를 얻을 수 있으므로 근본 원인을 더 빠르게 분석하고 DevOps 및 IT 운영과 같은 팀과 더욱 효과적으로 협업할 수 있습니다.

elastic

공격 표면

전체적인 분석을 위해 모든 보안 관련 데이터를 수집하세요.

주요 고려 사항	SIEM 지침
지금 그리고 곧 어떤 데이터 소스가 중요한가?	오늘날의 공격자들을 극복하는 데 중요한 가시성을 확보하는 것은 어렵지만 매우 중요하며, 공급업체와 기술 간의 상호 운용성이 필요합니다. 폐쇄형 포트폴리오를 통해 필요한 모든 가시성을 제공할 수 있다고 주장하는 대기업은 현실적이지 않습니다. SIEM은 데이터의 양, 다양성, 속도에 관계없이 관련 데이터를 중앙 집중화해야 합니다. 이 데이터를 개방형 스키마(예: CEF, ECS, OCSF)로 정규화하고 비정형 검색 및 후속 분석을 위해 원시 사본을 보존해야 합니다. 사전 구축된 통합 기능으로 새로운 데이터 원본의 온보딩을 간소화할 수 있습니다. 커넥터 수를 무시하고 대신 현재 및 향후 도구와의 중복을 평가하세요. 또한 새로운 통합의 속도와 기존 통합을 유지하기 위한 노력도 검토하세요. 특정 기술 영역의 경우, 다음에 대해 더 자세히 알아보세요. • **클라우드 인프라 및 애플리케이션:** SIEM이 IaaS 및 PaaS 기술 전반에 대한 가시성을 제공하는가? 클라우드 워크로드에 대해서는 어떤가? 컨테이너와 오케스트레이션 도구의 경우는 어떤가? 분석가가 메트릭, 애플리케이션 추적 및 CI/CD 로그에 액세스할 수 있는가? • **호스트 원격 분석:** 분석가가 풍부한 호스트 활동 및 시스템 메트릭에 액세스할 수 있는가? 임시 검사를 수행할 수 있는가? • **네트워크 활동 및 흐름:** SIEM을 통해 서로 다른 네트워크 장치, 클라우드 기술 및 호스트 전반에 걸쳐 균일한 분석을 수행할 수 있는가? • **사용자 활동 및 컨텍스트:** SIEM이 광범위한 소스의 사용자 데이터를 연관시키고 신속한 분석을 위해 이를 보강하는가? 권한 있는 사용자, 위험한 사용자 등을 식별하는가? • **IoT 및 OT 데이터:** SIEM이 일반적인 IoT 및 OT 데이터 형식을 지원하는가? • **서드파티 컨텍스트:** SIEM은 위협 인텔리전스, 취약성, 자산 데이터 및 기타 컨텍스트로 데이터를 보강하여 SecOps, 위협 인텔리전스 관리, 취약성 관리 및 공격 표면 관리를 용이하게 하는가? CTI 분석가가 동일한 플랫폼을 사용할 수 있는가?
새로운 데이터 소스를 얼마나 자주 온보딩해야 하는가?	SIEM은 일반적인 엔터프라이즈 SOC에 배포된 수십 가지 보안 기술 각각에 대해 기본 지원을 제공하지 않으므로, 광범위한 노력과 전문 지식 없이 맞춤형 데이터 소스를 통합할 수 있는 솔루션을 선택하세요. 이상적으로, 이 솔루션은 생성형 AI를 통해 맞춤형 데이터 통합을 생성하고 검증할 수 있어 진화하는 기술 스택에 보조를 맞추는 데 필요한 수동 작업을 크게 줄일 수 있습니다. 이 프로세스가 대부분 수작업으로 진행된다면 문서화가 강력할까요? 기존 통합은 독점적인가요, 아니면 개방적인가요? 다른 커뮤니티 구성원으로부터 얼마나 쉽게 빌리고 협업할 수 있나요? 통합할 때마다 컨설팅 시간을 소모해야 하나요? 사용자 정의 데이터 통합을 생성하고 검증하는 데 시간이 얼마나 걸리나요? 몇 시간, 며칠, 아니면 생성형 AI를 사용해 단 몇 분 밖에 걸리지 않나요?

elastic

중앙 집중화할 수 있는 데이터의 양을 제한하는 기술 또는 라이선싱 문제가 있는가?	레거시 SIEM의 한계로 인해 데이터 수집 및 분석이 방해되어 가시성이 떨어지고 SecOps 워크플로우가 느려질 수 있습니다. 기술적 복잡성이 첫 번째 원인입니다. 모든 쿼리에 대해 데이터를 다시 정규화해야 하는 솔루션은 본질적으로 비효율적입니다. 마찬가지로, 레거시 SIEM은 수집 및 분석의 확장성이 좋지 않은 것으로 악명이 높으며 데이터 급증과 대용량 소스로 인해 이러한 문제가 더욱 복잡해집니다. 유연하지 않은 가격 책정(예: 디바이스별, 사용자별, 바이트별)은 위험 프로필, 경영진의 우선순위, 규정 준수 요구사항에 관계없이 모든 고객을 동일한 경직된 틀에 가두어 SOC의 유연성을 제한합니다. 보안 팀은 과도한 복잡성, 인위적인 라이선싱 제한 또는 기타 장애물 없이 모든 데이터를 신속하게 분석할 수 있어야 합니다.
실행 가능한 데이터를 얼마나 오랫동안 보관해야 하는가?	위협이 오래 지속될수록 위험은 증가하며, 위협이 초기 공격의 기록보다 더 오래 지속될 수 있다면 진입 지점을 봉쇄하고 거점을 제거하기 위해 엄청나게 오랜 추측을 통한 작업이 필요하게 됩니다. 안타깝게도, 저장 공간 비용으로 인해 많은 조직에서 데이터를 조기에 폐기하게 됩니다. 일부 SIEM을 사용하면 자주 액세스하지 않는 데이터를 플랫폼 외부 아카이브로 이동하여 고객이 저장 공간 비용을 줄일 수 있습니다. 이러한 옵션 중 가장 고급 옵션인 Elastic의 프로즌 티어를 사용하면 모든 데이터에 대해 직접적이고 원활한 쿼리가 가능합니다. 그러나 대부분의 SIEM은 대량 데이터 리하이드레이션이 필요하고 기본적으로 아카이브를 검색할 수 없어 분석이 몇 시간씩 지연되고 비용이 증가합니다. 규정 준수뿐만 아니라 보안을 강화하려면 검색할 수 없는 아카이브에 안주하지 마세요. SIEM의 데이터 관리 옵션을 통해 SOC 팀은 다음을 수행할 수 있어야 합니다. • 데이터 백홀로 인한 지연 및 비용 없이 클라우드와 지리적 위치에 저장된 로그의 상관 관계 분석 • 계층화된 SOC의 요구 사항을 충족하도록 데이터 보존, 성능 및 비용 최적화 • 몇 분 만에 수년간의 아카이브를 검색하여 숨어 있는 위협과 새로운 익스플로잇 발견

방어

상상할 수 있는 모든 보안 운영 사용 사례를 해결하세요.

주요 고려 사항	SIEM 지침
시그니처리스 공격을 어떻게 차단하는가?	고급 분석은 엔터티 분석, 머신 러닝(ML), 행동 분석 및 통계 분석과 같은 시그니처리스 기술을 통해 알려지지 않은 위협을 발견하여 충실도 높은 경보를 보완합니다. 이러한 접근 방식은 기존 방법에 비해 다음과 같은 주요 이점을 제공합니다. • 방대한 양의 데이터를 분석하여 기존 방법으로는 간과할 수 있는 악성 활동을 찾아내어 탐지 정확도를 높입니다. • 실무자가 보안 사고의 발생 가능성과 영향을 줄이기 위한 사전 조치를 취할 수 있도록 지원하여 위협을 완화합니다. • 분석가가 중대한 위협보다 앞서 나갈 수 있도록 데이터 엔지니어링 및 위협 우선순위 지정을 자동화하여 팀 효율성을 향상합니다. SIEM의 사용자 및 엔터티 행동 분석(UEBA) 기능을 평가하려면 다음을 고려하세요. • SIEM에서 데이터를 별도의 UEBA 저장소에 복제할 필요가 없는지 확인하여 계획되지 않은 비용을 방지합니다. • 대부분의 보안 팀에는 데이터 과학자가 없기 때문에 SIEM은 일반적인 사용 사례에 대해 프로덕션에 즉시 사용 가능한 ML 작업과 맞춤형 ML 작업을 생성하기 위한 직관적인 도구를 제공해야 합니다. • 최적의 성능을 위해 솔루션은 지도 및 비지도 ML을 모두 제공해야 합니다. • 분석가는 탭을 계속 전환하지 않고도 인사이트에 쉽게 액세스할 수 있어야 합니다. • 솔루션은 쉽게 설명할 수 있는 실행 가능한 인사이트를 제시해야 합니다. 데이터 시각화도 고려해보세요. 기본을 넘어서, 데이터를 탐색할 수 있는 직관적인 인터페이스를 제공하고 관련 인사이트, 지침 및 컨텍스트가 담긴 SIEM을 추진하세요. 또한 데이터 상호 연관성, 시스템 명령 및 프로세스 보기, 클라우드 상태 검사 등의 전문화된 시각화도 찾아보세요.
위협 탐지를 어떻게 자동화할 계획인가? (다음 페이지)	정교한 캠페인이 점점 더 흔해지고 있으며, 상품 공격도 증가하고 있습니다. 안타깝게도 기존의 시그니처 기반 탐지 방법은 위협을 놓치거나 오탐을 발생시키거나 중단되는 경향이 있습니다. SIEM에는 보안 전문가가 만들고 유지 관리하는 현장 테스트를 거친 강력한 탐지 규칙 라이브러리가 함께 제공되어 공격자의 도구, 전술 및 절차를 찾아내야 합니다. 이러한 규칙은 고객이 자동화된 위협 탐지를 효율적으로 구현하고 강화하는 데 도움이 됩니다. 위험 기반 경보 우선 순위 지정은 분석가가 가장 우려되는 위협에 집중하여 경보 피로(35% 보안 팀의 가장 큰 과제)를 줄이고 자동화를 가능하게 하는 데 도움이 됩니다.

elastic

위협 탐지를 어떻게 자동화할 계획인가?	아직 일반화되지는 않았지만, 생성형 AI는 이미 경보 분류에 혁명을 일으키기 시작했습니다. AI를 통해 대규모 경보 세트를 전체적으로 평가할 수 있는 솔루션을 찾아보세요. 일련의 일회성 이벤트가 아닌 다른 의심스러운 활동의 맥락에서 경보를 분석함으로써 AI 기반 경보 분류는 공격자의 체류 시간과 관련 위험을 줄입니다. 전략적인 방식으로 탐지를 자동화하면 위험과 알림 피로를 줄일 수 있으므로 사전 구축된 탐지를 MITRE ATT&CK® 프레임워크에 맞게 조정하는 SIEM을 선택하세요. 이 솔루션은 탐지 엔지니어가 새로운 규칙을 구현하기 전에 테스트하고 자동화된 레드팀 구성을 용이하게 하는 데 도움이 됩니다. 처음 사용하는 동안과 그 이후에도 정기적으로 규칙 성능을 모니터링하고 규칙 예외를 업데이트할 사람을 지정해야 합니다.
위협 헌팅 관행이 있는가?	사일로화된 데이터와 느린 쿼리가 위협 헌터를 지연시켜서는 안 됩니다. 모든 데이터를 빠르게 분석하고 즉시 피벗할 수 있는 SIEM을 선택하세요. 사전 구축된 ML 작업에서 생성된 증거 기반 가설을 사용하여 헌팅을 시작하세요. 사전 구축된 조사 쿼리, 호스트 검사 기능 및 기타 기능도 헌터를 지원해야 합니다. 상황별 위협 인텔리전스와 AI에서 생성된 인사이트를 통해 분석을 더욱 가속화하세요.
예방, 탐지, 검사, 대응 기능이 모든 호스트 시스템에 배포되어 있는가?	소수의 퍼스트 파티 SIEM 에이전트는 데이터 수집을 넘어 다음과 같은 엔드포인트 보안 기능을 제공합니다. • 랜섬웨어 및 Malware로부터 엔드포인트 보호 • 가상 머신, 컨테이너, 서버리스 워크로드와 같은 클라우드 기반 리소스를 위협으로부터 보호 • 호스트 내 분석으로 위협 탐지 • Osquery로 시스템 검사 • 엔드포인트 기반 대응 조치 호출
규정 준수 요구 사항은 무엇인가?	조직에 적용되는 규제 및 규정 준수 프레임워크와 표준을 준수하면 불필요한 벌금, 가동 중단 시간, 평판 훼손을 방지하는 데 도움이 됩니다. 귀하의 환경에서 규정 준수 관련 기술에 대한 데이터 통합을 제공하는 SIEM을 찾아보세요. 이 솔루션은 개방형 스키마 및 AI 지원을 통해 맞춤형 통합 개발을 가속화해야 합니다. 규정 준수 보고는 말 그대로 어제 오늘의 일이 아니므로 실시간 규정 준수 모니터링과 사전 예방적 시행의 길을 모색하세요. 이러한 변화를 지원하려면 위반 사항에 대해 경보를 보내고 자율적이거나 분석가가 호출한 조치로 대응할 수 있는 SIEM을 선택하세요. 규정 준수 이해관계자에게 알리려면 유연하고 직관적인 시각화 및 구축 도구를 찾으세요. POS 단말기나 개발 서버와 같은 중요한 시스템이 규정 준수 범위의 일부인 경우, 파일 무결성 모니터링(FIM), Malware 탐지 및 관련 엔드포인트 보안 기능에 대한 요구 사항을 고려하세요. 마지막으로, 선택한 SIEM이 특정 보안 및 규정 준수 요구 사항을 충족하는지 확인하세요.

elastic

SIEM 성공 체크리스트

각 고객마다 고유한 요구 사항과 우선 순위가 있겠지만, 수많은 성공적인 SIEM 프로젝트에서 얻은 이러한 요구 사항부터 시작하는 것이 좋습니다.

데이터 수집 및 정규화

- 이 솔루션을 사용하면 클라우드 인프라 및 애플리케이션, 호스트, 네트워크 장치, 사용자, IoT 및 OT 등을 포함한 모든 보안 관련 데이터 소스에서 수집할 수 있습니다.
- 이 솔루션은 수많은 데이터 소스와의 사전 구축된 통합을 제공하고 정기적으로 새로운 통합을 출시합니다.
- 이 솔루션은 오픈 소스 스키마를 사용하여 데이터를 정규화합니다.
- 이 솔루션은 데이터를 실행 가능한 형태로 효율적으로 보관하여 수년간의 아카이브에 걸쳐 위협 헌팅, 사고 조사 및 규정 준수를 지원합니다.

탐지 및 예방

- 이 솔루션은 다양한 자동 탐지 방법을 제공하고 사전 구축된 강력한 규칙 세트를 제공합니다.
- 이 솔루션은 고급 분석을 통해 숨겨진 위협을 찾아냅니다.
- 사전 구축된 분석은 폐쇄형 블랙박스가 아닌 개방형이며 고객 환경에 맞게 조정할 수 있습니다.
- 이 솔루션은 빠른 실시간 및 기록 분석을 제공합니다.
- 고객은 특정 환경과 사용 사례에 맞게 탐지를 쉽게 사용자 정의하고 생성할 수 있습니다.
- 이 솔루션은 탐지 기술을 MITRE ATT&CK에 매핑합니다.
- 이 솔루션은 예방 기능을 적용하여 명확하게 식별된 위협을 제거하고 분석가의 업무량을 최소화합니다.

elastic

조사, 헌팅, 대응

이 솔루션은 관련 인사이트, 지침 및 컨텍스트를 표시하여 조사 및 대응을 신속하게 처리합니다.

이 솔루션을 통해 분석가는 거의 실시간으로 데이터를 검색할 수 있습니다.

이 솔루션을 사용하면 임시 호스트 및 클라우드 워크로드 검사가 가능합니다.

분석가는 효율성을 크게 저하시키지 않고 수년간의 데이터를 검색할 수 있습니다.

이 솔루션은 협업, 증거 수집, 기록 보관을 용이하게 하는 사례 관리 기능을 제공합니다.

이 솔루션은 분석가가 트리거하는 자율적인 대응 조치를 지원합니다.

이 솔루션은 핵심 SOAR 기능을 제공하고 서드파티 시스템과 통합하여 조직 간 워크플로우를 간소화합니다.

배포 아키텍처

이 솔루션은 온프레미스, 클라우드, 하이브리드 및 멀티 클라우드 아키텍처에서의 배포를 지원합니다.

이 솔루션을 통해 보안팀은 통합 가시성을 유지하면서 데이터 레지던시 요건을 충족할 수 있습니다.

세분화된 역할 기반 액세스 제어(RBAC)는 위험을 줄이고, 규정 준수를 지원하며, 조직 간 협업을 촉진합니다.

이 솔루션은 단일 관리 계층을 통해 여러 테넌트(예: 조직의 사업 부문, 지역)를 지원합니다.

이 솔루션은 실행 가능한 데이터의 효율적인 장기 저장을 지원하는 데이터 관리 기능을 제공합니다.

elastic

Elastic Security로 미래의 SOC를 구축하세요

Elastic Search AI 플랫폼 기반

AI 기반 보안 분석은 SIEM의 미래입니다.

사각 지대 제거

- 사전 구축된 통합으로 데이터를 수집하고 AI를 통해 몇 분 만에 맞춤형 커넥터를 구축하세요.
- 즉시 검색 가능한 수년간의 아카이브를 효율적으로 보관하세요.
- 백홀에 따른 비용과 복잡성 없이 데이터가 있는 곳에서 데이터를 분석하세요.
- 인프라(온프레미스, 하이브리드, 멀티 클라우드, SaaS)를 선택하고 필요에 따라 조정하세요.

방어 강화

- Elastic Security Labs의 연구 기반 탐지 규칙을 활용하세요.
- 탐지 규칙과 데이터 쿼리를 AI로 변환하여 SIEM 마이그레이션을 쉽게 하세요.
- 턴키 ML로 주요 사용 사례를 해결하고 맞춤형 ML로 새로운 사용 사례를 해결하세요.
- 헌터에게 사용자 및 엔터티 위험 점수를 제공합니다.
- 기본 및 서드파티 엔드포인트와 클라우드 보안으로 보호를 확장하세요.

SecOps 워크플로우 가속화

- Attack Discovery를 통해 경보를 전체적으로 분석하고 분석가를 안내하세요.
- AI 지원 및 전문가가 작성한 조사 가이드를 통해 분석가의 역량을 강화하세요.
- 선택한 LLM을 활용하여 비공개 컨텍스트에서 AI를 기반으로 작업하세요.
- 보안, 옵저버빌리티, 검색을 위한 단일 플랫폼으로 운영을 단순화하세요.

elastic