CSV Manager for Security Hub

Overview

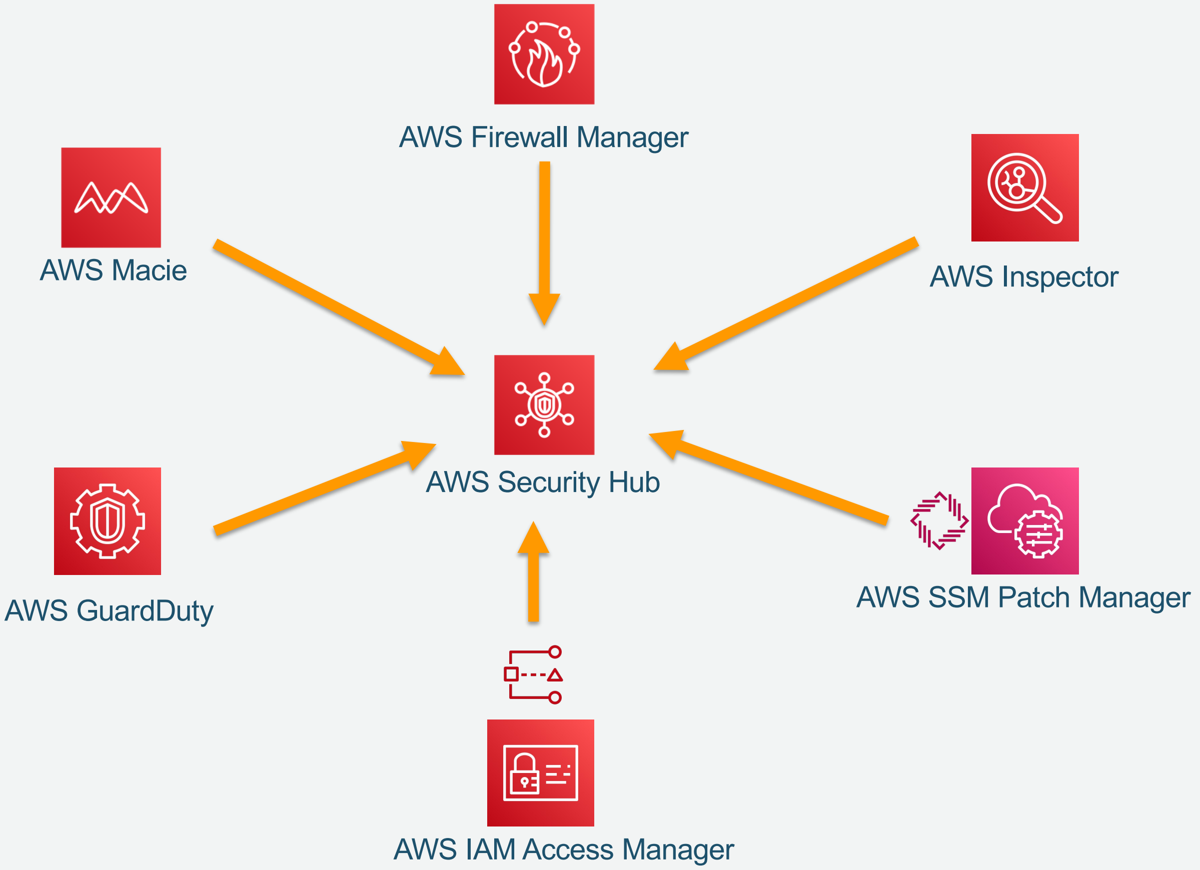
February 11, 2022

AndyRobinson
nandrob@amazon.com

Agenda

- Security Hub Overview
- Why CSV Manager for Security Hub?
- CSV Manager for Security Hub CSV Files
- Periodic Exports
- Unscheduled Exports
- Imports

Security Hub Overview



aws professional services

Why CSV Manager for Security Hub?

- Thousands or tens of thousands of findings
- Many are spurious, duplicates, or expected
- Limited web UI
- CSV Manager for Security Hub Export output easily analyzed
- CSV Manager for Security Hub Update allows mass updates

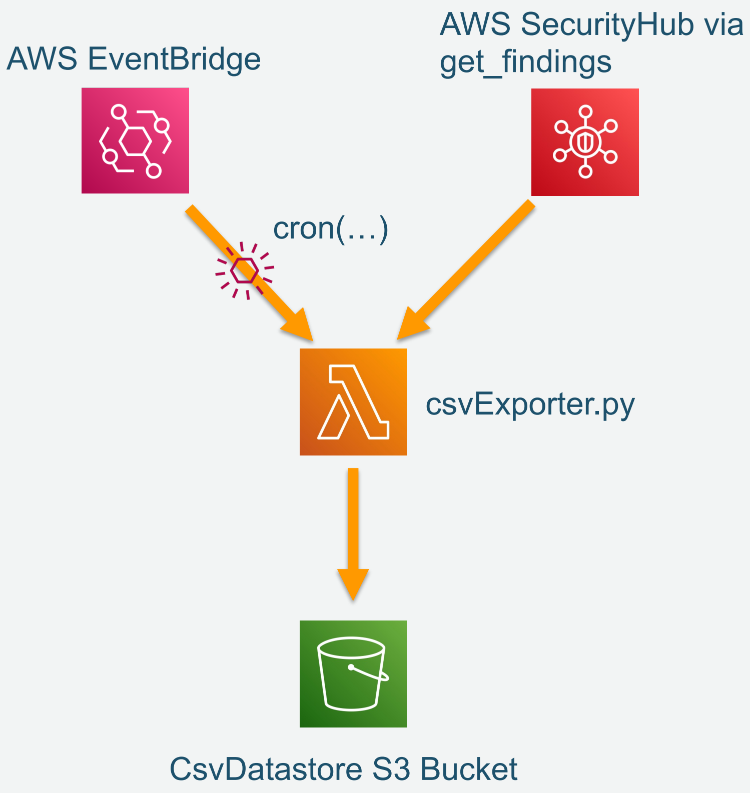
CSV Manager for Security Hub CSV Files

- Security Hub findings are large JSON objects
- Export produces comma-separated values (CSV) file
- Flattens each finding into 37 columns (currently)
- Suitable for database import
- 12 columns can be updated
- Edit with Excel, text editor, etc.

Periodic Exports

- ➢ Configured by updating ShfxExtractor stack Frequency Parameter e.g.

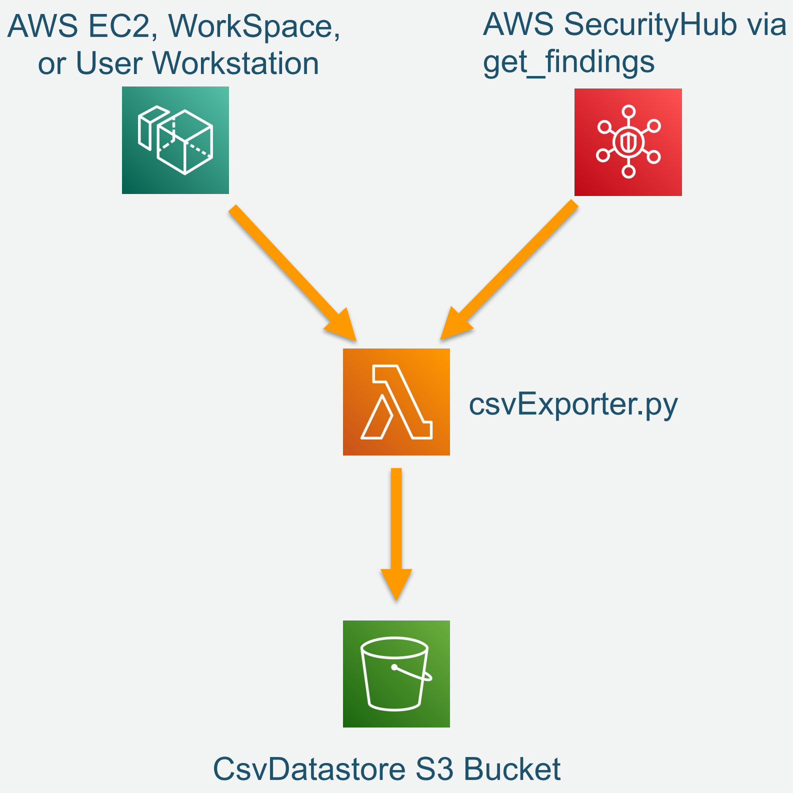
  cron(0 8 ? * SUN *)
- ➢ AWS EventBridge rule triggers csvExporter.py as AWS Lambda function
- ➢ Findings obtained using Security Hub get_findings API
- ➢ Output CSV written to S3 bucket defined in the CsvDatastore stack



aws professional services

Unscheduled Exports

- ➢ Run as a command from a workstation with AWS CLI, Boto3, and Python 3
- ➢ Can also be run as a Lambda or using an SSM Automation
- ➢ Findings obtained using get_findings API
- ➢ Output CSV written to S3 bucket defined in the CsvDatastore stack
- ➢ Can be run whenever required, with whatever filters are needed



AWS EC2, WorkSpace, or User Workstation

AWS SecurityHub via get_findings

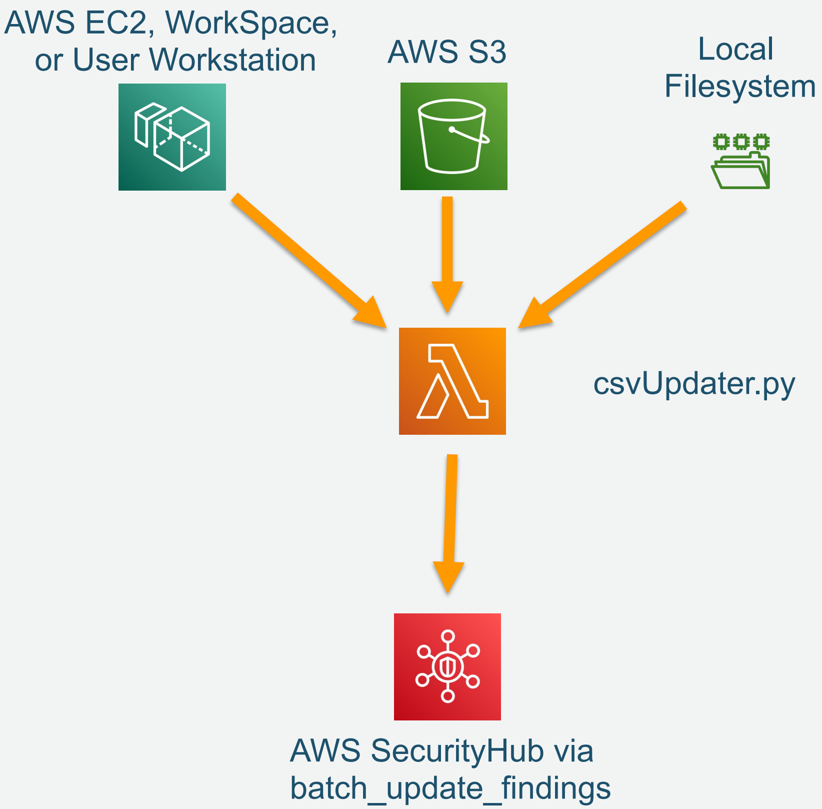
csvExporter.py

CsvDatastore S3 Bucket

aws professional services

Imports

- ➢ Run as a command from a workstation with AWS CLI, Boto3, and Python 3
- ➢ Run as a Lambda or from an SSM automation
- ➢ Input CSV read from any S3 bucket *or* from a local file
- ➢ Uses batch_update_findings API to update SecurityHub
- ➢ Should always run unscheduled export first, and modify that CSV for import



AWS EC2, WorkSpace, or User Workstation

AWS S3

Local Filesystem

csvUpdater.py

AWS SecurityHub via batch_update_findings

Questions, Discussion & Next Steps

aws professional services