VECTRA®
Security that thinks.®

# Integration with AWS Security Hub

Cognito v5.4

AWS Security Hub is a service that provides a comprehensive view of high-priority security alerts and compliance status across all AWS accounts. These alerts may be originated by other AWS services like Amazon GuardDuty, Amazon Macie or Amazon Inspector, or by partner solutions like Vectra Detect.

In order to enable security analysts to quickly act on security incidents, Vectra Cognito publishes host scores to AWS Security Hub when a host's threat and certainty score exceed a customer-defined threshold.

The score, along with other details are published in the AWS Security Finding Format (ASFF), a sample of which is as follows:

## Schema for Vectra-generated Security Hub finding

```
{
 "SchemaVersion": "Vectra release-based",
 "Id": "Vectra Brain identifier",
 "ProductArn": "AWS ARN including AWS account ID",
 "GeneratorId": "host",
 "AwsAccountId": "AWS account ID",
 "Types": [
  "Unusual Behaviors/Network Flow"
 ],
 "CreatedAt": "First host alert timestamp",
 "UpdatedAt": "Latest host alert timestamp",
 "Severity": {
  "Product": Normalized Score divided by 10,
  "Normalized": Normalized score for Vectra host based on Threat and Certainty
 },
 "Confidence": Certainty score of Vectra Host
 "Criticality": Threat score of Vectra Host,
 "Title": "Vectra Cognito Detect: hostID - thresholds",
 "Description": "Cognito host alert for hostID",
 "SourceUrl": "URL to Vectra Host in the Cognito UI",
 "ProductFields": {
  "aws/securityhub/FindingId": " Security Hub finding ID",
  "aws/securityhub/SeverityLabel": "Mapping",
  "aws/securityhub/ProductName": "Detect",
  "aws/securityhub/CompanyName": "Vectra"
 },
 "Resources": [
  {
    "Type": "AwsEc2Instance",
    "Id": "AWS Resource Name",
    "Details": {
      "Other": {
        "Hostname": "Vectra hostID"
      }
    }
  }
 ],
 "WorkflowState": "New",
 "RecordState": "Active"
}
```

Vectra posts findings only for AWS hosts, not on-premise hosts monitored by the Vectra Brain.

The scoring for a host is automatically updated when there are changes.

### Severity Mapping

The severity mapping that Vectra reports to Security Hub is derived as a function of Vectra’s threat score and certainty score for the host.

| Vectra Threat Score | Vectra Certainty Score | AWS Security Hub severity |
|---|---|---|
| 0 | 0 | Informational |
| <50 | <50 | Low |
| <=50 | >50 | Medium |
| >50 | <=50 | High |

| | | |
|---|---|---|
| >50 | >50 | Critical |

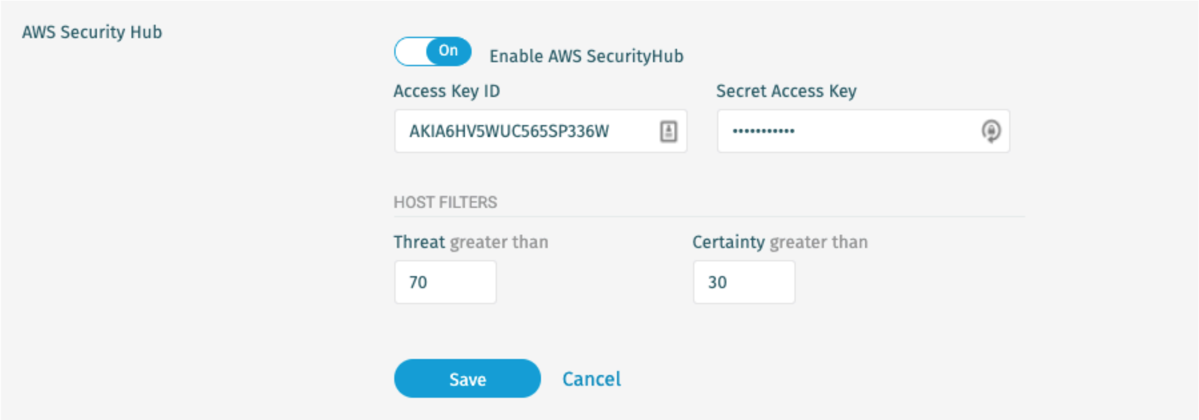
## Configuration

To configure the Vectra Brain to publish findings to AWS Security Hub, log in to the Vectra Brain.

AWS Security Hub requires the AWS External Connector is configured for Host identification of AWS ec2 instances.  Navigate to External Connectors tab under Settings.  If not currently configured, then configure AWS connector for Host ID.  Refer to the AWS Sensor Deployment guide for details.

Navigate to the Notifications tab under Settings.

Click Edit against AWS Security Hub.



AWS Security Hub

On Enable AWS SecurityHub

Access Key ID: AKIA6HV5WUC565SP336W

Secret Access Key: •••••••••••

HOST FILTERS

Threat greater than: 70

Certainty greater than: 30

- Enable AWS Security Hub
- Add an Access Key ID and Secret Key Access for a user role with the required privileges to post findings to AWS Security Hub.
- Select the thresholds above which hosts findings should be published to AWS Security Hub.
- Click Save