

Sécurité dans les environnements infonuagiques

Module 3: Gestion des Configurations (Part 2)

Armstrong Foundjem

Polytechnique Montréal

Automne 2023

Plan

- ① VPC & EC2 security
 - ① Data Protection
 - ② Infrastructure Security
 - ③ IAM
 - ④ Resilience
 - ⑤ Compliance Validation
 - ⑥ Vulnerability Analysis
 - ⑦ Threat Analysis

- 1 Data Protection
- 2 Infrastructure security
- 3 IAM
- 4 Resilience
- 5 Compliance validation
- 6 Vulnerability Analysis
- 7 Threat Analysis

MFA

- Use Multi-factor Authentication (MFA) to check users access to the VPC infrastructure using a time-based one-time password (TOTP) algorithm.
 - Go to **Users > Security Credentials** to setup a virtual MFA device

The screenshot shows the AWS IAM console interface for a user. At the top, there are tabs for 'Groups', 'Permissions', 'Security Credentials', and 'Access Advisor'. The 'Security Credentials' tab is selected. Below the tabs, there are two main sections: 'Access Keys' and 'Sign-In Credentials'.

Access Keys Section:

- Text: "Use access keys to make secure REST or Query protocol requests to any AWS service API. For your protection, you should never share your access keys. We recommend that you rotate your access keys frequently. [Learn more about Access Keys](#)"
- Button: "Create Access Key"
- Table:

Access Key ID	Created	Last Used	Last Used Service	Last Used
AKIAJSLD6X3HY7ECPORQ	2016-10-19 09:10 PDT	N/A	N/A	N/A

Sign-In Credentials Section:

- Text: "User Name: Rob" (with a "Manage Password" button)
- Text: "Password: Yes"
- Text: "Last Used: 2016-10-21 10:16 PDT"
- Text: "Multi-Factor Authentication Device: No" (with a "Manage MFA Device" button highlighted by a red box)

- Grant access to VPC for MFA-authenticated users using IAM policy

SSL/TLS encryption

```
"Statement":[
  {
    "Sid": "AllowActionsForEC2",
    "Effect": "Allow",
    "Action": ["ec2:RunInstances",
              "ec2:DescribeInstances",
              "ec2:StopInstances "],
    "Resource": "*"
  },
  {
    "Sid": "AllowActionsForEC2WhenMFAIsPresent",
    "Effect": "Allow",
    "Action": "ec2:TerminateInstances",
    "Resource": "*",
    "Condition": {
      "Bool": { "aws:MultiFactorAuthPresent": "true" }
    }
  }
]
```

- Enforce SSL/TLS (up to 1.2) for traffic encryption using AWS Certificate Manager. On AWS CLI,
 - Request a public certificate: *aws acm request-certificate --domain-name www.polystudent.com* (more options)
 - Check renewal status: *aws acm describe-certificate --certificate-arn arn:aws:acm:region:userID:certificate/cert_ID*
 - Import certificates: *aws acm import-certificate --certificate fileb://xx.pem --private-key fileb://xxxx.pem* (more options)

Logging

- Enable logging and monitoring using AWS Flow logs and AWS Cloud Trail
 - *Flow logs*: capture inbound/outbound IP flow information to/from network interfaces of the VPC and stores it on S3/CloudWatch

Create flow log

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can

Resources vpc-e816e482 ⓘ

Filter* All ⓘ

Destination
 Send to CloudWatch Logs ⓘ
 Send to an S3 bucket

S3 bucket ARN* arn:aws:s3:::atl-vpc-demo ⓘ

Please note, a resource-based policy will be created for you and attached to the target bucket.

Log record format

Format
 AWS default format
 Custom format

Format preview \${account-id} \${instance-id} \${tcp-flags}

Log format* Specify the fields to include in the flow log record. [Learn more](#) ⓘ

account-id instance-id tcp-flags

Clear all

- *Cloud Trail*: records and monitors logs across multiple regions or a single region

Data Protection At Rest & In Transit

- Encrypt AWS Flow and Cloudtrail logs using AWS KMS
- Encrypt network traffic and S3 using AWS KMS and Macie

Log file SSE-KMS encryption [Info](#)

Enabled

Customer managed AWS KMS key

New

Existing

AWS KMS alias

cloudlogs-s3-encryption-key

▼ Additional settings

Log file validation [Info](#)

Enabled

- Use AWS KMS and Cloud HSM to generate FIPS 140-2 compliant cryptographic keys
- Enable ingress/egress traffic control using AWS NACL, Security Groups, and Network Access Analyzer

Traffic Mirroring

- Enable traffic mirroring to copy the network traffic for monitoring (e.g., level of workloads, intrusion detection system, packet analysis)
- Enable network routing control using AWS route analyzer

Network Manager ×

Global networks

Networking-workshop-...
Dashboard
Transit Gateways
On-premises
Devices
Sites

Network Manager > Global networks > Networking-workshop-global-network > Route Analyzer

Overview | Details | Geographic | Topology | Events | Monitoring | **Route Analyzer**

Networking-workshop-global-network Route Analyzer

The Route Analyzer analyzes the routing path between a specified source and destination. Note, Route Analyzer checks the routes on Transit Gateway route tables only. [Learn more](#)

Source	Destination
Transit Gateway tgr	Transit Gateway tgr
Transit Gateway attachment PIAttach	Transit Gateway attachment VPN1
IP address Private IP address 10.0.0.10	IP address Private IP address 10.4.0.10

Include return path in results
 Middlebox appliance? [Info](#)
If selected, state those that are known in the results

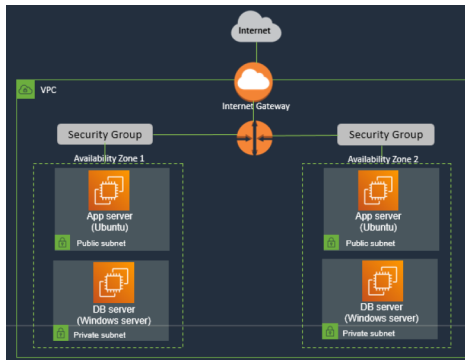
Run route analysis

Sondage 😊: <https://app.wooclap.com/ZSDLFI>.

wooclap

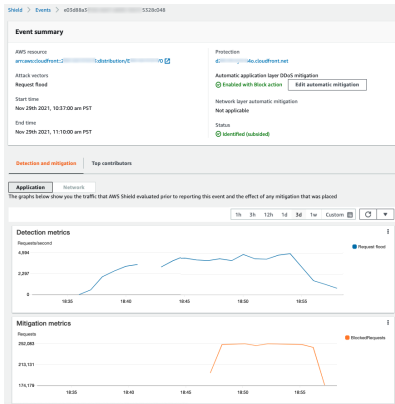
Network Isolation

- Isolate network in the VPC
 - subnets to isolate the tiers (e.g., app server, database server) in the VPC
 - private subnets for your instances that must not be accessed directly from the internet



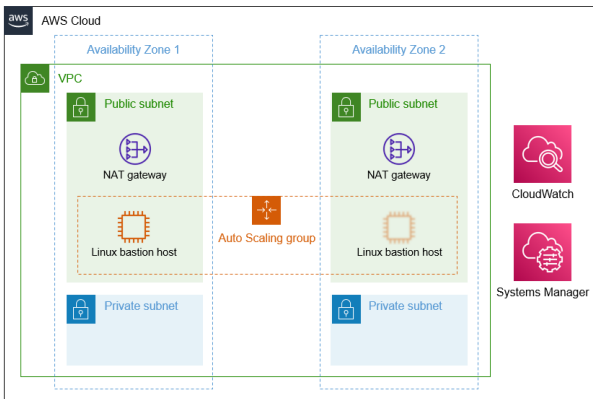
DDoS prevention

- Mitigate DDoS attacks
 - Use AWS Shield to automatically respond to and mitigate DDoS attacks
 - Use AWS WAF as first line to monitor HTTP and HTTPS requests forwarded to protected web apps
 - Use AWS CloudFront for protection at the edge by content caching



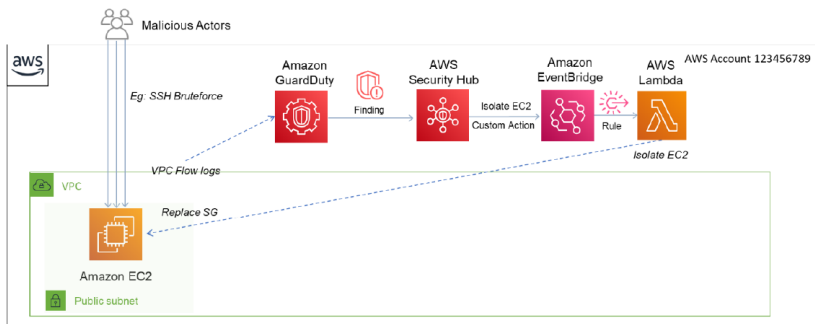
Inbound/Outbound network protection

- Use bastion host / NAT gateway for internet access from an instance in a private subnet.
- Use security groups to protect private and public subnets from potential threats from the ingress/egress traffic



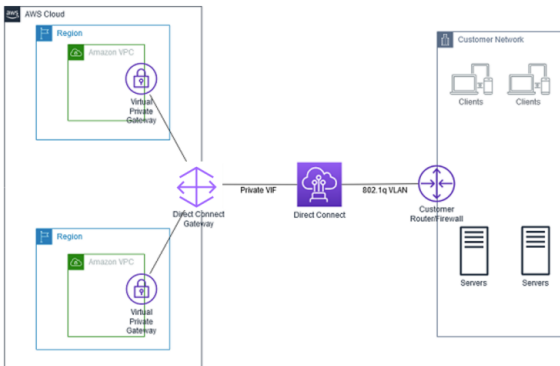
Logging and Monitoring

- Use VPC Flow Logs to monitor the ingress/egress traffic that reaches your VPC instances
- Use AWS Security Hub and AWS GuardDuty to check for malicious network accessibility from your VPC instances
- Use AWS Lambda to take immediate actions (e.g, isolate/delete instance).



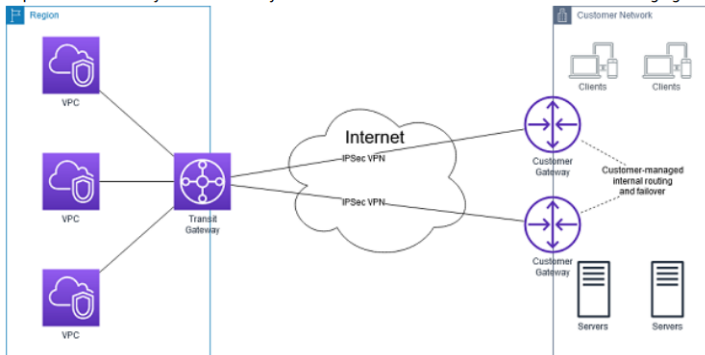
Remote Access Security

- Use Virtual Private Network or AWS Direct Connect to establish private connections from remote networks to VPCs
 - *AWS Direct Connect* helps to establish a dedicated connection between on-premises network to one or many VPCs in a single region (without/through a gateway)



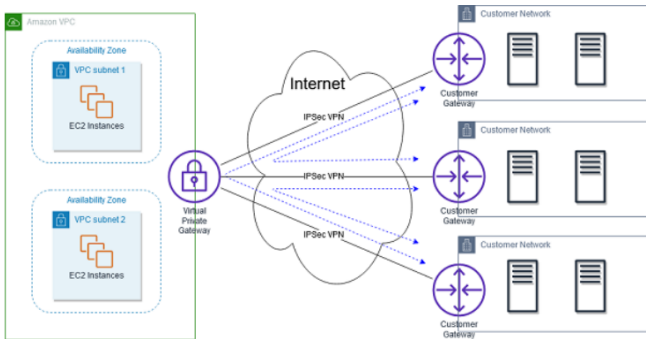
Remote Access Security

- Use Virtual Private Network or...(Next)
 - *AWS Transit Gateway* helps to interconnect VPCs and customer networks, allowing IPsec VPN connections or Direct Connect VPN connections.



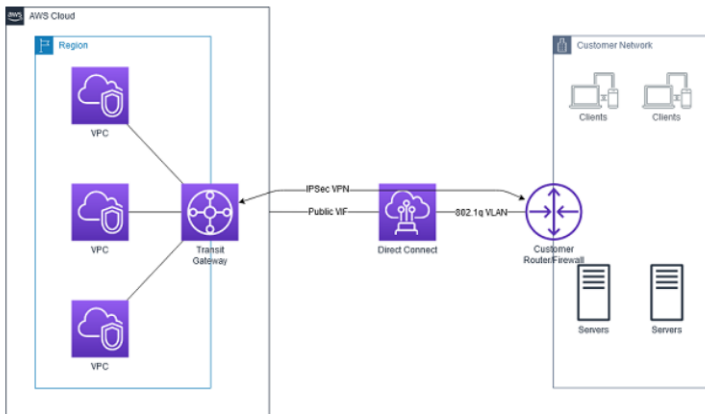
Remote Access Security

- Use Virtual Private Network or...(Next)
 - *AWS VPN CloudHub* is a low-cost hub-spoke model allowing secure primary/backup connectivity between multiple branch offices using a virtual private gateway with multiple customer gateways



Remote Access Security

- Use Virtual Private Network or...(Next)
 - *AWS Direct Connect + Transit Gateway + VPN* can be combined to minimize the cost and latency of IPsec VPN connections to multiple VPCs in the same region



Sondage 😊: <https://app.wooclap.com/XYLCCG>.

wooclap

VPC Management policies

- Help to define security policies to be applied on VPC and subnets
- Recall that an IAM policy specifies the effect (e.g., Allow, Deny), actions (e.g., ec2:CreateVPC) and resources (e.g., arn:aws:ec2:*:*:route-table/*).
- For example, the following policy allows one to create VPC and its associated subnets, routing tables, and internet gateways

```
"Statement": [{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateVpc",
    "ec2:CreateSubnet",
    "ec2:DescribeAvailabilityZones",
    "ec2:CreateRouteTable",
    "ec2:CreateRoute",
    "ec2:CreateInternetGateway",
    "ec2:AttachInternetGateway",
    "ec2:AssociateRouteTable",
    "ec2:ModifyVpcAttribute"
  ],
  "Resource": "*"
}]
```

VPC Management Policies

- Enforce an IAM policy to manage VPC resources (e.g., modification routing table, deleting internet gateway) given a purpose tag (e.g., test, dev, production)

```
{
  "Effect": "Allow",
  "Action": "ec2:DeleteInternetGateway",
  "Resource": "arn:aws:ec2:*:*:internet-gateway/*",
  "Condition": {
    "StringEquals": {
      "ec2:ResourceTag/Purpose": "Test"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:DeleteRouteTable",
    "ec2:CreateRoute",
    "ec2:ReplaceRoute",
    "ec2:DeleteRoute"
  ],
  "Resource": "arn:aws:ec2:*:*:route-table/*",
  "Condition": {
    "StringEquals": {
      "ec2:ResourceTag/Purpose": "Test"
    }
  }
}
```

Security Group policies

- Enforce an IAM policy to manage egress/ingress security groups attached to a VPC (create, update, modify, revoke)

```
"Statement": [{
  "Effect": "Allow",
  "Action": [
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
    "ec2:ModifySecurityGroupRules"
  ],
  "Resource": "arn:aws:ec2:region:account-id:security-group/*",
  "Condition": {
    "ArnEquals": {
      "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
    }
  }
}],
```

Remote Access Policies

- Enable an IAM policy to use AWS Direct Connect for secure Network to VPC communication

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": [  
      "directconnect:*",  
      "ec2:DescribeVpnGateways"  
    ],  
    "Resource": "*"   
  }  
]
```

- When the policy is enabled, we can now create a direct connect

```
aws directconnect create-connection --location us-east-1  
--bandwidth 5Gbps --connection-name "PolyStudent  
Connection"
```

Remote Access Policies

- Enable IAM policy to use AWS VPC Peering for secure VPC to VPC communication

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": "ec2:CreateVpcPeeringConnection",  
    "Resource": "arn:aws:ec2:region:account-id-1:vpc/*"  
  },  
  {  
    "Effect": "Allow",  
    "Action": "ec2:CreateVpcPeeringConnection",  
    "Resource": "arn:aws:ec2:region:account-id-1:vpc-peering-connection/*",  
    "Condition": {  
      "ArnEquals": {  
        "ec2:AcceptorVpc": "arn:aws:ec2:region:account-id-2:vpc/vpc-id"  
      }  
    }  
  }  
]
```

- When the policy is enabled, we can now create a VPC peering connection

```
aws ec2 create-vpc-peering-connection --vpc-id vpc1  
--peer-vpc-id vpc2
```

Logging policies

- Enable VPC flow logging on S3 buckets. Two actions are needed: *s3:PutObject* for write access and *s3:GetBucketAcl* for read access.

```
{
  {
    "Sid": "AWSLogDeliveryWrite",
    "Effect": "Allow",
    "Principal": {
      "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "my-s3-arn",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": account_id,
        "s3:x-amz-acl": "bucket-owner-full-control"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:logs:region:account_id:*"
      }
    }
  },
  {
    "Sid": "AWSLogDeliveryAclCheck",
    "Effect": "Allow",
    "Principal": {
      "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3:::bucket_name",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": account_id
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:logs:region:account_id:*"
      }
    }
  }
}
```


Traffic Mirroring policies

- Enforce IAM policy to allow the creation of a traffic mirror session for backup/redundancy and monitoring purposes

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": "ec2:CreateTrafficMirrorSession",  
    "Resource": [  
      "arn:aws:ec2:*:*:traffic-mirror-target/tmt-12345645678",  
      "arn:aws:ec2:*:*:traffic-mirror-filter/*",  
      "arn:aws:ec2:*:*:network-interface/*"  
    ]  
  }  
]
```

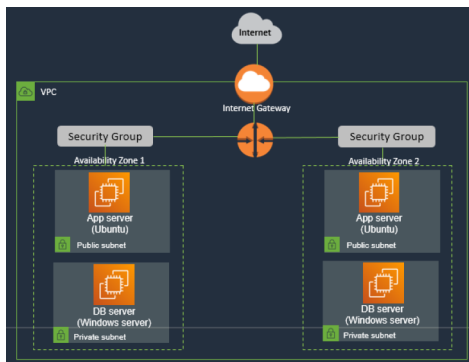
- When the policy is enforced, we can now create a traffic mirroring session
aws ec2 create-traffic-mirror-session --description "test backup" --traffic-mirror-target-id tmt-07feffffTest --network-interface-id eni-0702ffffffTest --session-number 1 --packet-length 25 --traffic-mirror-filter-id tmf-0436ffffffTest

Sondage 😊: <https://app.wooclap.com/XHDMKA>.

wooclap

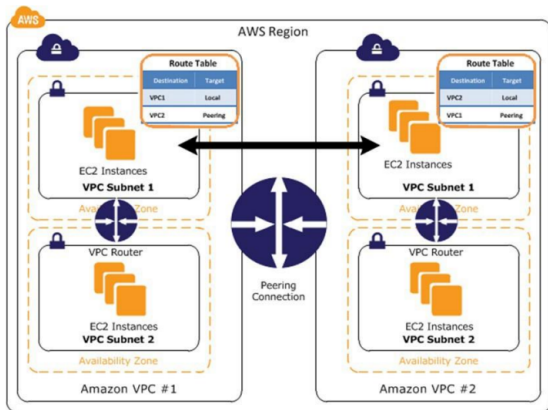
Availability Zones & Regions

- Use AWS Regions and Availability Zones (AZ) in the VPC infrastructure
- to allow multiple physically separated and isolated AZs connected with low-latency, high-throughput, and highly redundant networking



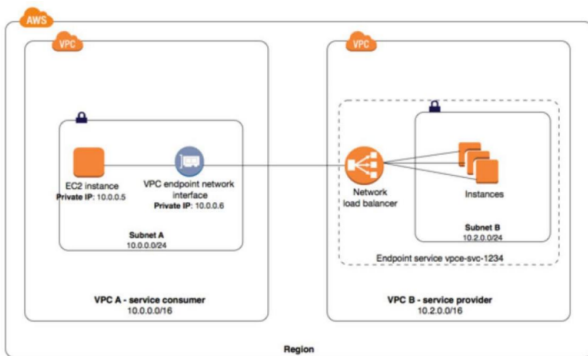
Data Replication

- Enforce replication/redundancy in one or multiple regions using VPC-to-VPC connectivity
 - *AWS VPC Peering* enables networking connection between two VPCs using their private IP addresses: no single point of failure, no network bandwidth bottleneck



Data Replication

- Enforce replication/redundancy in ... (Next)
 - *AWS PrivateLink* enables private connections between VPCs using interface VPC endpoints whose access can be made using AWS Direct Connect or managed using security groups



Sondage 😊: <https://app.wooclap.com/ASKIAD>.

wooclap

Audit Reports & Evidence

- Access audit reports using AWS Artifact such as Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, or ISO/IEC 27001:2013 reports
- Continuously collect evidence from AWS usage (VPC, S3, EC2, etc.) to simplify compliance with regulation/standards using AWS Audit Manager

AWS Audit Manager > Assessments > Create assessment

Step 1
Specify assessment details

Step 2
Specify AWS accounts in scope

Step 3
Specify AWS services in scope

Step 4
Specify audit owners

Step 5
Review and create

Specify AWS services in scope [info](#)

Choose the AWS services that this assessment collects evidence from.

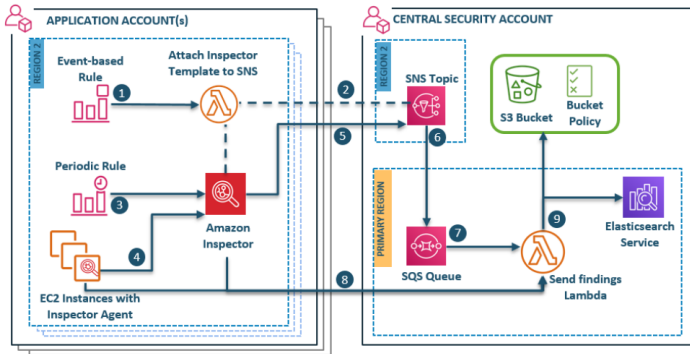
AWS services (11/11)

 < 1 >

<input checked="" type="checkbox"/>	AWS service	Category	Description
<input checked="" type="checkbox"/>	Amazon S3	Storage	Amazon Simple Storage Service (Amazon S3) is storage for the Internet.
<input checked="" type="checkbox"/>	Amazon Elastic Compute Cloud (Amazon EC2)	Compute	Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) Cloud.
<input checked="" type="checkbox"/>	AWS Lambda	Compute	AWS Lambda is a compute service that lets you run code without provisioning or managing servers.
<input checked="" type="checkbox"/>	AWS Identity and Access Management (IAM)	Security, identity, and compliance	AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS services.
<input checked="" type="checkbox"/>	AWS Single Sign-On	Security, identity, and compliance	AWS Single Sign-On (AWS SSO) is a cloud-based service that simplifies managing SSO access to AWS accounts and business applications.

Vulnerability Assessment

- Assess VPC, EC2 instances, and application configurations for exposure, vulnerabilities, and deviations from best practices using AWS Inspector



Vulnerability Logging & Monitoring

- Log and Monitor vulnerability findings from AWS Inspector agents to CloudTrail and CloudWatch

Amazon Inspector - Findings



Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. [Learn more.](#)

Add/Edit attributes

Last updated on February 3, 2019 1:40:49 AM (5m ago)



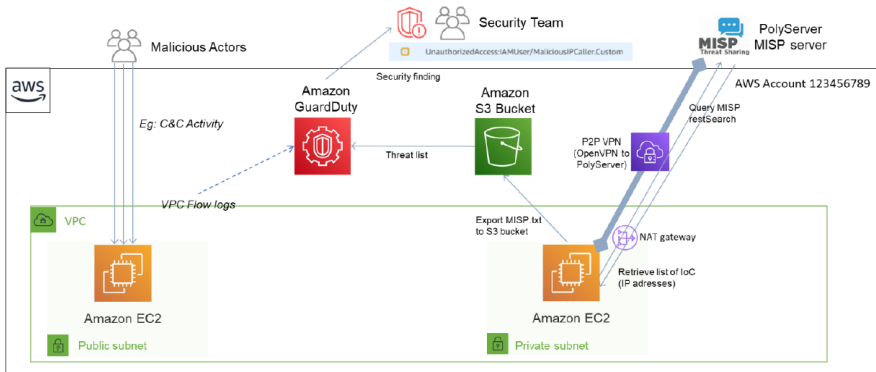
Filter

Viewing 1-6 of 6

<input type="checkbox"/>	Severity ⓘ	Date	Finding	Target	Template
<input type="checkbox"/>	Medium	Today at 1:2...	On instance i-0a9b5b8eb5bc156b7, TCP port 22 w...	Assessment-Targe...	Assessment-Temp..
<input type="checkbox"/>	Medium	Today at 1:2...	On instance i-04e36d2b75f057fb7, TCP port 22 wh...	Assessment-Targe...	Assessment-Temp..
<input type="checkbox"/>	Low	Today at 1:2...	On instance i-0a9b5b8eb5bc156b7, TCP port 80 w...	Assessment-Targe...	Assessment-Temp..
<input type="checkbox"/>	Low	Today at 1:2...	On instance i-04e36d2b75f057fb7, TCP port 80 wh...	Assessment-Targe...	Assessment-Temp..
<input type="checkbox"/>	Informational	Today at 1:2...	Aggregate network exposure: On instance i-0a9b5...	Assessment-Targe...	Assessment-Temp..
<input type="checkbox"/>	Informational	Today at 1:2...	Aggregate network exposure: On instance i-04e36...	Assessment-Targe...	Assessment-Temp..

Threat monitoring

- Continuously monitor AWS accounts, running resources (VPC Flow logs, EC2, S3) and generates detailed findings (alerts) about security postures on VPCs



Threat Detection

- From VPC Flow logs, GuardDuty checks the reputation of IP addresses and identify malicious IP of an EC2 instance (e.g., Backdoor CC activity).

The screenshot displays the AWS GuardDuty Findings console. The main view shows a list of findings with the following columns: Finding type, Resource, Last..., and Count. Two findings are listed, both of type 'Backdoor:EC2/C&CActivity:BDNS' and associated with 'Instance: i-05c110'. The first finding has a count of 3 and was detected 5 hours ago. The second finding has a count of 1 and was also detected 5 hours ago.

The right-hand pane provides details for the selected finding: 'Backdoor:EC2/C&CActivity:BDNS'. It includes a 'High' severity indicator and a description: 'EC2 instance i-05c110... is querying a domain name associated with a known Command & Control server.' Below this, there is an 'Investigate with Detective' link and an 'Overview' section with the following details:

Overview	
Severity	HIGH
Region	us-east-1
Count	3
Account ID	8129-...
Resource ID	i-05c...
Created at	05-04-2022 12:20:29 (4 hours ago)
Updated at	05-04-2022 12:25:16 (4 hours ago)

Sondage 😊: <https://app.wooclap.com/SFLUBI>.

wooclap