샘플 분석 환경 구성

2025.12.27 (토)

최병주

샘플 분석 환경 구성

악성코드의 기능, 동작 방식, 목적을 파악하기 위한 환경 구성

샘플 분석 환경 구성(Cloud)

Customer Service Policy for Penetration Testing

Permitted Services

- Amazon EC2 instances, WAF, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS AppSync
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments
- Amazon Elastic Container Service
- AWS Fargate
- Amazon OpenSearch Service
- Amazon FSx
- Amazon Transit Gateway

Customers seeking to test non approved services will need to work directly with AWS Support or your account representative.

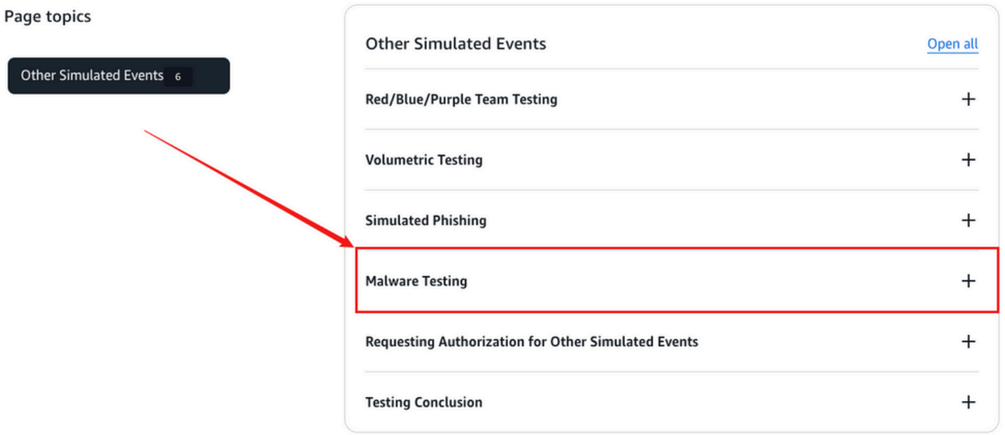
Prohibited Activities

Customers seeking to test non approved services will need to work directly with AWS Support or your account representative.

- DNS zone walking via Amazon Route 53 Hosted Zones
- DNS hijacking via Route 53
- DNS Pharming via Route 53
- Denial of Service (DoS), Distributed Denial of Service (DDoS),
- Simulated DoS, Simulated DDoS (These are subject to the DDoS Simulation Testing policy Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)
- S3 bucket takeover
- Subdomain Takeover

Prohibited Services for Outbound Penetration Testing

- Amazon API Gateway



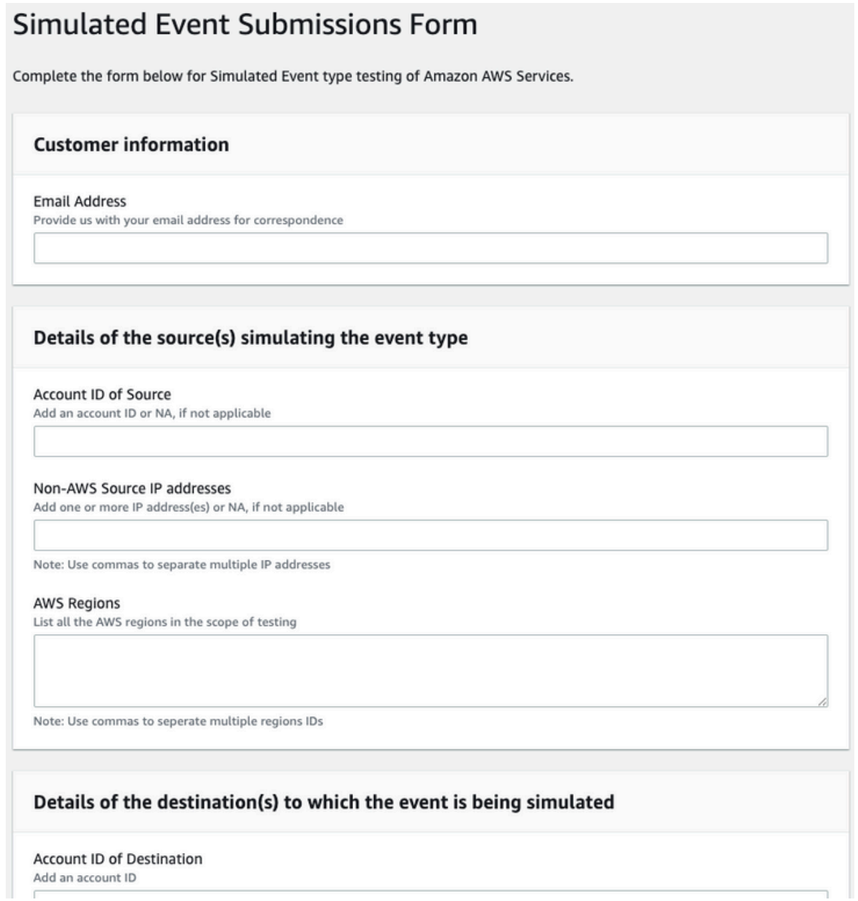
Malware Testing is the practice of subjecting malicious files or programs to applications or antivirus programs to improve security features.

Customers seeking to perform Malware Testing must submit a Simulated Events form for review.

Review를 거친 후 멀웨어 테스트 가능

(Penetration Testing)

샘플 분석 환경 구성(Cloud)



Simulated Event Submissions Form

Complete the form below for Simulated Event type testing of Amazon AWS Services.

Customer information

Email Address
Provide us with your email address for correspondence

Details of the source(s) simulating the event type

Account ID of Source
Add an account ID or NA, if not applicable

Non-AWS Source IP addresses
Add one or more IP address(es) or NA, if not applicable

Note: Use commas to separate multiple IP addresses

AWS Regions
List all the AWS regions in the scope of testing

Note: Use commas to seperate multiple regions IDs

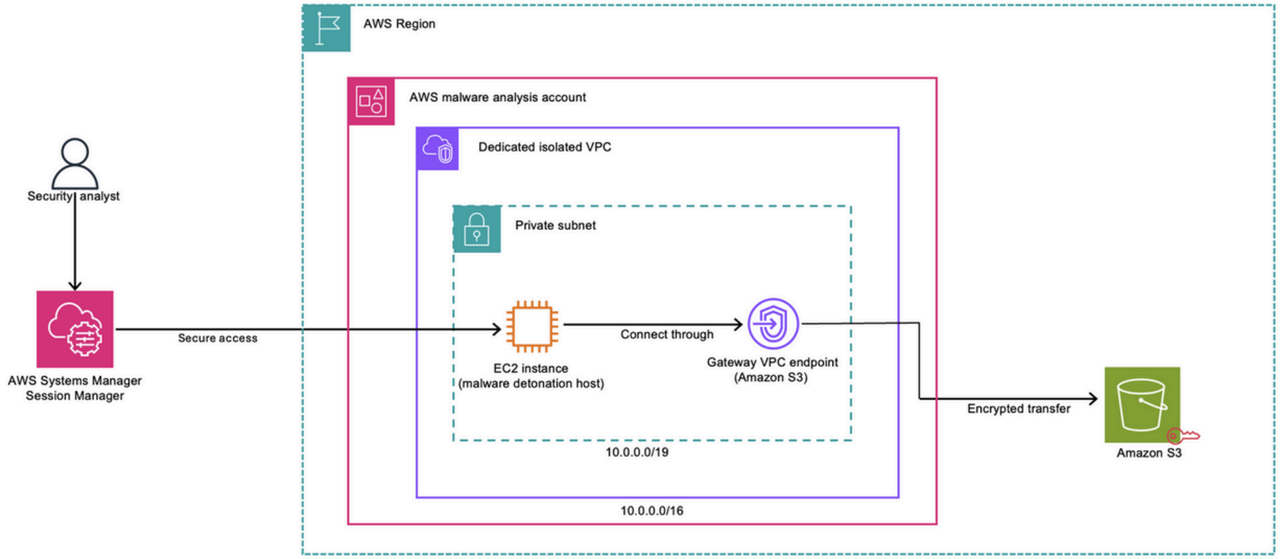
Details of the destination(s) to which the event is being simulated

Account ID of Destination
Add an account ID

번역
이 활동으로 인해 악용 신고가 접수되거나 AWS IP 평판에 부정적 영향이 발생할 경우, 활동 중단 사유가 됩니다.
이 활동은 악성코드가 자동으로 서비스 거부 트래픽을 전송하는 등 AWS 서비스에 영향을 주어서는 안 됩니다. 이 활동으로 인한 영향 발생 시 활동 중단 사유가 됩니다.
이 활동은 규정된 아키텍처 및 보안 모델을 사용하여 수행되어야 합니다. 고객은 발생할 수 있는 문제에 대해 자산을 지속적으로 모니터링하고 평가해야 합니다.
AWS는 부정적 영향이나 본 약관 위반이 확인될 경우 이 활동을 불허할 권리를 보유합니다.
고객은 제3자의 악용 신고에 적시에 응답해야 합니다.
고객은 보안 연구와 관련하여 Amazon에 대한 법적 청구 또는 기타 피해에 대해 Amazon을 면책하고 손해를 배상해야 합니다.

- 수행할 악성코드 분석에 대한 세부사항
- 테스트 환경 내 인스턴스 보안에 대한 세부사항
- 활동이 환경 내 문제를 일으키거나 외부로 유출되지 않도록 하기 위한 보안 조치 세부사항
- 테스트 환경 운영 기간

샘플 분석 환경 구성(Cloud)



RE: Your AWS Inquiry [ ] [AWS ID] 받은편지함 ×

Trust and Safety <trustandsafety@support.aws.com>

영어(영국) 한국어 이메일 번역

Hello,

Thank you for contacting us. We do allow malware analysis testing on AWS, but there are specific terms and conditions that must be met and agreed to.

These conditions are not subject to negotiation.

Any abuse report or negative impact on AWS IP reputation that is a result of this activity is cause to disallow it's continuance.
The activity will not impact any AWS service, such as through malware automatically sending denial of service traffic. Any impact that is a result of this activity is cause to disallow it's continuance.
The activity will be conducted using a prescribed architecture and security model. The customer will continuously monitor and assess their assets for any issues that may result.
We also reserve the right to disallow this activity should we determine any negative impact or violation of these terms.

These are general requirements for how a customer should architect their solution:

This will be carried out in a secure VPC
The VPC and instances will have inbound traffic restricted to a set of IP addresses owned by the customer.
The instances involved will not have public IP addresses.
The instances will not be allowed to send any packets to the internet using an AWS owned source IP address. (Customer can use a VPN, BYOIP or other tunneling mechanism so none of the traffic directly originates from AWS IP Space)
DNS should be disabled in the VPC to prevent malware looking up command and control domains.
Malware should be detonated in a sandbox.
Systems involved should be fully patched and hardened in accordance to security best practices.
System monitoring and logging should be in place and reviewed.
Simulation services, such as INetSim are allowed but must be run within the same VPC as the malware.
Secure S3 bucket and have encryption turned on

If you will meet and agree to the terms and conditions listed above we will move forward with the approval process.

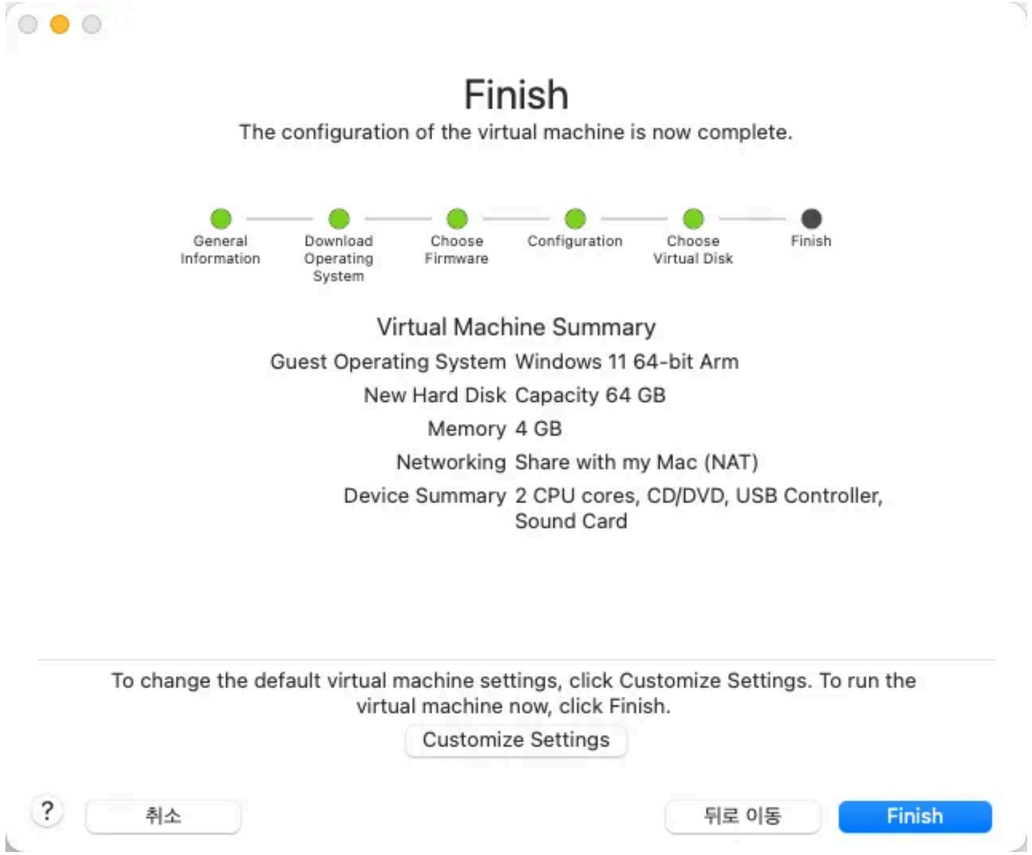
Please submit your request directly to (https://console.aws.amazon.com/support/contacts#/simulated-events).

Required Information

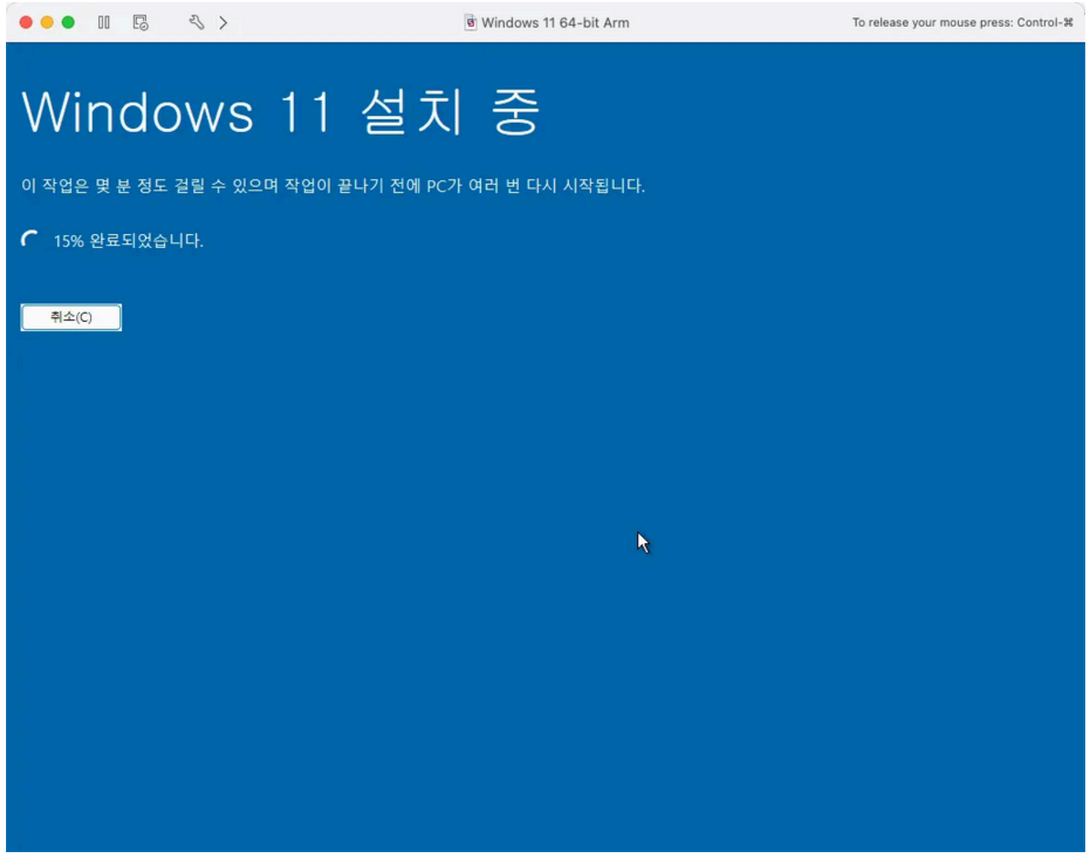
2 Emergency contact names and phone numbers (Please submit 1 more, we need atleast 2 phone numbers)

Contact Information of the team/person that will be doing the testing: Name, Email Address, Phone Number
Length of time the testing environment will be live:

샘플 분석 환경 구성(VMWare)

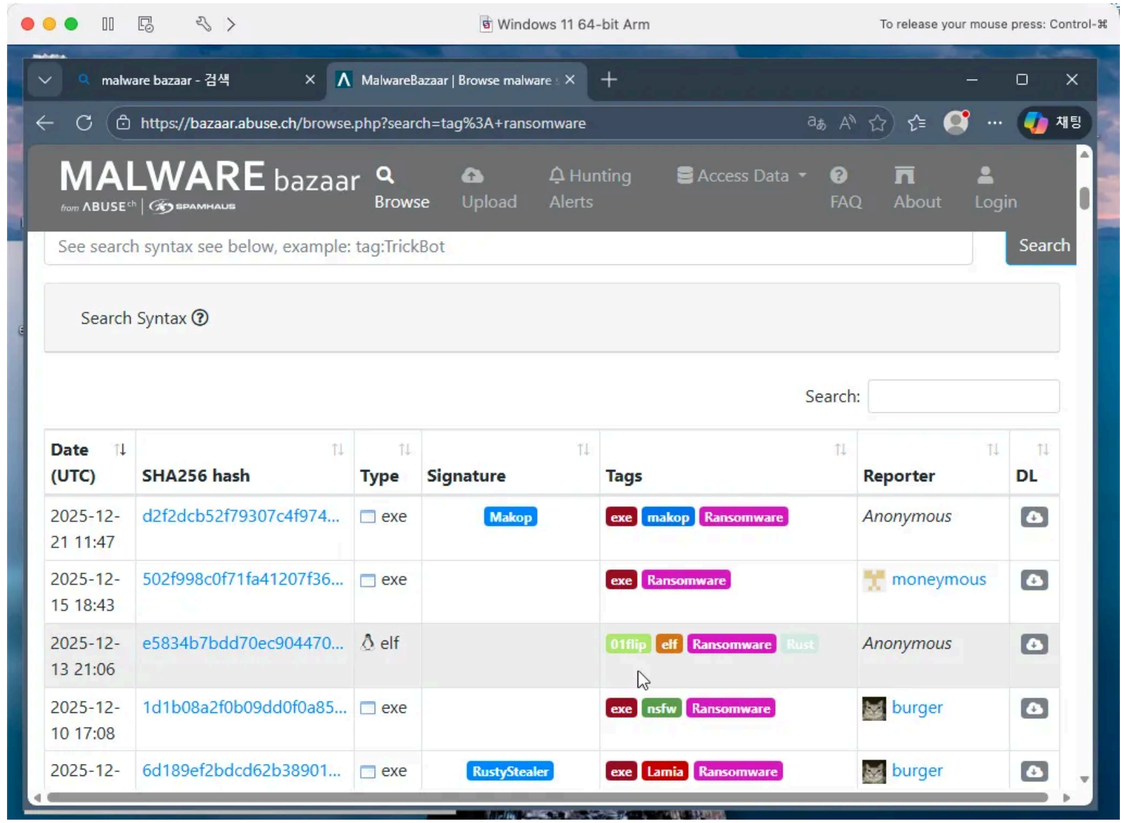


샘플 분석 환경 구성(VMWare)



도구	다운로드
PE Studio	https://www.winitor.com/download
Process Monitor	https://learn.microsoft.com/sysinternals/downloads/procmon
Process Explorer	https://learn.microsoft.com/sysinternals/downloads/process-explorer
Autoruns	https://learn.microsoft.com/sysinternals/downloads/autoruns
Wireshark	https://www.wireshark.org/download.html
Regshot	https://sourceforge.net/projects/regshot/

샘플 분석 환경 구성(VMWare)



사이트	특징	링크
MalwareBazaar	최신 샘플, 태그 검색, API 제공	https://bazaar.abuse.ch
theZoo	GitHub, 교육용, 유명 샘플	https://github.com/ytisf/theZoo
VirusTotal	샘플 다운로드 (유료)	https://virustotal.com
Malshare	API 기반	https://malshare.com

샘플 분석 환경 구성(VMWare)