

보안요건을 위한 소소한 자동화 이야기!

하나투어
DevOps 팀
이금춘



2024년 6월 27일 (목) 오후 7:00 GMT+9 참석자(93명)

2024년 5월 23일 (목) 오후 7:00 GMT+9 참석자 50명
2024년 4월 25일 (목) 오후 7:00 GMT+9 참석자 44명
2024년 3월 28일 (목) 오후 7:00 GMT+9 참석자 75명
2024년 2월 15일 (목) 오후 7:00 GMT+9 참석자 43명
2024년 1월 18일 (목) 오후 7:00 GMT+9 참석자 66명

2023년 12월 14일 (목) 오후 7:00 GMT+9 참석자 50명
2023년 11월 16일 (목) 오후 7:00 GMT+9 참석자 33명
2023년 10월 19일 (목) 오후 7:00 GMT+9 참석자 44명
2023년 9월 21일 (목) 오후 7:00 GMT+9 참석자 55명
2023년 8월 17일 (목) 오후 7:00 GMT+9 참석자 68명
2023년 7월 19일 (수) 오후 7:00 GMT+9 참석자 53명
2023년 6월 22일 (목) 오후 7:00 GMT+9 참석자 51명
2023년 5월 31일 (수) 오후 7:00 GMT+9 참석자 40명
2023년 4월 20일 (목) 오후 7:00 GMT+9 참석자 53명
2023년 3월 23일 (목) 오후 7:00 GMT+9 참석자 37명
2023년 2월 22일 (수) 오후 7:00 GMT+9 참석자 46명

2019년 8월 27일 (화) 오후 7:00 GMT+9 참석자 41명
2019년 6월 20일 (목) 오후 7:00 GMT+9 참석자 83명

순서

저는요..

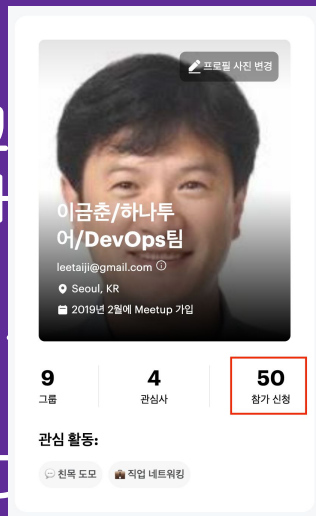
EventBridge 로 보안팀 안심시키기

SessionManager 로 서버 접근 솔루션 비용
절약하기

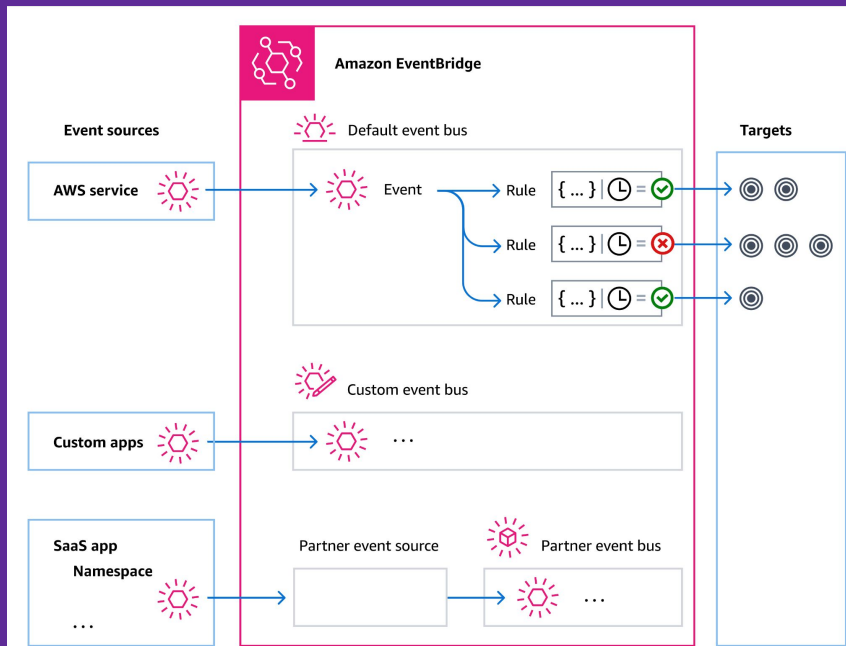
RunCommand 로 취약점 점검 스크립트
실행하기

저는요..

학교다닐 때는 C언어를 주로 했었고
첫 회사는 바다이야기 같은 성인용게임개발을 했었고
자바가 대세라 자바배워서 SI 프로젝트를 위주로 개발하
기업용 검색엔진 회사에서 검색엔진 좀 맛보고
KBS 에서 클라우드 전환 프로젝트 하면서 AWS 를 시
베스핀글로벌에서 AWS 좀 더 배우고
위메프, 하나투어 같은 서비스 회사를 다니고 있습니다



EventBridge 로 보안팀 안심시키기



Event Sources (발굴하기)

EventBridge 다음을 포함한 이벤트 소스에서 이벤트를 수신할 수 있습니다.

- AWS 서비스
- 사용자 정의 애플리케이션
- 서비스형 소프트웨어(SaaS) 파트너

Targets (생색내기)

대상은 이벤트가 규칙에 정의된 이벤트 패턴과 일치할 때 이벤트를 EventBridge 보내는 리소스 또는 엔드포인트입니다.

대상은 여러 이벤트 버스에서 다양한 이벤트를 수신할 수 있습니다.

자세한 정보는 [아마존 EventBridge 타겟](#)을 참조하세요.

EventBridge 로 보안팀 안심시키기 - AWS WAF



21시 :

WAF 유입량이 급증 (식별)

22시30분 :

blacklist 로 특정 아이피 차단. (전파 프로세스 없음)

23시 :

서비스 유입량 급 하락

서비스 페이지 접속 안됨

00시 50분 :

blacklist 에 등록된 ip 가 NAT IP 임을 식별

00시 55분 :

blacklist 에 등록된 ip 차단 해지

EventBridge 로 보안팀 안심시키기 - AWS WAF

AWS WAF > Web ACLs > [Redacted]

[Redacted] Download web ACL as JSON

< Traffic overview **Rules** Associated AWS resources Custom response bodies Logging and metrics Sampled requests CloudWatch >

Rules (22) Edit Delete Add rules ▼

Find rules

<input type="checkbox"/>	Name	Action	Priority	Custom response
<input type="checkbox"/>	whitelist	Allow	0	-
<input type="checkbox"/>	XFF_blacklist	Count	1	-
<input type="checkbox"/>	blacklist	Block	2	-
<input type="checkbox"/>	custom_method_check	Block	3	Status 400, error_page_231213
<input type="checkbox"/>	account_Brute	Count	4	-
<input type="checkbox"/>	Block-use-agent	Block	5	-
<input type="checkbox"/>	1000r_5m_overseas_IP	Block	6	-
<input type="checkbox"/>	attack_ip	Count	7	-
<input type="checkbox"/>	FND_PDF_Upload	Allow	8	-
<input type="checkbox"/>	Amadaus_exception_handling_20220812	Allow	9	-

EventBridge 로 보안팀 안심시키기 - AWS WAF

Creation method

Method

☐ Use schema
Use an Amazon EventBridge schema to generate the event pattern.

☒ Use pattern form
Use a template provided by EventBridge to create an event pattern.

☐ Custom pattern (JSON editor)
Write an event pattern in JSON.

Event pattern Info

Event source
AWS service or EventBridge partner as source

AWS services

WAF

WAF Regional

Select a service provider

Event pattern
Event pattern, or filter to match the events

1

Enter the event JSON

Copy

Test pattern

Edit pattern

WAFv2 가 없네??

Cancel

Previous

Next

Event pattern Info

Event source
AWS service or EventBridge partner as source

AWS services

CloudTrail

Event type
The type of events as the source of the matching pattern

AWS API Call via CloudTrail

Event pattern
Event pattern, or filter to match the events

```
1 {
2   "source": ["aws.cloudtrail"],
3   "detail-type": ["AWS API Call via CloudTrail"],
4   "detail": {
5     "eventSource": ["cloudtrail.amazonaws.com"]
6   }
7 }
```

cloudtrail 은 아닌것 같은데??

Copy

Test pattern

Edit pattern

All events that are delivered via CloudTrail have **AWS API Call via CloudTrail** as the value for **detail-type**. Events from API actions that start with the keywords List, Get, or Describe are not processed by EventBridge, with the exception of events from the following STS actions: GetFederationToken and GetSessionToken. Data events (for example, for Amazon S3 object level events, DynamoDB, and AWS Lambda) must have trails configured to receive those events. [Learn more.](#)

Event Type Specification 1

☒ Any operation

☐ Specific operation(s)

Cancel

Previous

Next

EventBridge 로 보안팀 안심시키기 - AWS WAF

CloudTrail > Event history

Event history (25+) [Info](#)

Event history shows you the last 90 days of management events.

Lookup attributes

Event name ...

<input type="checkbox"/>	Event name	Event time	User name	Event source	Resource type
<input type="checkbox"/>	UpdateWebACL	May 29, 2024, 17:19:37 (UTC+0...		wafv2.amazonaws.com	-
<input type="checkbox"/>	UpdateWebACL	May 29, 2024, 17:19:25 (UTC+0...		wafv2.amazonaws.com	-
<input type="checkbox"/>	UpdateWebACL	May 29, 2024, 14:19:45 (UTC+0...		wafv2.amazonaws.com	-
<input type="checkbox"/>	UpdateWebACL	May 29, 2024, 14:19:40 (UTC+0...		wafv2.amazonaws.com	-
<input type="checkbox"/>	UpdateWebACL	May 24, 2024, 16:20:24 (UTC+0...		wafv2.amazonaws.com	-
<input type="checkbox"/>	UpdateWebACL	May 24, 2024, 16:20:20 (UTC+0...		wafv2.amazonaws.com	-
<input type="checkbox"/>	UpdateWebACL	May 22, 2024, 18:08:53 (UTC+0...		wafv2.amazonaws.com	-
<input type="checkbox"/>	UpdateWebACL	May 22, 2024, 18:08:48 (UTC+0...		wafv2.amazonaws.com	-
<input type="checkbox"/>	UpdateWebACL	May 16, 2024, 19:30:34 (UTC+0...		wafv2.amazonaws.com	-
<input type="checkbox"/>	UpdateWebACL	May 16, 2024, 19:30:27 (UTC+0...		wafv2.amazonaws.com	-

```
1 {
2   ... "eventVersion": "1.08",
3   ... "userIdentity": {
4     ... "type": "IAMUser",
5     ... "principalId": "AIDA2...",
6     ... "arn": "arn:aws:iam:695809562949:user/...@hanatour.com",
7     ... "accountId": "695809562949",
8     ... "accessKeyId": "ASIA...",
9     ... "userName": "...@hanatour.com",
10    ... },
11   ... },
12   ... "eventTime": "2024-05-29T08:19:37Z",
13   ... "eventSource": "wafv2.amazonaws.com",
14   ... "eventName": "UpdateWebACL",
15   ... "awsRegion": "ap-northeast-2",
16   ... },
17   ... "requestParameters": {
18     ... "name": "ant-dcr-waf-web-acl",
19     ... "scope": "REGIONAL",
20     ... "id": "58670cec-edcf-4174-a529-c7b3a380c70e",
21     ... "defaultAction": {
22       ... "allow": {},
23     },
24     ... "description": "waf web acl for skshieldus",
25     ... "rules": [
26       ... {
27         ... "name": "whitelist",
28         ... "priority": 0,
29         ... },
30       ... {
31         ... "name": "XFF_blacklist",
32         ... "priority": 1,
33         ... },
34       ... {
35         ... "name": "blacklist",
36         ... "priority": 2,
37         ... },
38       ... ],
39     ... },
40   ... },
41   ... },
42   ... },
43   ... },
44   ... "eventType": "AwsApiCall",
45   ... "apiVersion": "2019-04-23",
46   ... "recipientAccountId": "695809562949",
47   ... },
48   ... },
49 }
```

EventBridge 로 보안팀 안심시키기 - AWS WAF

```
{
  "version": "0",
  "id": "UUID",
  "source": "event source",
  "detail-type": "event name",
  "account": "ARN",
  "time": "timestamp",
  "region": "region",
  "resources": [
    "ARN"
  ],
  "detail": {
    JSON object
  }
}
```

source

이벤트를 생성한 서비스를 식별합니다. AWS 서비스에서 발생하는 모든 이벤트는 'aws'로 시작합니다. 고객이 생성한 이벤트는 "aws"로 시작되지 않는 한 어떤 값이라도 가질 수 있습니다.

예시)

arn:aws:wafv2:ap-northeast-2:695809562949:regional/webacl/....

detail-type

source 필드를 함께 사용하여 detail 필드에 나타나는 필드와 값을 식별합니다.

CloudTrail 전달한 이벤트는 의 **AWS API Call via CloudTrail** 값으로 사용됩니다.

detail

이벤트에 대한 정보를 포함하는 JSON 객체입니다. 이벤트를 생성하는 서비스에 따라 이 필드의 내용이 결정됩니다. "{}"이(가) 될 수 있습니다.

EventBridge 로 보안팀 안심시키기 - AWS WAF

```
{  
  "source": ["aws.wafv2"],  
  "detail-type": ["AWS API Call via CloudTrail"],  
  "detail": {  
    "eventSource": ["wafv2.amazonaws.com"],  
    "eventName": ["UpdateWebACL", "CreateWebACL", "DeleteWebACL", "UpdateIPSet"]  
  }  
}
```

EventBridge 로 보안팀 안심시키기 - AWS WAF

Amazon EventBridge > Rules > Create rule

Step 1
[Define rule detail](#)

Step 2
[Build event pattern](#)

Step 3
Select target(s)

Step 4 - optional
[Configure tags](#)

Step 5
[Review and create](#)

Select target(s)

Permissions

Note: When using the EventBridge console, EventBridge will automatically configure the proper permissions for the selected targets. If you're using the AWS CLI, SDK, or CloudFormation, you'll need to configure the proper permissions.

Target 1

Target types
Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.

☐ EventBridge event bus

☐ EventBridge API destination

☒ AWS service

Select a target [Info](#)

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

SNS topic

Topic

aws-noti

EventBridge 로 보안팀 안심시키기 - AWS WAF

AWS Notification Message



○ aws-noti-for-changed-waf <no-reply@sns.amazonaws.com>

받는 사람: aws-noti-for-changed-waf

```
{
  "eventName": "UpdateWebACL",
  "accountId": [REDACTED],
  "userName": [REDACTED],
  "awsRegion": [REDACTED],
  "sourceIPAddress": [REDACTED],
  "requestParametersName": "hnt-dcr-waf-web-acl"
}
```

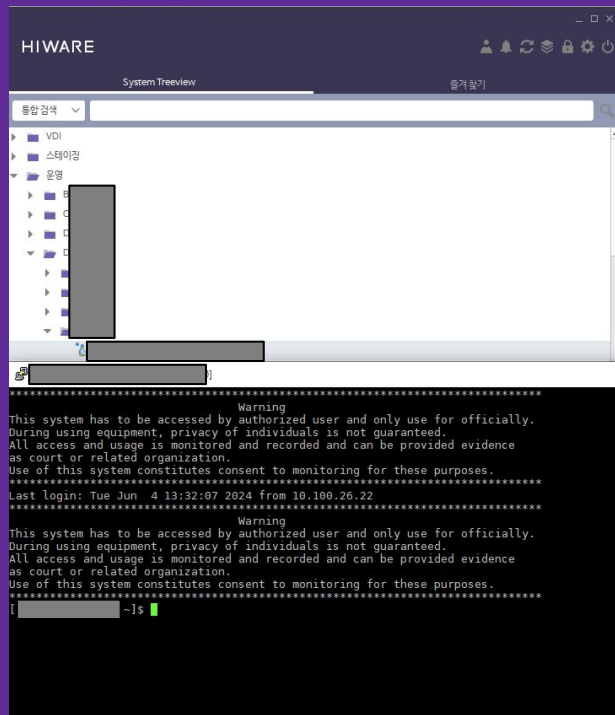
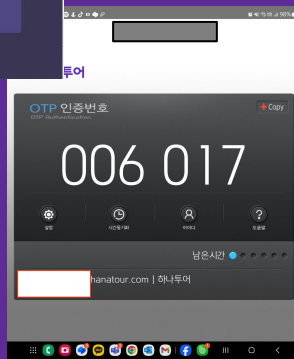
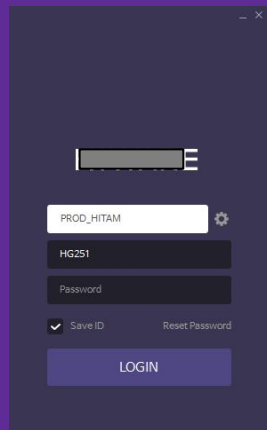
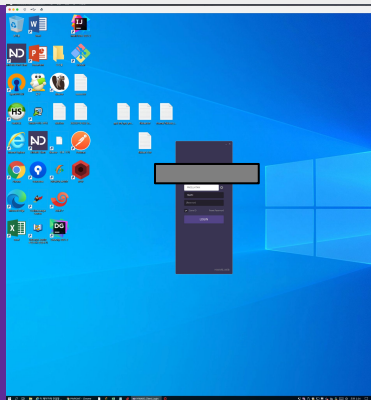
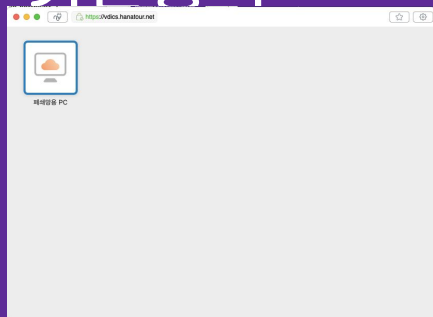
EventBridge 로 보안팀 안심시키기 - Security Group

```
{
  "source": ["aws.ec2"],
  "detail-type": ["AWS API Call via CloudTrail"],
  "detail": {
    "eventSource": ["ec2.amazonaws.com"],
    "eventName": ["AuthorizeSecurityGroupIngress", "RevokeSecurityGroupIngress", "CreateSecurityGroup", "DeleteSecurityGroup",
"AuthorizeSecurityGroupEgress", "RevokeSecurityGroupEgress"]
  }
}
```

EventBridge 로 보안팀 안심시키기 (부록) - Session Manager

```
{
  "source": ["aws.ssm"],
  "detail-type": ["AWS API Call via CloudTrail"],
  "detail": {
    "eventSource": ["ssm.amazonaws.com"],
    "eventName": ["StartSession"]
  }
}
```

SessionManager 로 서버 접근 솔루션 비용 절약하기 - 기존방식



SessionManager 로 서버 접근 솔루션 비용 절약하기 - 사전 조건

지원되는 운영 체제	Linux, macOS, Windows Session Manager에서는 AWS Systems Manager에서 지원되는 모든 Linux 및 macOS 버전을 지원합니다. Session Manager는 Windows Server 2012부터 Windows Server 2022까지 지원합니다.
SSM Agent	세션을 통해 연결하려는 관리형 노드에 AWS Systems Manager SSM Agent 버전 2.3.68.0 이상이 설치되어 있어야 합니다.
엔드포인트에 연결	연결하려는 관리형 노드는 다음 엔드포인트에 대한 HTTPS(포트 443) 아웃바운드 트래픽도 허용해야 합니다. <ul style="list-style-type: none">• ec2messages.<i>region</i>.amazonaws.com• ssm.<i>region</i>.amazonaws.com• ssmmessages.<i>region</i>.amazonaws.com
AWS CLI	(옵션) AWS Systems Manager 콘솔 또는 Amazon EC2 콘솔 대신 AWS Command Line Interface(AWS CLI)를 사용하여 세션을 시작한 경우 로컬 시스템에 CLI 버전 1.16.12 이상이 설치되어 있어야 합니다. <code>aws --version</code> 을 호출해 버전을 확인할 수 있습니다.

SessionManager - 세션 접속 이력 조회

AWS Systems Manager > Session Manager

Session Manager

Sessions Session history Preferences

Sessions

Filter sessions



Terminate

Start session

< 1 ... >

	Session ID	Owner	Instance ID	Document name	Reason	Start date	Status
<input type="radio"/>	z7xbb4qigb2pgj4omvztiudi5y	arn:aws:iam::618569531126:user/...	I-096...			Fri, 07 Jun 2024 08:14:11 GMT	Connected
<input type="radio"/>	ga7zckdacj7udhrbxx2ilmrw4	arn:aws:iam::618569531126:user/...	I-008...			Wed, 05 Jun 2024 08:22:04 GMT	Connected
<input type="radio"/>	ur.com-mbevxyghvdmss2yid4n2v4bmf4	arn:aws:iam::618569531126:user/...	I-068...			Mon, 27 May 2024 23:13:15 GMT	Connected
<input type="radio"/>	ur.com-wutidcvjpazpxnzalxcyw2wze	arn:aws:iam::618569531126:user/...	I-048...			Mon, 27 May 2024 22:58:47 GMT	Connected
<input type="radio"/>	qfhtaypggqkcc4wwm7vdk7s2cq	arn:aws:iam::618569531126:user/...	I-0c4...			Wed, 22 May 2024 03:13:08 GMT	Connected
<input type="radio"/>	2y22vfgrjk57r3k5fy6rifbjy	arn:aws:iam::618569531126:user/...	I-028...			Mon, 20 May 2024 10:05:05 GMT	Connected
<input type="radio"/>	ur.com-arebps5nkym3o5pojinsogeval	arn:aws:iam::618569531126:user/...	I-065...			Fri, 17 May 2024 23:18:04 GMT	Connected
<input type="radio"/>	2mmd6ajtmbptnl7eibpfhwuqm	arn:aws:iam::618569531126:user/...	I-0e8...			Thu, 16 May 2024 04:13:03 GMT	Connected
<input type="radio"/>	ur.com-m7klm62qncx5ynxexqap3lja7u	arn:aws:iam::618569531126:user/...	I-093...			Wed, 15 May 2024 03:33:30 GMT	Connected
<input type="radio"/>	ur.com-sqqnzaiyakzgcj43lrescs4rri	arn:aws:iam::618569531126:user/...	I-0fa...			Wed, 15 May 2024 02:45:17 GMT	Connected

SessionManager - 작업 히스토리 조회

CloudWatch > Log groups > /aws/ssm/ > bmp3773i3clucb64jbq2gs7m

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Filter events - press enter to search

Clear 1m

▶	Timestamp	Message
		No older events at this moment. Retry
▶	2024-06-07T13:10:01.158+09:00	{"eventVersion":"1.0","eventTime":"2024-06-07T04:10:01Z","awsRegion":"ap-northeast-2","target":{"id":"i- <input type="text" value=""/> d52b"},"userIdentity":{"arn":"arn:aws:iam:: <input type="text" value=""/> :user/k
▶	2024-06-07T13:10:20.157+09:00	{"eventVersion":"1.0","eventTime":"2024-06-07T04:10:20Z","awsRegion":"ap-northeast-2","target":{"id":"i- <input type="text" value=""/> d52b"},"userIdentity":{"arn":"arn:aws:iam:: <input type="text" value=""/> :user/k
▶	2024-06-07T13:10:25.158+09:00	{"eventVersion":"1.0","eventTime":"2024-06-07T04:10:25Z","awsRegion":"ap-northeast-2","target":{"id":"i- <input type="text" value=""/> d52b"},"userIdentity":{"arn":"arn:aws:iam:: <input type="text" value=""/> :user/k
▶	2024-06-07T13:11:29.158+09:00	{"eventVersion":"1.0","eventTime":"2024-06-07T04:11:29Z","awsRegion":"ap-northeast-2","target":{"id":"i- <input type="text" value=""/> d52b"},"userIdentity":{"arn":"arn:aws:iam:: <input type="text" value=""/> :user/k
▶	2024-06-07T13:11:35.157+09:00	{"eventVersion":"1.0","eventTime":"2024-06-07T04:11:35Z","awsRegion":"ap-northeast-2","target":{"id":"i- <input type="text" value=""/> d52b"},"userIdentity":{"arn":"arn:aws:iam:: <input type="text" value=""/> :user/k
▶	2024-06-07T13:21:35.158+09:00	{"eventVersion":"1.0","eventTime":"2024-06-07T04:21:35Z","awsRegion":"ap-northeast-2","target":{"id":"i- <input type="text" value=""/> d52b"},"userIdentity":{"arn":"arn:aws:iam:: <input type="text" value=""/> :user/k
▶	2024-06-07T13:52:29.158+09:00	{"eventVersion":"1.0","eventTime":"2024-06-07T04:52:29Z","awsRegion":"ap-northeast-2","target":{"id":"i- <input type="text" value=""/> d52b"},"userIdentity":{"arn":"arn:aws:iam:: <input type="text" value=""/> :user/k

No newer events at this moment. Auto retry paused. [Resume](#)

SessionManager - 세션 유지 시간 지정 가능

AWS Systems Manager > Session Manager

Session Manager

Sessions | Session history | **Preferences**

General preferences

Idle session timeout 30 minutes	Maximum session duration 600 minutes
Run As ec2-user	KMS encryption Disabled

CloudWatch logging

Send session logs to CloudWatch Enabled	Enforce CloudWatch log encryption Yes
Logging option Stream session logs	CloudWatch log group /aws/ssm/

S3 logging

Send session logs to S3 Enabled	S3 bucket
Enforce S3 log encryption Yes	S3 prefix ap-northeast-2

Shell profiles

Specify environment variables, shell preferences, or commands you want to run when your session starts. [Learn more](#)

Linux shell profile

```
sudo su - ec2-user
```

Windows shell profile

```
-
```

유틸 세션 시간 제한 값 지정

기본적으로 20분 동안 활동이 없으면 세션이 시간 초과
1~60분 동안 비활성 상태이면 세션이 시간 초과되도록
지정가능

15분으로 설정할 것을 권장

세션 활동 로깅 활성화

CloudWatch Logs 및 Amazon S3

SessionManager - IAM policy 를 사용자에게 부여

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ssmAWS1131",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ssm:StartSession"
      ],
      "Resource": [
        "arn:aws:ec2:*:695809562949:instance/*"
      ],
      "Condition": {
        "DateLessThan": {
          "aws:CurrentTime": "2025-05-07T14:59:59Z"
        }
      },
      "StringEquals": {
        "aws:ResourceTag/Name": [
          "NaverHmac-dev"
        ]
      }
    }
  ]
}
.... > 우측에 표시
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    ...
    {
      "Sid": "Sid2",
      "Effect": "Allow",
      "Action": [
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource": "*",
      "Condition": {
        "DateLessThan": {
          "aws:CurrentTime": "2025-05-07T14:59:59Z"
        }
      }
    },
    {
      "Sid": "Sid3",
      "Effect": "Allow",
      "Action": [
        "ssm:TerminateSession"
      ],
      "Resource": "arn:aws:ssm:*:695809562949:session/${aws:username}-*",
      "Condition": {
        "DateLessThan": {
          "aws:CurrentTime": "2025-05-07T14:59:59Z"
        }
      }
    }
  ]
}
```

SessionManager - ToDo

(선택 사항) 세션의 명령에
대한 액세스 제한

사용자 지정 `Session` 유형 AWS Systems Manager(SSM) 문서를
사용하여 사용자가 AWS Systems Manager **Session Manager** 세션에서
실행할 수 있는 명령을 제한할 수 있습니다.

RunCommand - RunShellScript

안녕하세요. 정보보호팀 [redacted]입니다.

'23년 취약점 점검결과에 대해 지금까지 바쁘신 와중에도 조치 진행에 협조해 주셔서 감사드립니다.

현재 정보보호팀에서 조치에 대한 이행점검을 진행하고 있으며, 지난 한주간 조치 항목이 있는 서버를 대상으로 점검 스크립트를 구동 완료했습니다.

다만 일부 서버/EC2의 경우 하이퍼바이저를 통한 접근이 불가함에 따라 정보보호팀에서 자체적으로 스크립트 구동이 어려웠
아래와 같이 협조 요청을 드리고자 합니다.

바쁘시겠지만 조치 여부를 확인할 수 있도록 협조 요청 드립니다.
별도의 JIRA 등록이 필요한 경우 및 기한 내 확인이 어려우신 경우 말씀 부탁드립니다.

1. 협조요청사항 : 스크립트 구동 후 결과 파일 전달 (메일로 최신 또는 S3 업로드)
※ 스크립트 구동 방법 : 첨부파일 내 스크립트 파일 및 구동 가이드 참조
2. 스크립트 구동 대상 : [redacted] EC2
3. 협조요청 부서(팀) : [redacted]
4. 협조요청 기한 : 27.11.10 까지
5. 대상 정보 상세 :

Hostname(자산명)	서비스	IP	운영환경	관리부서	조치 항목	상태
[redacted]	DB #1	[redacted]	Prod	[redacted]		
	DB #2		Prod			
	DB #1		Prod			
	DB #2		Prod			
	하나복형 MTS DB #1		Prod			
	하나복형 MTS DB #2		Prod			
	인					
	vm 백서버 (nsx, vcenter)		PROD			
	AD 5		PROD			
	전결서버		VDI			
[redacted]	공 서버	[redacted]	VDI	[redacted]		
	parking		dev	DevOps팀	U-13	중지
	evops		dev	DevOps팀	U-13	구동중
	ops-logs		prod	DevOps팀	U-01, U-13	구동중
	fad		prod	DevOps팀	U-04	삭제
	relat		prod	DevOps팀	U-13	구동중
	pyword-batch		QA	DevOps팀	U-01	구동중
	id-eks					
	evops		dev	DevOps팀	U-13	삭제

정보보호팀 아이유입니다.
정보보호팀에서 취약점 점검을 해야 합니다.
스크립트 구동해주시고 결과 파일 전달
해주세요.
서버정보는 대략 이렇습니다



AWS Systems Manager > Run Command > Run a command

Run a command

Command document

Select the type of command that you want to run.

Search by keyword or filter by tag or attributes

Search: RunShell X

Clear filters

Name	Owner	Platform types
<div><div></div><div>AWS-RunShellScript</div><div></div></div>	Amazon	Linux, MacOS

Description

Run a shell script or specify the commands to run.

Document version

Choose the document version you want to run.

1 (Default)

Command parameters

Commands

(Required) Specify a shell script or a command to run.

1

Target selection

Choose a method for selecting targets.

Specify instance tags

Specify one or more tag key-value pairs to select instances that share those tags.

Target selection

Target selection

Choose a method for selecting targets.

☒ Specify instance tags

Specify one or more tag key-value pairs to select the instances that share those tags.

☐ Choose instances manually

Manually select the instances you want to register as targets.

☐ Choose a resource group

Choose a resource group that includes the resources you want to target.

Specify instance tags

Specify one or more instance tag key-value pairs to identify the instances where the tasks will run

Tag key

Enter a tag key and optional value applied to the instances you want to target, and then choose Add.

Tag value (optional)

Add

Env: dev X

RunCommand - 실행 명령어

스크립트 실행

```
aws s3 cp s3://<bucket_name>/security/scripts/ec2_linux_20231115.sh - | sudo bash
```

스크립트 실행 결과 파일을 S3 로 저장

```
sudo aws s3 mv *result.txt s3://<bucket_name>/security/check_result/2023/hnt-cloud/dev/
```

(부록) GitHub Copilot 시연

AMI 목록을 먼저 출력하고
해당 AMI를 사용하는 모든
EC2 찾아주는 쉘 스크립트
작성해줘

끝으로...

📅 2024년 6월 27일 목요일



-김옥희

아들 화이팅. 아들은 오늘도 발표 잘하리라 믿는다. 열심히 잘하고있는 아들이 자랑스럽다. 오늘도 화이팅. ♡♡♡♡♡

오전 8:37

오전 9:08

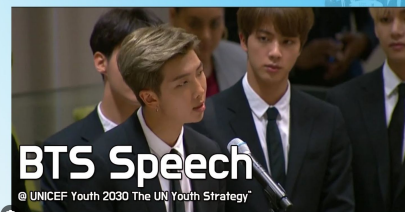
ㅎㅎㅎ 뭘 격려까지 ㅎㅎ 참석자가 90명이 넘어서 긴장되긴 해요



-김옥희

우리 아들은 잘할거야 힘내~~~

오전 9:43



시간이 된다면.. **같이 얘기 하고 싶어요...**

인프라 구성시 승인 프로세스를 어떻게 하시는지..

DevOps 는 주로 어떤일을 하는게 맞는건지..

**비용관련되어서 관심이 많다보니 일이 너무 많은 데
담당인력이 있는 회사가 있으실까요?**