



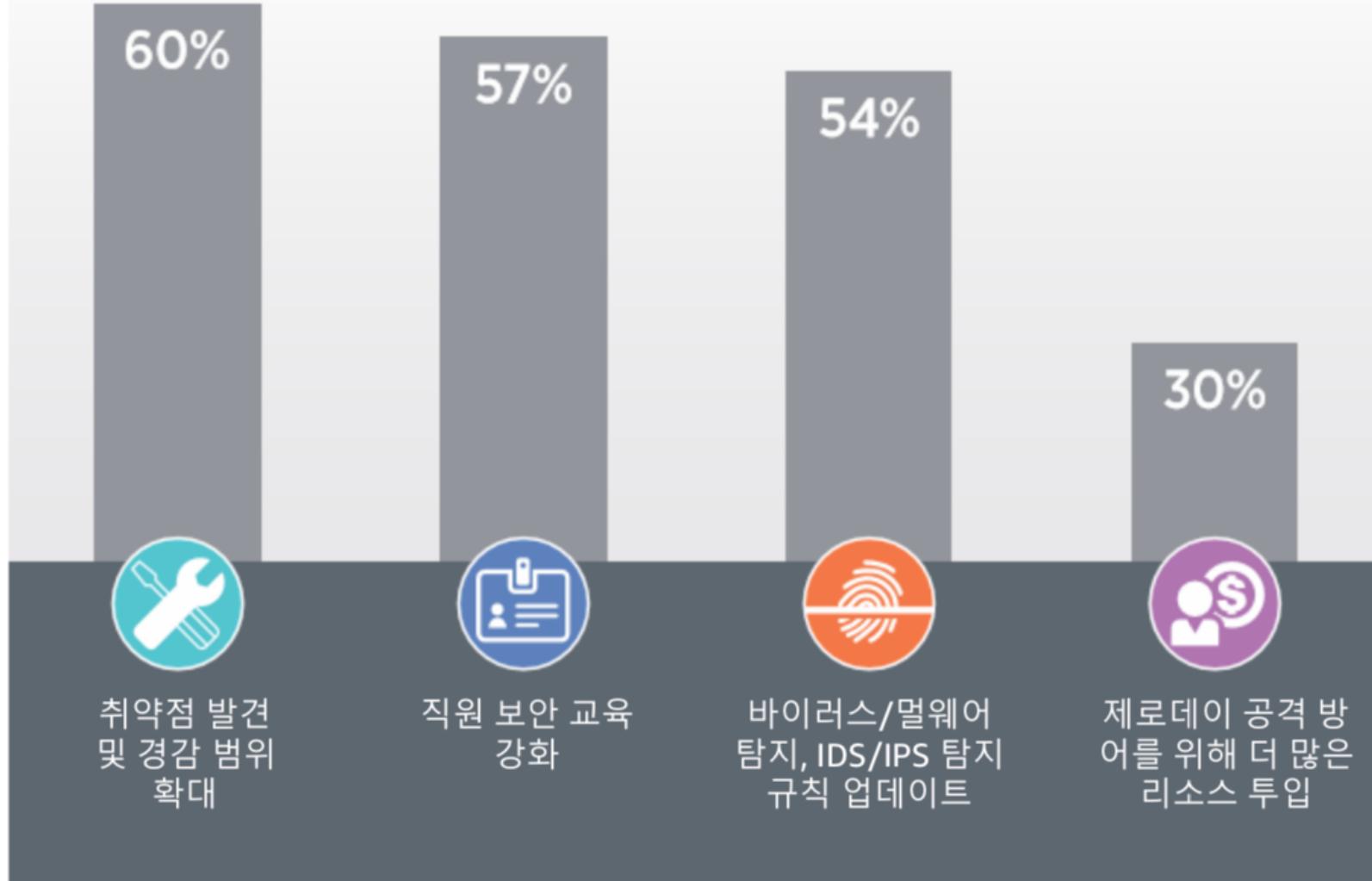
AWSKRUG 강남 모임

2018/08/08

Amazon GuardDuty



보안 이슈 발생시, 취하는 대응 방안들



Amazon GuardDuty 는 취약점 발견과 경감 조치, 위협 탐지와 예방 측면에서 보안 인력들이 취할 수 있는 대응방식을 강화시켜줍니다.

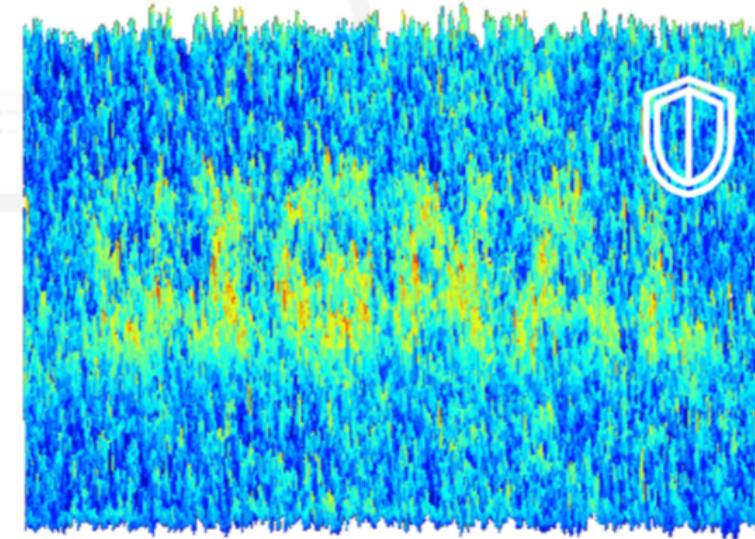
Source: 2017 Forbes Insights – "Enterprises Reengineer Security in the Age of Digital Transformation"

건초더미에서 바늘 찾기



GuardDuty는 보안 인력들이 방대한 양의 로그 데이터 속에서 신속하게 위협을 탐지할 수 있도록 도와줍니다. 이를 통해, AWS환경에 대한 악의적이거나 의심스러운 행동들에 대해 신속하게 대응하고 보안을 향상시킬 수 있게 해줍니다.

Amazon GuardDuty: All Signal, No Noise



GuardDuty 위협 탐지 및 통지 서비스

위협 탐지 유형들

정찰

인스턴스 침해

계정 침해

Data Sources



VPC flow logs



DNS Logs



CloudTrail Events

Findings

HIGH

MEDIUM

LOW

대응

탐지

통보

Amazon GuardDuty: 특장점

- 관리형 위협 탐지 서비스
- 아키텍쳐 변경이나 성능 저하 없이 손쉽게 원클릭 활성화
- AWS 어카운트 및 리소스에 대한 상시 모니터링
- EC2 및 IAM에 관련된 위협 발견
- No Agents, no Sensors, no Network Appliances
- 글로벌 커버리지, 리전 기반 적용
- 머신러닝 기반 이상 행동 탐지 기능 탑재
- 추가적인 보호 기능을 위한 파트너 연계
- 간단하고 효과적인 가격 체계



Launch

현재 14개 리전 지원!

- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)
- EU (Ireland)
- EU (Frankfurt)
- EU (London)
- Canada (Central)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Seoul)
- Asia Pacific (Tokyo)
- Asia Pacific (Mumbai)
- South America (Sao Paulo)

GuardDuty 멀티 어카운트 지원

- 멤버 어카운트의 추가는 콘솔 혹은 API를 활용.
- 멤버쉽 초청을 보낸 어카운트가 Master 어카운트가 되고, 승인하면 멤버로 조인됨.



GuardDuty 위협 탐지 유형들

정찰

인스턴스 대사과정:

- Port Probe/Accepted Comm
- Port Scan (intra-VPC)
- Brute Force Attack (IP)
- Drop Point (IP)
- Tor Communications

어카운트 대사과정:

- Tor API Call (failed)

인스턴스 침해

- C&C Activity
- Malicious Domain Request
- EC2 on Threat List
- Drop Point IP
- Malicious Comms (ASIS)
- Bitcoin Mining
- Outbound DDoS
- Spambot Activity
- Outbound SSH Brute Force
- [Unusual Network Port](#)
- [Unusual Traffic Volume/Direction](#)
- [Unusual DNS Requests](#)
- [Domain Generated Algorithms](#)

어카운트 침해

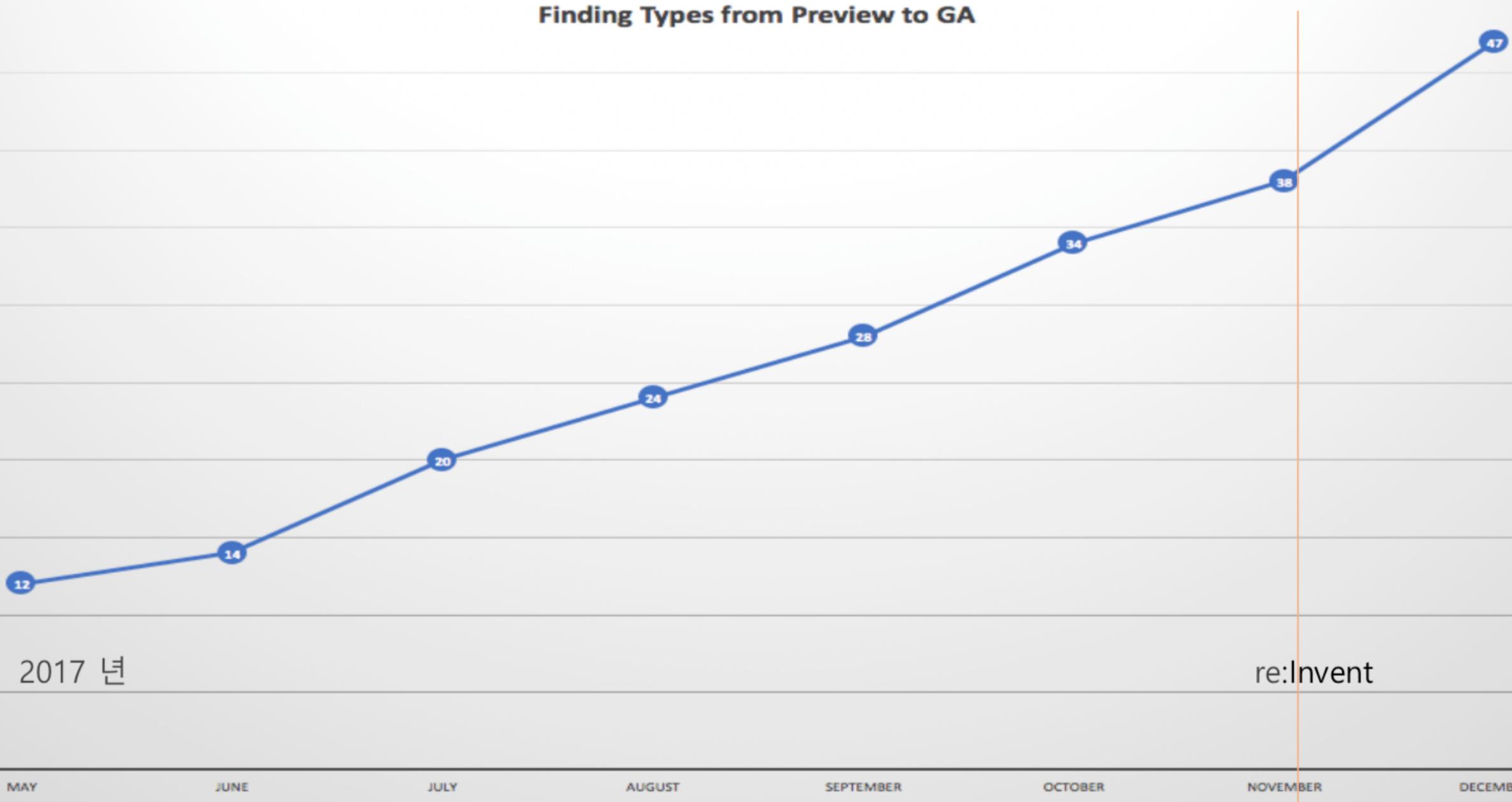
- Malicious API Call (bad IP)
- Tor API Call (accepted)
- CloudTrail Disabled
- Password Policy Change
- [Instance Launch Unusual](#)
- [Region Activity Unusual](#)
- [Suspicious Console Login](#)
- [Unusual ISP Caller](#)
- [Mutating API Calls \(create, update, delete\)](#)
- [High Volume of Describe calls](#)
- [Unusual IAM User Added](#)

 시그니쳐 기반 상태 비유지 탐지 내역

 상태유지 행위 기반 탐지 및 비정상 행동 분석

지속적인 탐지 케이스 향상

Finding Types from Preview to GA



GuardDuty 지원 데이터 소스

VPC Flow Logs



VPC flow logs

- VPC Flow Logs 분석. Flow Logs에 대한 별도의 활성화 작업은 필요 없음. 로그데이터에 대한 수집은 독립적인 복제 스트림을 통해 수행됨.
- 별도 SIEM 분석환경이 있는 경우, 기존 대로 VPC Flow Logs를 활성화하여 이용할 것을 권장.

DNS Logs



DNS Logs

- EC2인스턴스가 알려진 타겟 도메인으로 접근했던 DNS 로그 분석.
- Route 53 query log를 포함한 DNS 로그 정보. DNS 기반 분석을 위해 Route 53이 반드시 필요한 것은 아님.

CloudTrail Events



CloudTrail Events

- 관리 콘솔, SDK, CLI 등을 통해 발생된 AWS API호출을 기록한 CloudTrail history 분석.
- API호출에 이용된 소스 IP주소를 포함해서 사용자와 어카운트에 대한 식별.

목록: 신뢰 및 위협 IP 목록

GuardDuty는 다음 지능형 피드 정보를 활용하고 있습니다. :

- CrowdStrike
- Proofpoint

커스텀 신뢰IP 목록과 알려진 위협 목록을 통해 Finding의 기능을 확장할 수 있습니다.

- 해당 인프라 혹은 어플리케이션과의 안전한 통신을 할 수 있는 신뢰된 IP목록을 탐지 예외처리(Whitelisting, 오탐 방지).
- 알려진 악성 IP주소들에 대한 위협 목록. GuardDuty는 위협 목록을 기반으로 finding을 생성.

Hard Limits: 어카운트 당 **1개의 신뢰 목록** 과 **6개의 위협 목록**까지 관리 가능

신뢰 IP 목록



고객 및 파트너 제공 알려진 위협 목록

GuardDuty 탐지 내역: Console / API

AWS 관리 콘솔

EC2 Instance [Close](#)

i-e2f5f524
performing outbound port scans.

Recon:EC2/Portscan [Q](#) [Q](#)

Actions [▼](#)

This finding was:

⚠ EC2 Instance i-e2f5f524 is performing outbound port scans against remote host 10.0.0.158.

Severity	Region	Count
Medium Q Q	us-west-2	1

Account ID [Q](#) [Q](#)
1851063622...
[Q](#) [Q](#)

Last seen
2017-11-01 15:53:28 (an hour ago)

Resource Affected [▼](#)

Resource role	Resource type
ACTOR	Instance Q Q

Instance ID [Q](#) [Q](#)
i-e2f5f524
[Q](#) [Q](#)

Image ID
ami-494e7279
[Q](#) [Q](#)

Tags
Name: tester
Inspector: Enabled

Private IP address
10.0.1.224
[Q](#) [Q](#)

Subnet ID
subnet-d44ca8bc
[Q](#) [Q](#)

Private dns name
ip-10-0-1-224.us-west-2....
[Q](#) [Q](#)

VPC ID
vpc-de4ca8b6 [Q](#) [Q](#)

위협정보의 신속한 확인:

- 심각도
- 리전
- 횟수/빈도
- 위협 유형
- 대상 리소스
- 소스 정보
- Viewable via CloudWatch Events

API / JSON 포맷

추가 분석을 위해 Finding Data를 Export:

```
  "type": "Recon:EC2/Portscan",
  "resource": {
    "resourceType": "Instance",
    "instanceDetails": {
      "imageId": "ami-494e7279",
      "instanceId": "i-e2f5f524",
      ...
    },
    "service": {
      "serviceName": "guardduty",
      "detectorId": "6caf9da84f873e4"
    },
    "action": {
      "actionType": "NETWORK_CONNECTION",
      "networkConnectionAction": {
        "connectionDirection": "OUTBOUND",
        "remoteIpDetails": {
          "ipAddressV4": "10.0.0.1"
        }
      }
    }
  },
  "resourceRole": "ACTOR",
  "additionalInfo": {
    "portsScannedSample": [
      146,
      83,
      110,
      ...
    ],
    "eventFirstSeen": "2017-11-01T22:52:36Z",
    "eventLastSeen": "2017-11-01T22:53:28Z",
    ...
  },
  "severity": 5,
  "createdAt": "2017-11-01T23:00:10.179Z",
  "updatedAt": "2017-11-01T23:00:10.179Z",
  "title": "EC2 Instance i-e2f5f524 performing outbound port scans.",
  "description": "EC2 Instance i-e2f5f524 is performing outbound port scans aga...
```

GuardDuty 탐지 내역: Severity Levels

LOW

- 의심스럽거나 악의적인 행위가 리소스를 탈취하기 전에 차단됨.
- Severity : 0.1 ~ 3.9 범위

대처 방안:

- 즉각 대응할 필요는 없음. 향후 정보 차원의 활용 용도

MEDIUM

- 평상시 행동 패턴과 다른 의심스러운 행위 탐지.
- Severity : 4.0 ~ 6.9

대처 방안:

- 추가 조사 필요
- 리소스의 행위를 변화시킨 신규 설치 소프트웨어가 있는지 확인
 - 설정 내역의 변경 확인
 - 리소스에 대한 AV 스캐닝 수행 (허락되지 않은 소프트웨어 탐지)
 - IAM 주체에 부여된 권한 확인

HIGH

- 리소스가 이미 탈취되어 허락되지 않은 행동을 수행하고 있음.
- Severity : 7.0 ~ 10.0

대처방안:

- 즉각적인 대처 필요
- 인스턴스 터미네이트
 - IAM access key 교체

탐지 내역 처리: 자동화

- 탈취된 인스턴스에 대한 처리
- 유출된 AWS 자격증명에 대한 처리

- Lambda Function 이용:
 - 현재 Security Group에서 제외하고 양방향 통신을 차단
 - EBS volume(s)에 대한 스냅샷
 - 보안팀에 경보

자동 대응



GuardDuty 가격 체계*

	N. Virginia Ohio Oregon	Mumbai Ireland London N. California	Canada Central Frankfurt Seoul Singapore Sydney	Tokyo	Sao Paulo
VPC Flow Log and DNS Log Analysis (GB당)					
First 500 GB / month	\$1.00	\$1.10	\$1.15	\$1.18	\$1.75
Next 2000 GB / month	\$0.50	\$0.55	\$0.58	\$0.59	\$0.88
Over 2500 GB / month	\$0.25	\$0.28	\$0.29	\$0.29	\$0.44
AWS CloudTrail Event Analysis					
Per 1,000,000 events / month	\$4.00	\$4.40	\$4.60	\$4.72	\$7.00

Free Trial: Any new account to Amazon GuardDuty can try the service **for 30-days at no cost**. Provides access to the full feature set and detections during the free trial. GuardDuty will display the volume of logs processed and estimated daily average service charges to provide a tailored price estimate for GuardDuty to protect all AWS accounts.

Amazon GuardDuty 고객



Goldman
Sachs



COMCAST



FINRA

NETFLIX



AUTODESK®



twilio



Blackboard®



ATLASSIAN



mapbox



WEBROOT®



INSTRUCTURE

GuardDuty 파트너



splunk>



proofpoint.

Deloitte.

RAPID7

accenture

+ sumologic

RedLock

Trustwave®



IBM



Find All GuardDuty Partners At: aws.amazon.com/guardduty/partners



네트워크 보안



Virtual Private Cloud

가상 사설 네트워크



Web Application F/W

악성 웹 트래픽 필터링

NEW!



WAF Managed Rule Sets

WAF 파트너 룰셋



Shield

디도스 방어



Certificate Manager

SSL/TSL 인증서 발급 및 관리

NEW!



지능형 위협탐지

계정 및 권한 관리



IAM

사용자 접근관리 및 키 암호화



SAML Federation

온프레미스 사용자 저장소와 SAML 2.0연계



NEW!



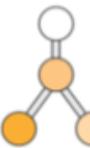
AWS SSO

콘솔 및 앱에 대한 SSO 및 권한 관리



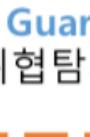
Directory Service

MS Active Directory에 대한 관리형 서비스



Organizations

복수개의 어카운트에 대한 중앙 관리



지능형 위협탐지

데이터 보안



Key Management Service

암호화 키 생성 관리



CloudHSM

하드웨어 기반 키 저장소



Server-Side Encryption

유연한 데이터 암호화 옵션



Inspector

어플리케이션 취약점 분석



Amazon Macie

지능형 데이터 방지



컴플라이언스

Service Catalog

표준 카탈로그 생성 관리



Config

리소스 인벤토리 변경 추적



CloudTrail

사용자 및 API 사용 추적



CloudWatch

리소스 및 어플리케이션 모니터링



Artifact

AWS 컴플라이언스 리포트 셀프서비스

