ManageEngine
ADSolutions

Cloud Security Plus

Amazon AWS, Microsoft Azure, 그리고 Salesforce 를 위한 정교한 로그 관리 프로그램

목 차

- Cloud Security Plus 는 어떤 기능을 가지고 있는가?
- Cloud Security Plus 는 어떤 로그를 수집하는가?
- 어떻게 동작하는가?
- 사용 예
- 라이선스 종류

Cloud Security Plus 는 무엇을 제공하는가?

다양한 클라우드 환경의 데이터를 분석하는 정교한 로그 관리 시스템

- Amazon Web Services (AWS)
- Microsoft Azure
- Salesforce

Cloud Security Plus 는 어떤 기능을 가지고 있는가?

- 내재된 종합 보고서
  - 사용자 활동
  - IAM (Identity and Access Management)관리 액션
  - 보안 그룹(권한 변경 보고서)
  - 네트워크 보안 보고서
    - VPC 활동 (Virtual Private Cloud) 보고서
    - DNS 보고서
  - Storage 보고서
    - Traffic 보고서
    - 관리 활동 보고서
  - Load Balancer 보고서
  - Relational Database 관리 액션

Amazon Web Services (AWS)

- AWS CloudTrail AWS 계정 사용자의 모든 활동을 감사 추적하는 기능을 제공합니다. Cloud Security plus for AWS 의 CloudTrail 데이터 분석 기능을 이용하면, 실시간으로 보안 그룹 변경, 무단 사용자 접속, Admin 권한 변경과 같은 중요 보안 관련 이벤트를 실시간으로 감시할 수 있습니다.

- Amazon S3, EC2, Route 53, Elastic IP, Elastic Network Interfaces, WAF, RDS, STS, VPC, ELB, 와 Auto Scaling 에서 발생하는 이벤트에 대한 상세한 정보를 제공합니다.

- **로그 Source** - *CloudTrail logs, S3 server access logs, and ELB access logs*

AWS

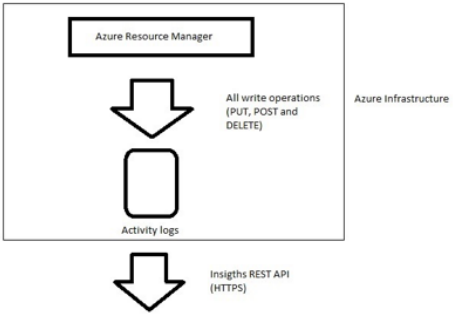
ManageEngine

Azure

- The Azure Activity Log 는 Azure에서 발생하는 subscription-level 이벤트에 대한 심층적인 로그를 분석을 제공합니다. Activity Log를 이용하면, 사용자가 가입한 모든 자원에서 수행되는 모든 write 동작(PUT, POST, DELETE)에 대해 누가, 언제, 무엇을 했는지를 파악합니다. 또한 오퍼레이션 상태와 관련된 속성을 파악할 수 있습니다.

- **로그 Source** - *Activity log*

Azure


Azure Resource Manager
All write operations
(PUT, POST and
DELETE)
Azure Infrastructure
Activity logs
Insigths REST API
(HTTPS)
ManageEngine
Cloud Security Plus

Salesforce

- 이벤트 모니터링은 Salesforce 가 사용자의 데이터를 안전하게 보호하는 여러 도구들 중의 하나입니다. 가입자 기업의 사용자 활동을 자세하게 파악할 수 있습니다. 이들 사용자의 활동을 이벤트라고 칭합니다. 사용자의 개별 이벤트를 보거나, 이벤트의 추세를 추적하다가 이상한 이벤트가 발생하면 신속히 식별하여, 기업의 데이터를 보호합니다. 추적이 되는 이벤트는 다음과 같습니다:
  - Logins, Logouts
  - URI (web clicks in Salesforce Classic)
  - Lightning (web clicks, performance, and errors in Lightning Experience and the Salesforce mobile app)
  - Visual force page loads, Apex executions
  - Report exports

- **로그 Source** - *Salesforce Event Monitoring*

CloudSecurity Plus의 자동화 기능과 장점

- 내장된 각종 보고서
- 정교한 검색 제공
- 주요 이벤트 실시간 경보

Use cases 1: AWS

EC2 Instance 상태 변경

Denial of service, botnets, malware, ransomware 및 기타 유형의 외부 공격이 널리 알려져 있지만, 다른 위협한 사이버 보안 위협은 종종 무시됩니다. 그것은 조직 내부에서 오는 위협으로, 악의적이고 부주의 한 내부자에서 발생하는 위협입니다.

내부자 위협은 회복하기가 어려우며 처음에는 탐지하기가 더 어려울 수 있습니다. Amazon EC2 (Elastic Compute Cloud)는 클라우드에서 확장 가능한 컴퓨팅 용량을 제공합니다. 이 서비스를 사용할 때는 클라우드 인프라에 대한 침입 시도 또는 다른 무단 작업이 있는지 모니터하는 것이 좋습니다.

HSBC에서 발생한 한 시나리오에서, Falcini라는 직원은 높은 액세스 권한을 취득하여, EC2 인스턴스를 시작했습니다. 긴급 상황 발생시 Amazon Elastic Compute Cloud를 신속하게 가동할 수 있습니다. 이 상황에서 그는 Compute Cloud의 백업을 수행하고 해당 인스턴스를 중지했습니다. 인스턴스 시작 또는 중지 활동을 모니터링하는 것이 중요합니다.

Cloud Security Plus 는 이 상황을 어떻게 돕는가?

Cloud Security Plus의 최근 EC2 인스턴스 상태 변경 보고서는 시작 또는 중지를 포함한 모든 인스턴스 변경 사항을 보고하며, 관리자에게 즉시 경고할 수 있습니다.

Use cases 2:

AWS S3 트래픽 분석 보고서

비즈니스 연속성을 고려할 때, 가장 먼저 떠오르는 것은 재해 복구입니다. 비즈니스에 대한 악의적인 공격, 직원에 의한 인적 오류 또는 지역 클라우드 중단 사고와 같은 재난이 발생했을 때, 이를 즉시에 대응하려면 필요에 따라 바로 검색할 수 있는 미션 크리티컬 한 데이터를 별도로 백업하는 것이 중요합니다. Amazon S3에서 신속한 파일 백업을 위해, S3의 트래픽 분석이 매우 중요합니다. Amazon S3 스토리지가 삭제되거나 업데이트되면 어떻게 될까요?

Cloud Security Plus 는 이 상황을 어떻게 돕는가?

CloudSecurity Plus의 'S3 버킷 활동 보고서'는 S3 버킷 액티비티의 실패, 삭제 및 업데이트를 추적하고 정보를 지속적으로 제공합니다. 이 외에도 S3 트래픽 분석 보고서는 모든 s3 액세스 요구에 대한 현황을 제공합니다.

Use cases 3:

Azure – 네트워크 보안 그룹의 규칙 변경

네트워크 보안 그룹을 사용하여 Azure 가상 네트워크에서 Azure 리소스와의 네트워크 트래픽을 필터링할 수 있으므로 인바운드 네트워크 트래픽을 허용 또는 거부하거나 아웃 바운드 네트워크 트래픽을 허용 또는 거부하는 보안 규칙을 변경하면, 조직에 심각한 영향을 미칩니다. Network Security Group에서 변경 한 내용은 즉시 서브넷의 모든 VM에 적용됩니다. 따라서 네트워크 보안 그룹의 규칙 변경 또는 권한 변경을 추적하는 것이 매우 중요합니다.

Cloud Security Plus 는 이 상황을 어떻게 돕는가?

이 시나리오에서 CloudSecurity Plus는 어떻게 도움이 됩니까? 네트워크 보안 규칙 변경, 권한 변경, 서브넷 변경 등에 대한 기본 보고서를 제공합니다.

Use cases 4:

Salesforce – 최신 보고서 가져오기

Salesforce가 가장 널리 사용되는 CRM 이며, 이 클라우드 소프트웨어를 감사하면 잠재적 또는 실제 보안 문제를 진단하는 데 도움이 됩니다. 로그인 활동과는 별도로, 내보내는 보고서에 대한 감사는 시장에서 꼭 필요한 기능입니다. 특정 사용자의 보고서 또는 최근 보고서 내보내기 목록을 내 보낸 사용자를 파악하는 것이 필요합니다. 한 개인의 중요한 데이터를 포함할 수 있는 빈번한 보고서 송출은 악의적인 공격을 유발할 수 있습니다.

Cloud Security Plus 는 이 상황을 어떻게 돕는가?

CloudSecurity Plus를 사용하면 모든 Salesforce 관리자가 보고서 송출에 대한 사용자의 최근 활동을 추적하여, 필요한 경우 적절한 조치를 취할 수 있습니다.

라이선스 정책

- 라이선스 가격은 기본적으로 로그가 수집되는 클라우드 계정의 수에 따라 다릅니다.
- AWS 환경에서는 add-on (Log management of AWS S3 buckets) 제품이 별도로 라이선스 됩니다.

감사합니다

텔리맨트 주식회사
https://www.tmn.co.kr
02) 588-7350

기술 질문: inforeq@tmn.co.kr
견적 요청: sales-info@tmn.co.kr