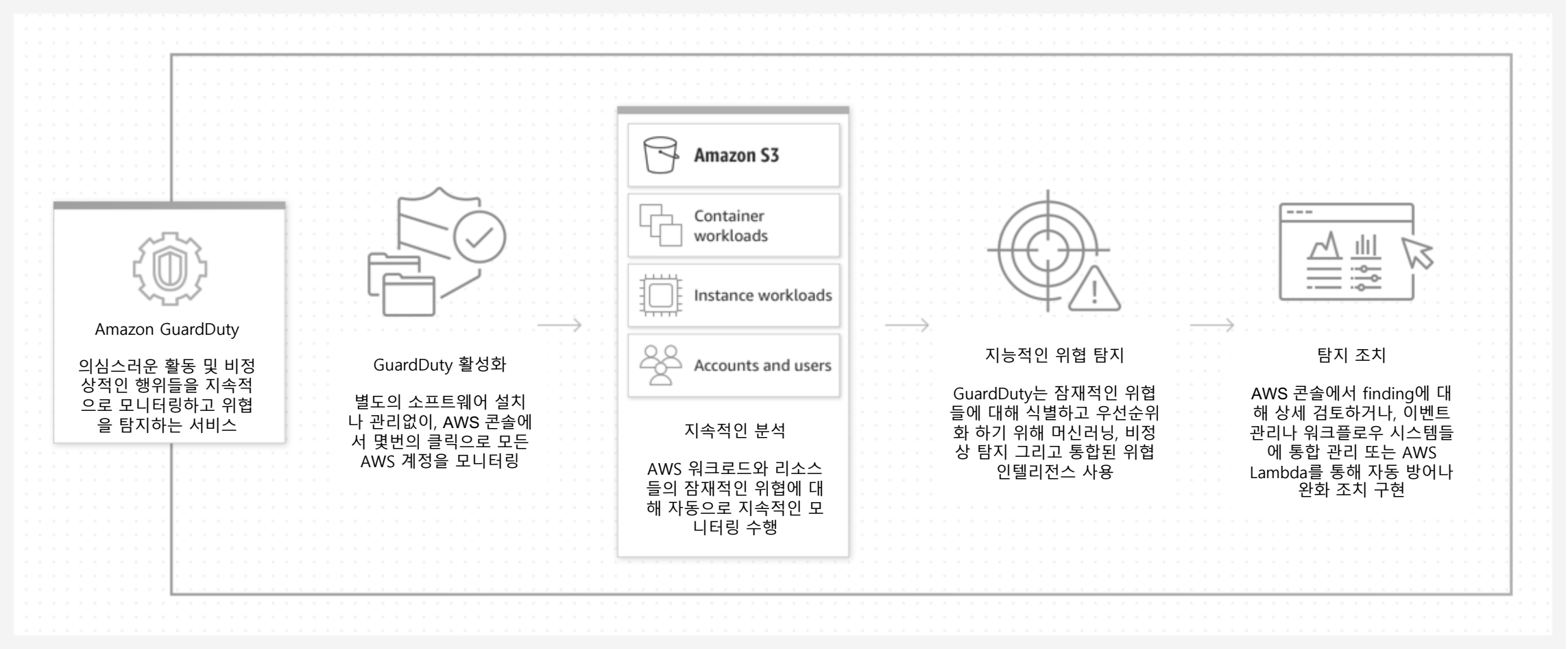
aws Professional Services

Amazon GuardDuty

박병화 (bhpark@amazon.com)
Sr. Security Consultant
AWS Proserve Korea

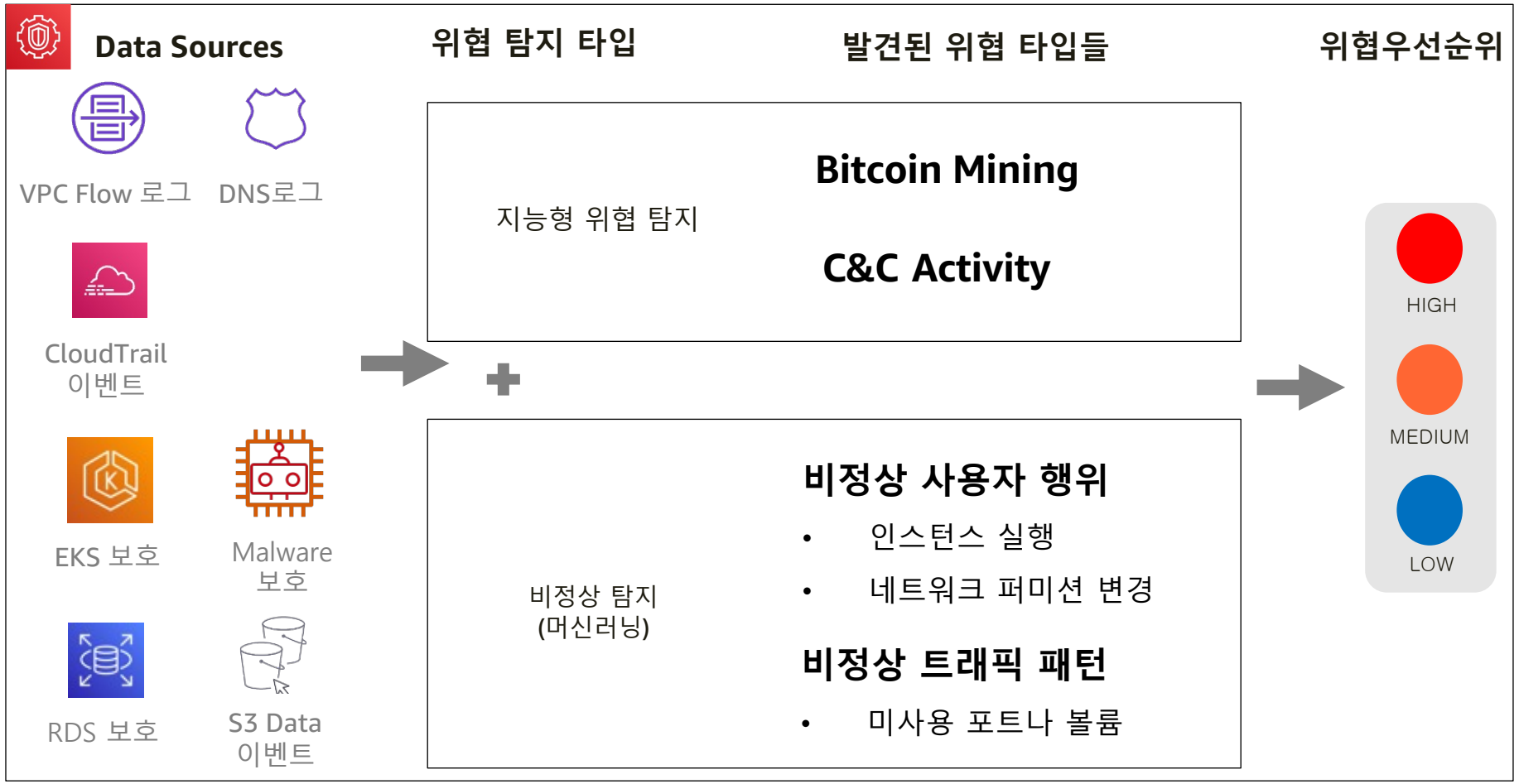
GuardDuty

- AWS 계정, 인스턴스, 컨테이너 워크로드, 사용자, 데이터베이스 및 스토리지에서 잠재적 위협 요소를 지속적으로 모니터링 제공
- 이상 탐지, 기계 학습, 행위 모델링 및 AWS와 글로벌 리딩 서드 파티의 위협 인텔리전스 피드를 사용하여 위협을 빠르게 찾아내며, 자동 대응을 시작하여 위협을 조기 완화



GuardDuty 동작 방식

- AWS 계정과 EC2 워크로드를 보호하기 위한 지능형 위협 탐지 및 지속적인 모니터링 서비스를 기계 학습기반으로 제공
- Organization하의 모든 계정의 Data Sources에 대해 서비스 영향 없이 로그 분석을 통해 위협에 대해 탐지하여 우선순위로 구분



Amazon Detective

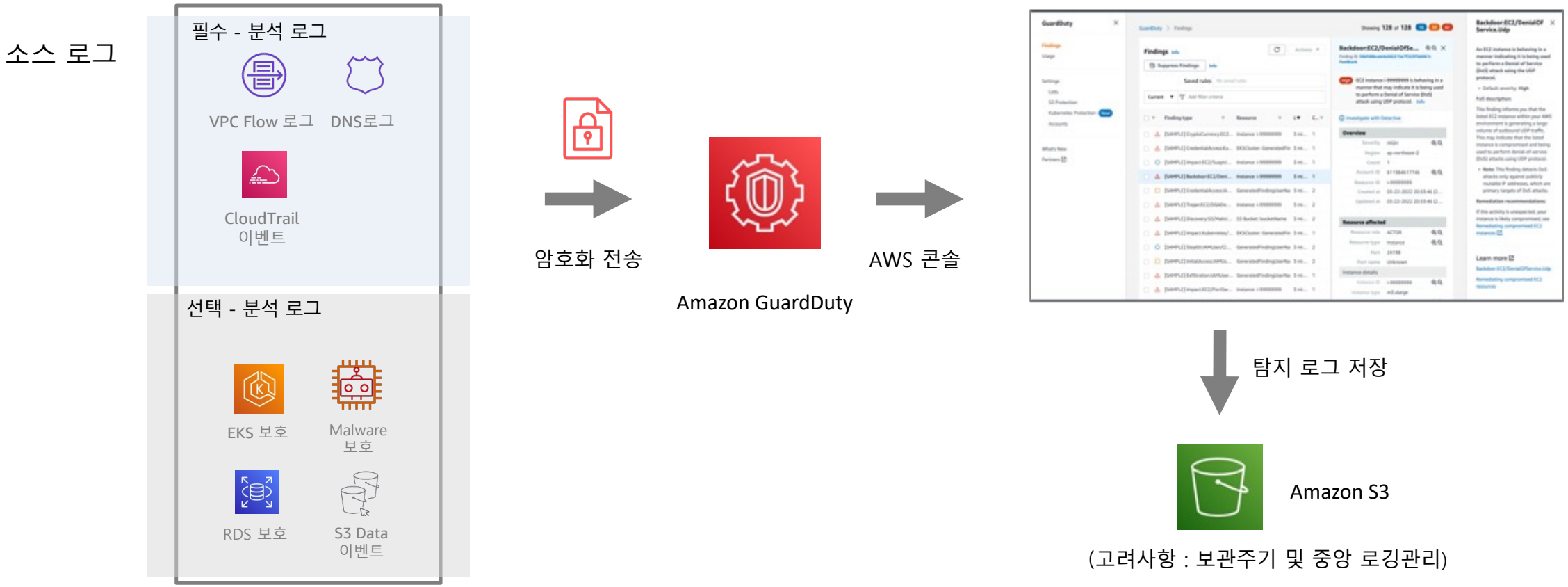
AWS Security Hub

Amazon CloudWatch

- 경고
- 완화조치
- 파트너 솔루션과 연동
- SIEM으로 전송

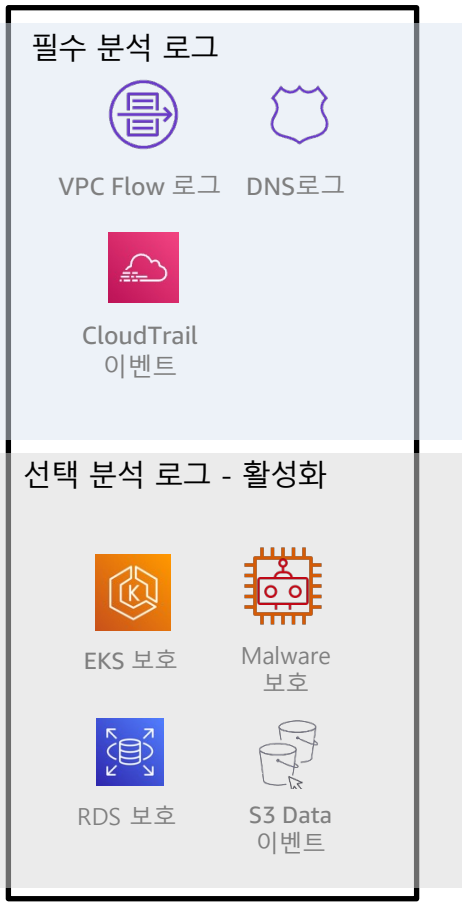
GuardDuty 동작 방식

- GuardDuty는 아래 데이터 소스들의 데이터를 분석하고 처리하며, 기본 데이터 원본을 사용하여 IAM 액세스 키 및 S3 버킷과 같은 AWS 리소스 유형과 관련된 이상을 감지
- 아래 소스 로그에서 GuardDuty로 전송하는 동안, 모든 로그 데이터는 암호화 처리 전송
- 학습을 위한 프로파일링, 비정상 탐지를 위한 로그로부터 추출된 다양한 데이터들은 분석 이후 폐기
- 계정 및 워크로드 성격에 따라 분석 소스 로그에 대해 선택 적용 (EKS, Malware, RDS, S3)



GuardDuty 동작 방식 (분석 소스 로그)

- GuardDuty의 분석 소스 로그는 필수와 선택으로 나누어지며, GuardDuty를 활성화시, 필수 로그들은 자동 활성화
- 단위 서비스 계정내의 보호대상 리소스 종류에 따라 선택 분석을 계정레벨에서 활성화



필수(분석 소스 로그)

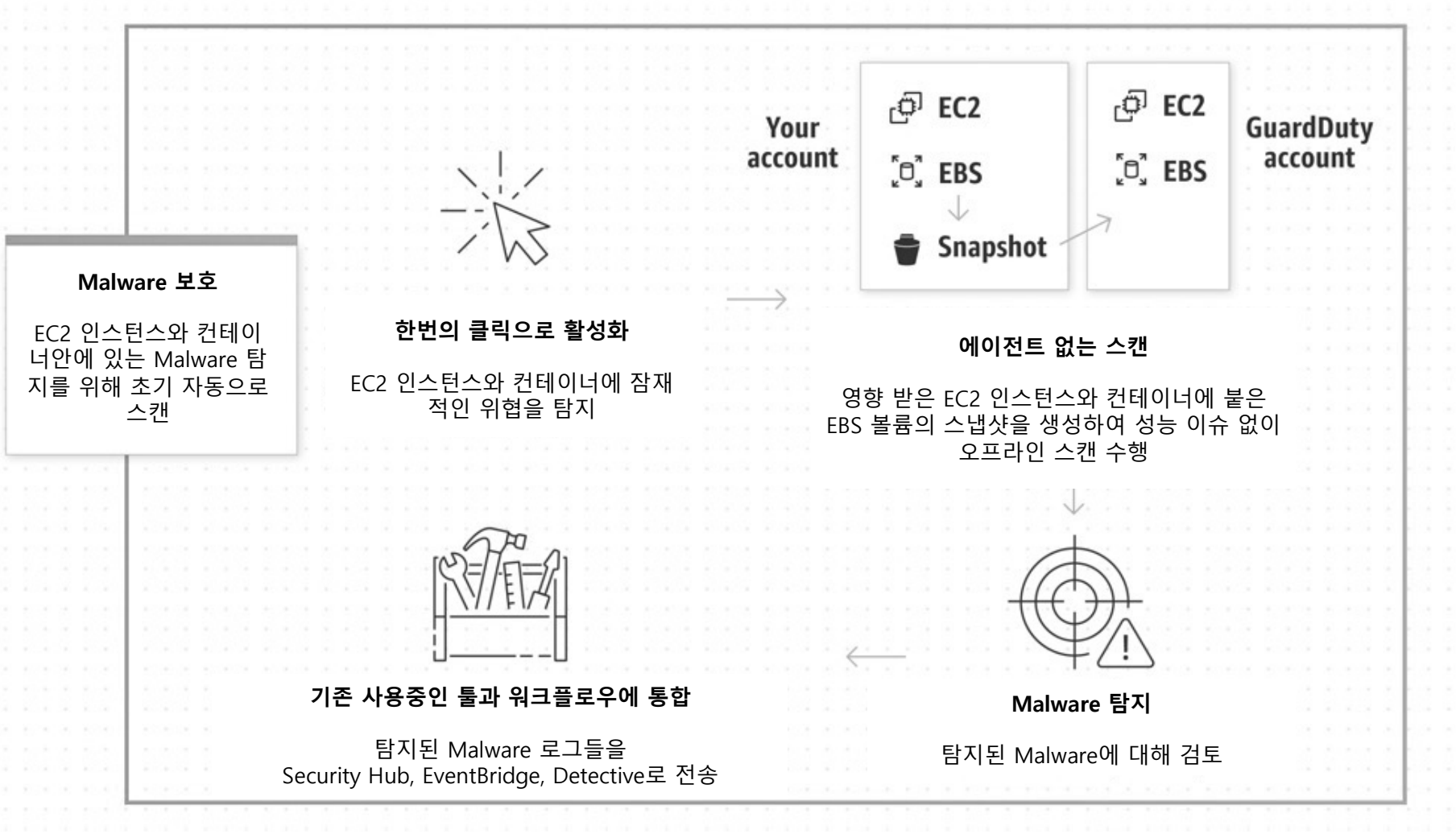
- VPC Flow 로그 : 환경 내 네트워크 인터페이스에서 송수신되는 IP 트래픽에 대한 정보를 캡처
- DNS 로그 : AWS 내부 DNS Resolver를 통해 DNS 요청 및 응답 로그에 액세스하고 처리하며 분석
- CloudTrail 로그 : AWS 관리 콘솔, AWS SDK, CLI 및 특정 AWS 서비스를 사용하여 만든 API 호출을 포함하여 계정에 대한 AWS API 호출 기록 분석

선택(분석 소스 로그)

- EKS 보호 : 사용자, 애플리케이션 및 컨트롤 플레인에서 API 활동을 시간순으로 로그를 수집하여 Kubernetes API에 대한 위협을 탐지
- Malware 보호 : Amazon EC2 인스턴스 또는 컨테이너 워크로드에 연결된 Amazon Elastic Block Store(EBS) 볼륨에서 에이전트없이 스캔을 자동으로 시작하여 맬웨어의 존재 탐지.
- RDS 보호 : Amazon Aurora 데이터베이스(Amazon Aurora MySQL 호환 에디션 및 Aurora PostgreSQL 호환 에디션)에 대한 잠재적 액세스 위협에 대한 RDS 로그인 활동을 분석하고 프로파일링
- S3 Data 이벤트 : S3 보호를 위해 Object 수준의 API 작업을 모니터링하여 S3 버킷 내 데이터에 대한 잠재적인 보안 위험을 식별

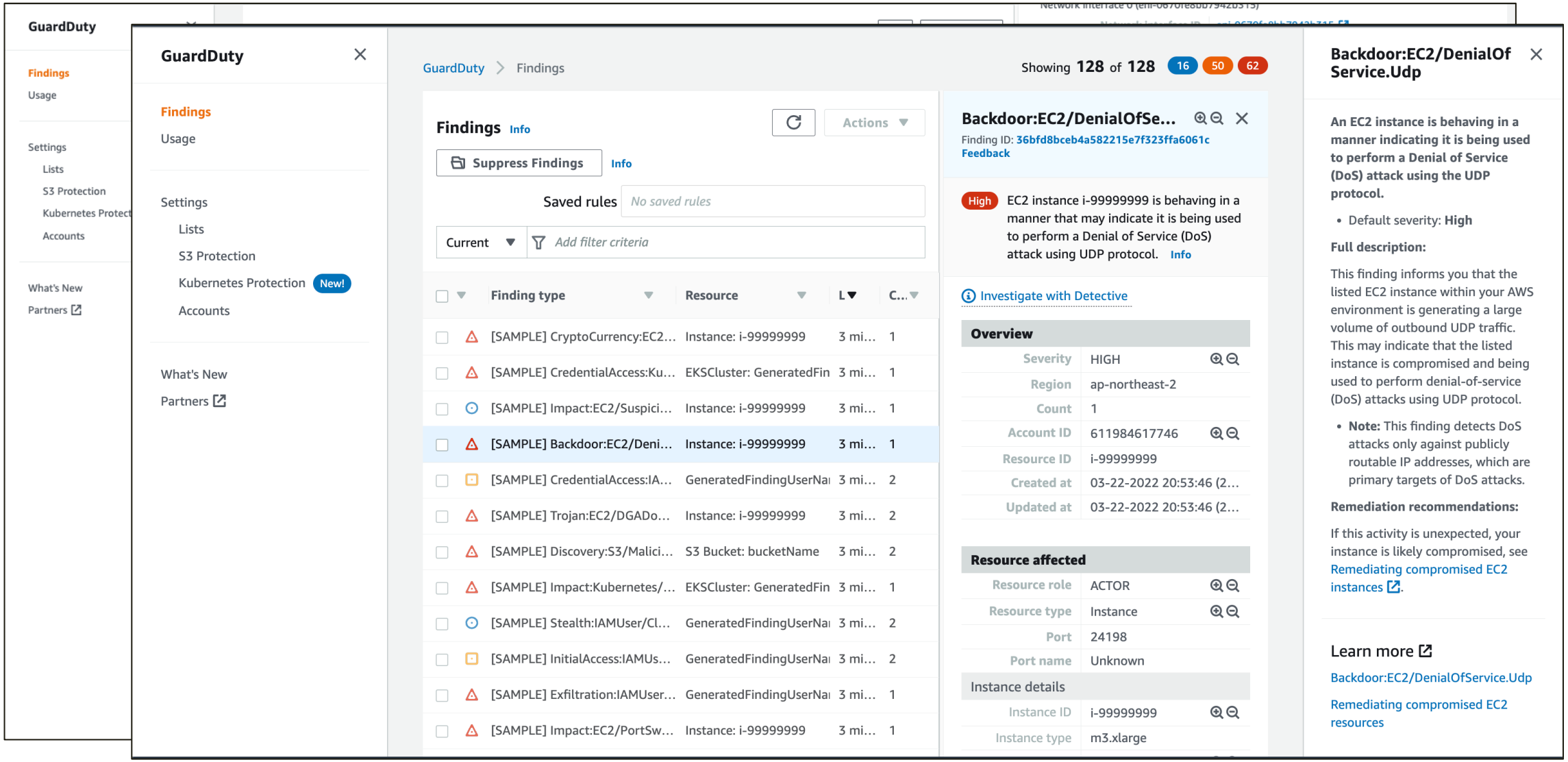
GuardDuty 동작 방식 (분석 소스 로그 : Malware 탐지)

- Amazon EC2 인스턴스 및 컨테이너 워크로드에 연결된 EBS 볼륨에 대해, 스냅샷을 생성하여 성능이슈 없이 오프라인 Malware 스캔 수행



GuardDuty Findings

- Findings과 알림, 그리고 상세 정보와 Detective를 통한 상관관계분석



GuardDuty 동작 방식 (분석 소스 로그 : S3 보호)

- Amazon S3의 데이터에 대한 위협을 사전에 탐지하며, 계정의 모든 버킷에 대해 자동으로 지속적인 업데이트
- S3 데이터 이벤트 모니터링이 활성화되면 GuardDuty는 즉시 모든 S3 버킷의 S3 데이터 이벤트 분석을 시작하고 악의적이고 의심스러운 활동에 대해 모니터링 수행
- 버킷이 Public으로 액세스할 수 있게 되면 경고를 수행하며, S3 데이터 이벤트 모니터링을 기반으로 위협을 감지하면 보안 결과를 생성
- S3 보호를 비활성화하면, GuardDuty는 즉시 이 데이터 원본 사용을 중지하고 S3 버킷에 저장된 데이터에 대한 액세스 모니터링을 중지

정책	의심스러운 접근	비정상적인 행위
• 버킷을 Public으로 생성 • Public 접근 차단 (Block public access) 비활성화 • Logging 비활성화 • Root 자격증명 사용	• 데이터 검색, 유출, 수정 : - 익명의 웹사이트 - 유출된 인스턴스 자격증 - 의심스러운 IP	• 비정상적인 위치(location) • 비정상적인 버킷 • 비정상적인 볼륨 • 비정상적인 오류 볼륨

GuardDuty 동작 방식 (분석 소스 로그 : EKS 보호)

- Amazon EKS 클러스터에서 Kubernetes 데이터 소스를 분석하여, 악의적이고 의심스러운 활동이 있는지 모니터링 수행
- GuardDuty EKS 보호를 비활성화하면, GuardDuty는 즉시 이 데이터 원본 사용을 중지하고 EKS 클러스터 모니터링 중지

정책	의심스러운 접근	의심스러운 행위
• 노출된 대시보드 • 기본 서비스 계정에 대한 관리자 액세스 • 익명 액세스 허용	• 데이터 검색, 유출, 수정 : - 익명의 웹사이트 - 성공한 익명 액세스 - 의심스러운 IP	• Kubernetes 시스템 Pod에서 실행 • 민감한 마운트가 있는 컨테이너 • Privilege 컨테이너

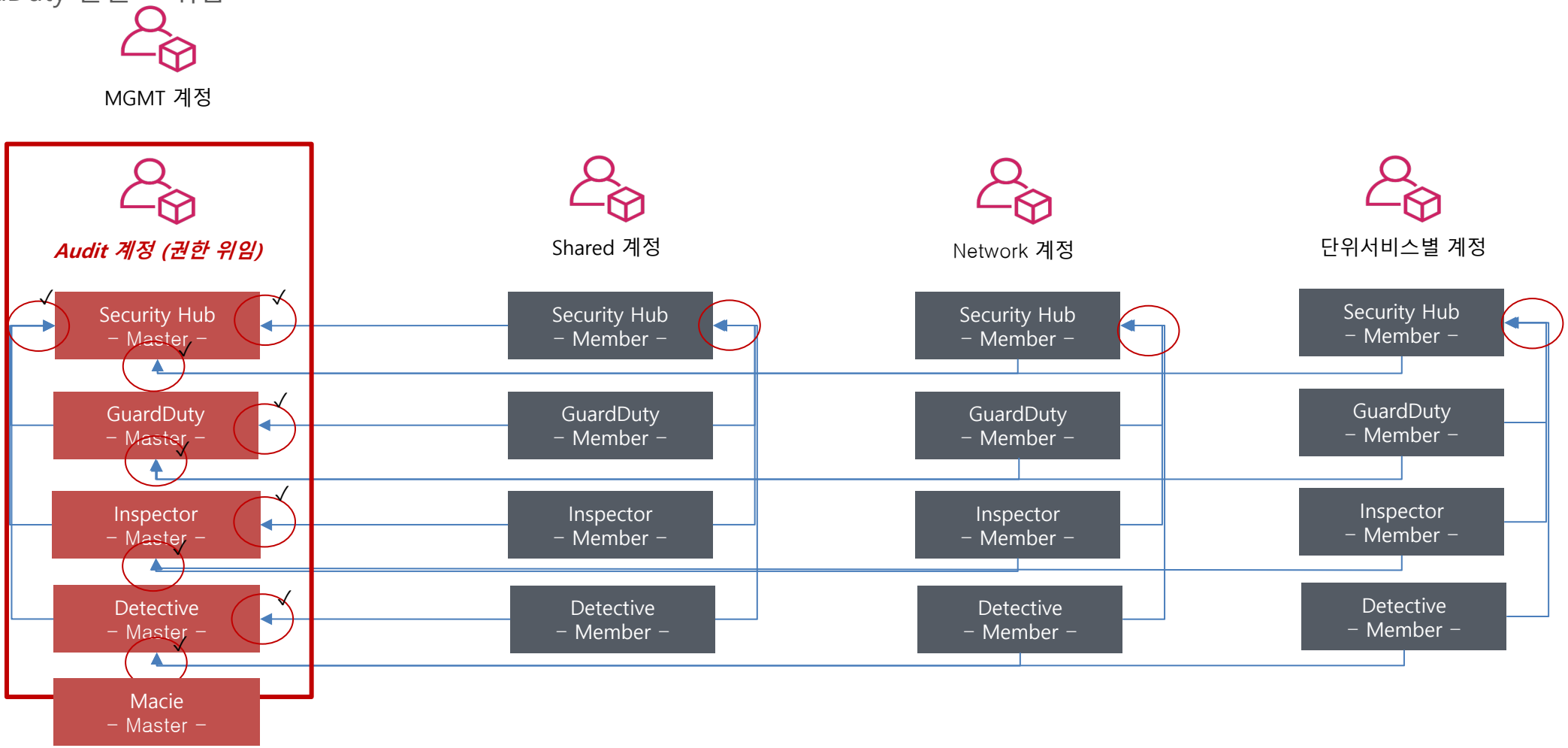
GuardDuty 탐지 위협 종류

- 50여개 이상의 탐지 타입을 제공하며, 지속적으로 업데이트 제공 (AWS 관리형 위협 탐지 서비스)
- https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-active.html

Backdoor Finding Types	Behavior Finding Types	Crypto Currency Finding Types
Policy Finding Types	Privilege Escalation Finding Types	Recon Finding Types
Impact Finding Types	Stealth Finding Types	Trojan Finding Types
Exfiltration Finding Types	DefenseEvasion & InitialAccess Finding Types	Persistence Finding Type
Execution Finding Types	Discovery Finding Types	PenTest Finding Types
Credential Access Finding Types	Unauthorized Access Finding Types	Persistence Finding Types

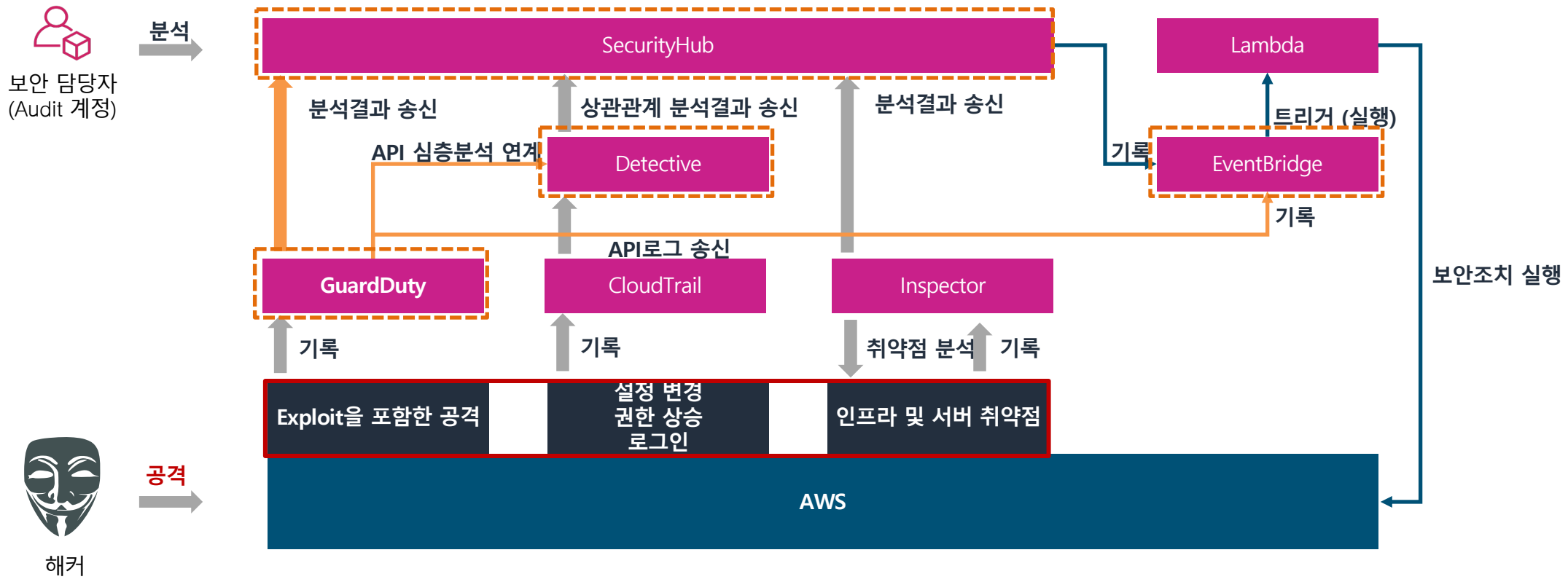
GuardDuty 관리 방식 설계 (위임정책)

- AWS Native 보안 솔루션은 중앙 관리를 위해 Payer(Management)계정에서 Audit 계정으로 권한 위임
- 위임받은 Audit 계정에서는 컨트롤 타워 조직내 모든 계정들에 대해 Master 역할 수행하며, 탐지된 위협들에 대해 Audit 계정의 GuardDuty 콘솔로 취합



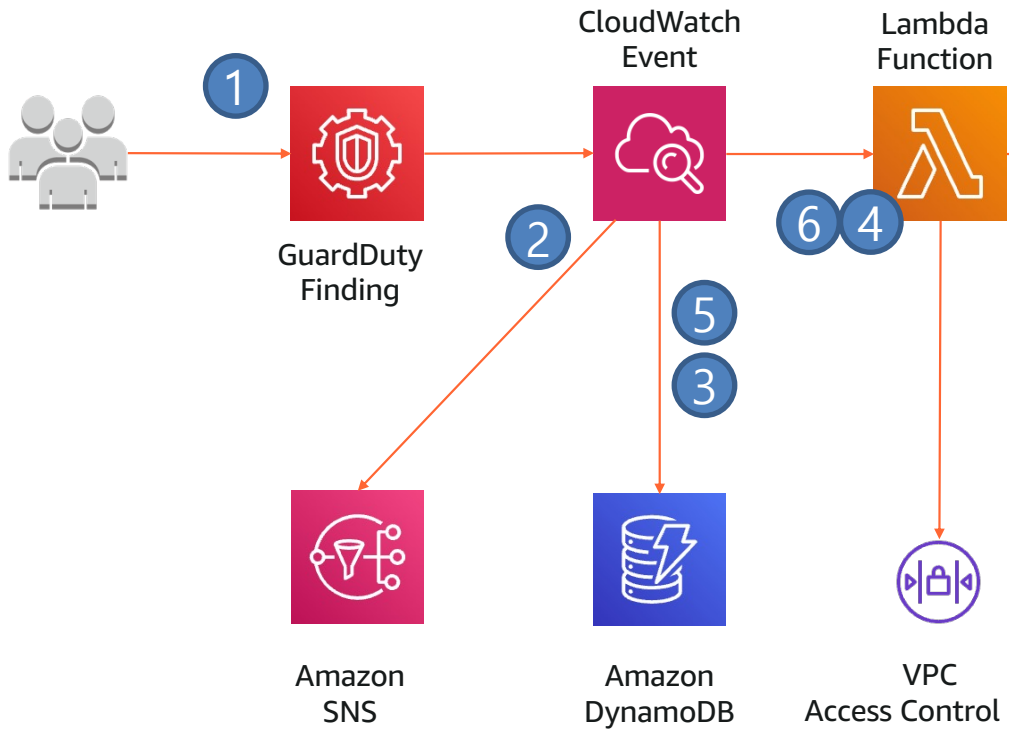
GuardDuty 동작 방식 설계 (연계 : AWS Native 서비스)

- GuardDuty에서 탐지된 위협 상세로그들을 SecurityHub로 전달하여 중앙 집중 로깅 관리 및 3rd Party SEIM과의 통합 고려
- AWS 리소스들과의 연관 관계 및 추적 분석을 위해 Detective와 연동하며, Detective를 통해 API 심층 분석 제공



GuardDuty 동작 방식 설계 (연계 : AWS Native 서비스)

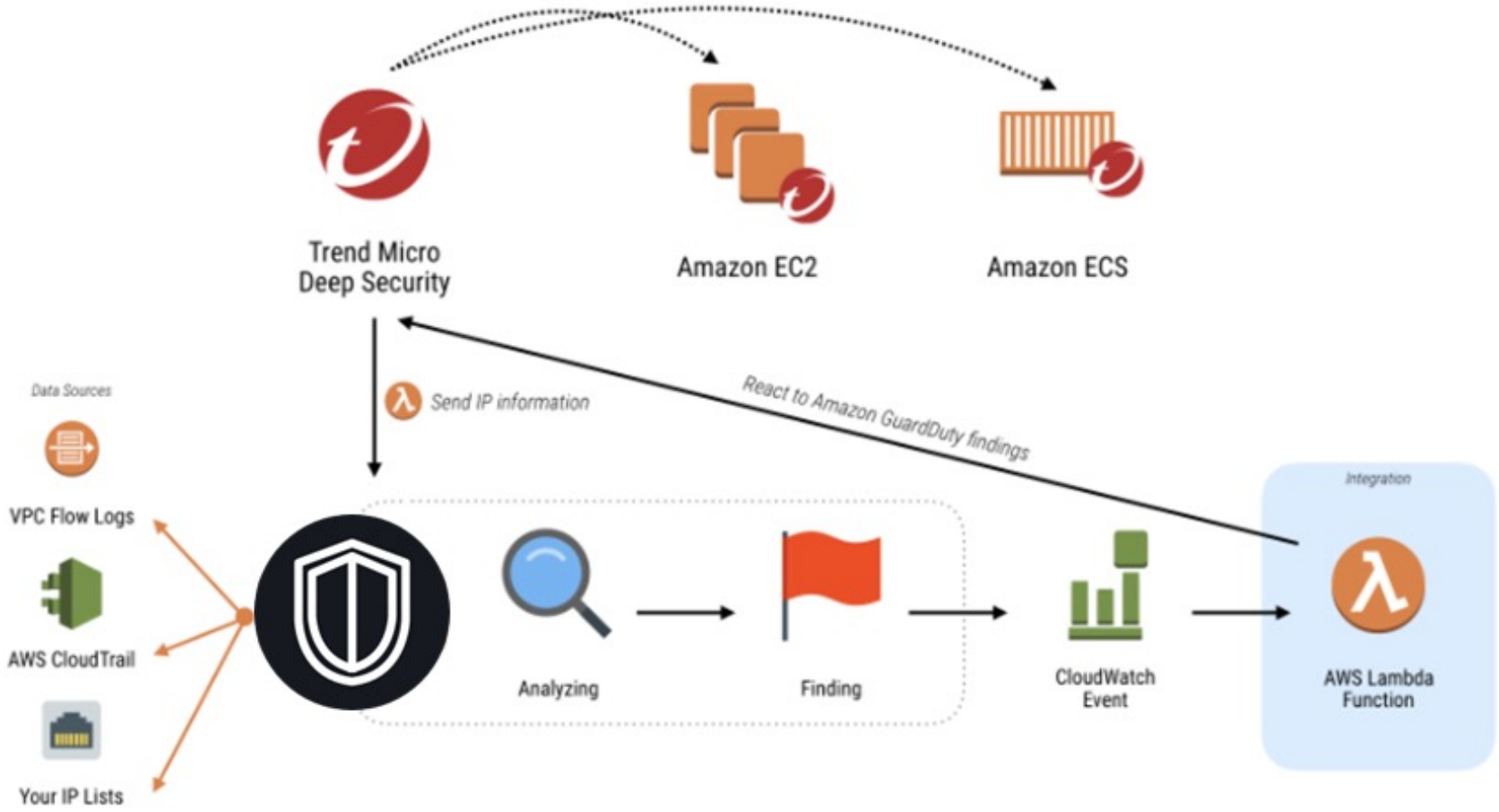
- EventBridge와 연계하여, GuardDuty에서 사전에 정탐으로 정의된 위협이 탐지되면, 자동으로 경감 조치 구현되도록 설계
- GuardDuty에서 정탐으로 정의된 위협의 범위에 대해 사전 정의 필요(Bruteforce 공격 등)
- 해당 위협을 발생시키는 Source IP에 대해 DynamoDB에 저장하고, NACL을 통해 해당 Source IP를 차단 수행 및 담당자에게 alert 전송
- 이후 일정시간(입력한 Retention 시간) 후, 해당 Source IP에 대해 NACL에서 차단 해제하는 자동화 구현



1. GuardDuty에서 위협을 탐지
2. 관련 이벤트를 관리자에게 SNS 전송
3. 공격자 IP 정보, 리전, 시간을 DynamoDB에 저장
4. Lambda 1 – 공격자 IP를 NACL에 Deny 정책으로 추가
5. DynamoDB에 NACL ACL ID 업데이트
6. Lambda 2 – 사전 설정한 Retention 시간(5 ~ 10080)에 해당되는 공격자 IP에 대해 NACL에서 Prune 작업

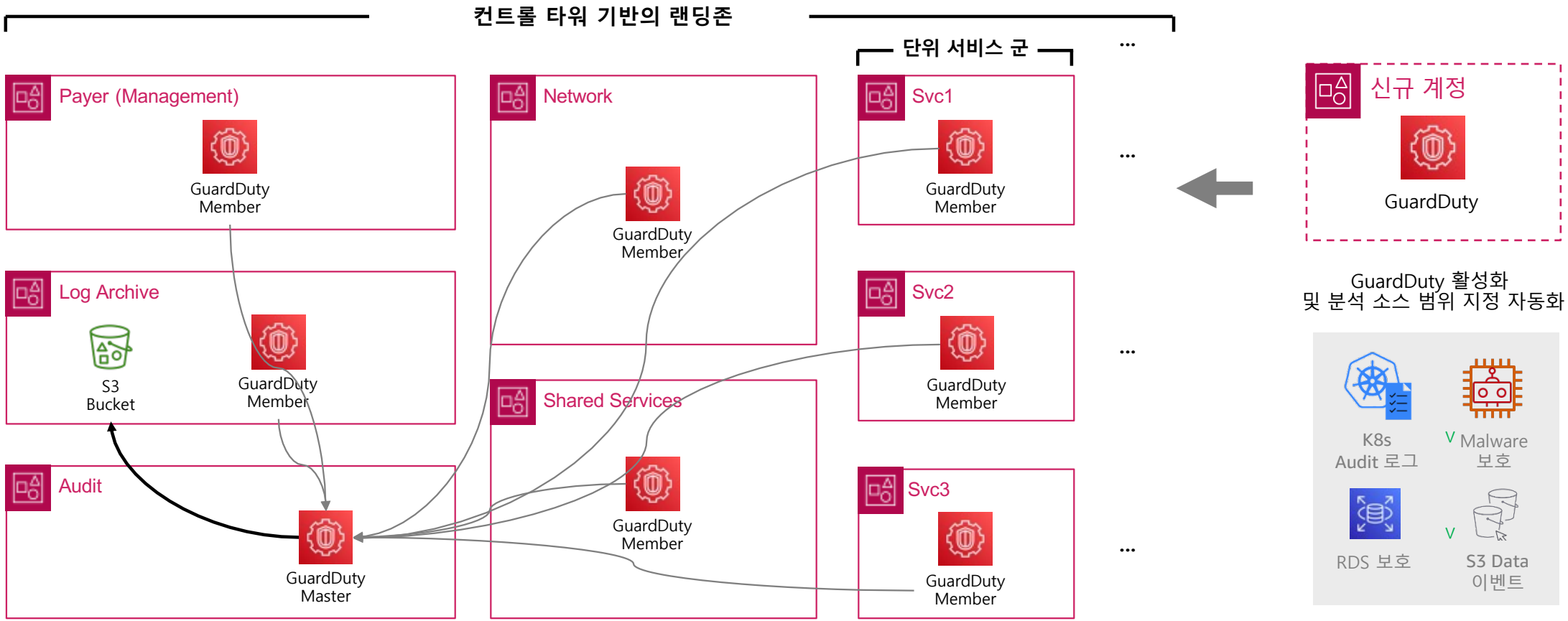
GuardDuty 동작 방식 설계 (연계 : Trend Micro Deep Security)

- AWS Lambda 함수는 Amazon GuardDuty와 Deep Security 간의 공동 워크플로를 생성
- Deep Security는 특정 Recon, UnAuthorizedAccess, CryptoCurrency, Backdoor 및 Trojan 탐지 결과 지원
- GitHub repo (https://github.com/deep-security/amazon-guardduty)



GuardDuty 관리 방식 설계 (로깅 및 신규 계정에 대한 자동화)

- 탐지된 위협 로그들은 중앙로깅 관리를 위해 Log Archive 계정의 S3와 CloudWatch Event로 전송하도록 설계
- 탐지된 위협 로그 업데이트 주기는 15분, 1시간, 6시간(기본값) 지원하며, OpenSearch와의 연동을 위해 최소값(15분)으로 변경
- S3 버킷에 저장된 로그는 보관 주기 정책에 따라 S3 LifeCycle 규칙 적용 (최소 1년 보관)
- Auto-enable GuardDuty를 통해 신규 계정 생성시, GuardDuty 활성화 및 분석 소스 범위 중 필수에 대해 자동 관리되도록 설계 (선택 분석 로그 적용은 개별 계정 리소스 종류에 따라 수동 관리)

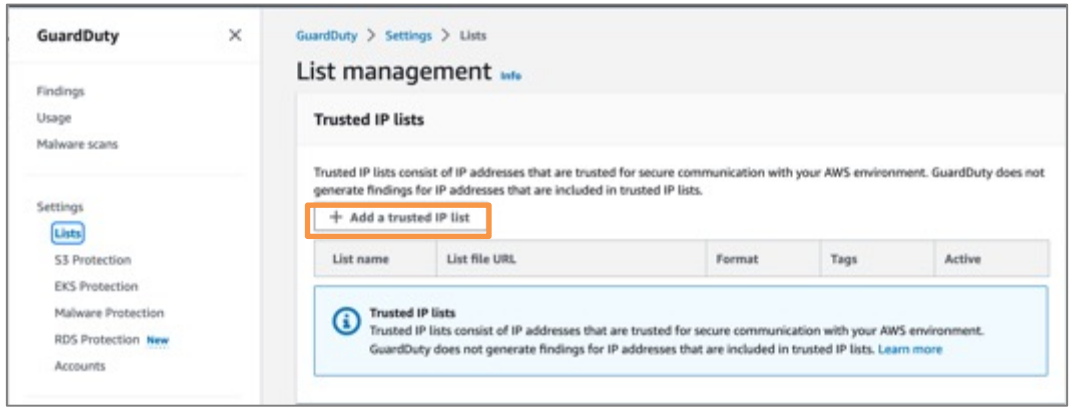


GuardDuty 관리 방식 (예외처리)

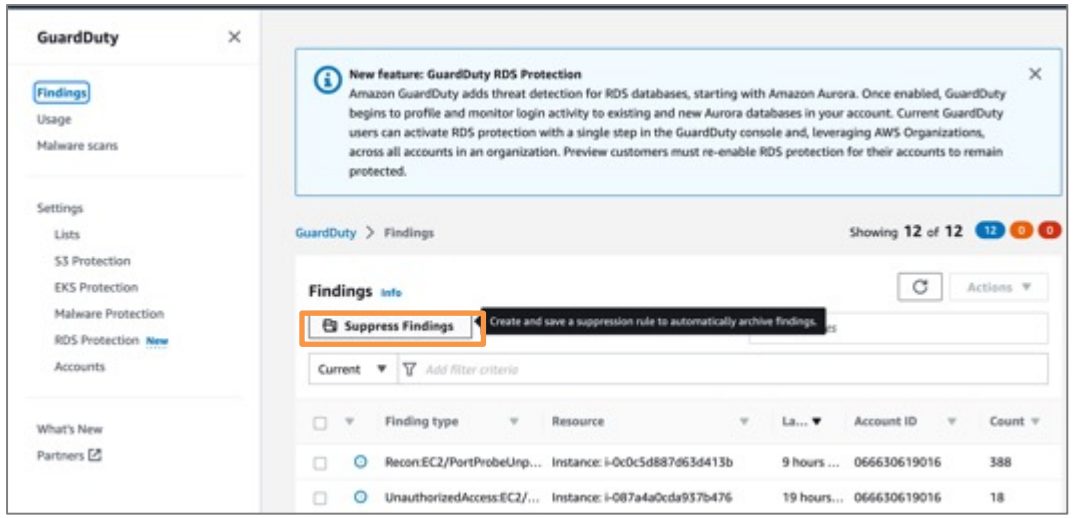
- GuardDuty에서 탐지된 위협에 대해 탐지오류로 확인 또는 예외승인처리가 된 경우, 예외처리 적용

  * 방안1) 해당 Source IP에 대해 '신뢰할수 있는 IP 목록'으로 추가
  신뢰할 수 있는 IP 목록은 AWS 환경과의 보안 통신을 위해 신뢰할 수 있는 IP 주소로 구성되며, GuardDuty는 신뢰할 수 있는 IP 목록에 포함된 IP 주소에 대한 탐지 결과 미생성

  * 방안2) 탐지로그에 대해 Suppression 적용하여 GuardDuty 콘솔에 로그가 뜨지 않도록 설정



<방안 1>



<방안 2>

GuardDuty 과금 기준

- Amazon GuardDuty의 과금기준은 아래 5가지 디멘션에 따라 책정되며, GuardDuty 분석을 위해 아래 로그 소스를 활성화하는데 추가 요금은 부과되지 않음
- https://aws.amazon.com/ko/guardduty/pricing/?nc1=h_ls

	Asia Pacific (Seoul)
VPC Flow 로그와 DNS 로그 분석	
최초 500GB/월	GB당 1.15 USD
다음 2,000GB/월	GB당 0.58 USD
다음 7,500GB/월	GB당 0.29 USD
10,000GB/월 초과	GB당 0.17 USD
AWS CloudTrail 관리 이벤트 분석	
이벤트 1백만 건	월이벤트 1백만 건당 4.60 USD
EBS 데이터 볼륨 스캔 분석	
Per GB / month	GB당 0.04 USD

	Asia Pacific (Seoul)
AWS CloudTrail S3 데이터 이벤트 분석	
최초 이벤트 5백만 건/월	이벤트 1백만 건당 0.90 USD
다음 이벤트 45억 건/월	이벤트 1백만 건당 0.45 USD
이벤트 50억 건 이상/월	이벤트 1백만 건당 0.23 USD
Amazon EKS 감사 로그	
최초 이벤트 1억 건/월	이벤트 1백만 건당 2.05 USD
다음 이벤트 1억 건/월	이벤트 1백만 건당 1.03 USD
이벤트 2억 건 이상/월	이벤트 1백만 건당 0.26 USD

Thank you!

Thank you!