AWS & Splunk “Take Action” Playbook: Identify & Resolve Security Incidents with Splunk, Phantom, AWS Security Hub and AWS Services

Scott Ward
Principal Solutions Architect | Amazon Web Services

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Problem statements

Backlog of compliance requirements

1. Many compliance requirements, and not enough time to build the checks

Too many security alert formats

2. Dozens of security tools with different data formats

Too many security alerts

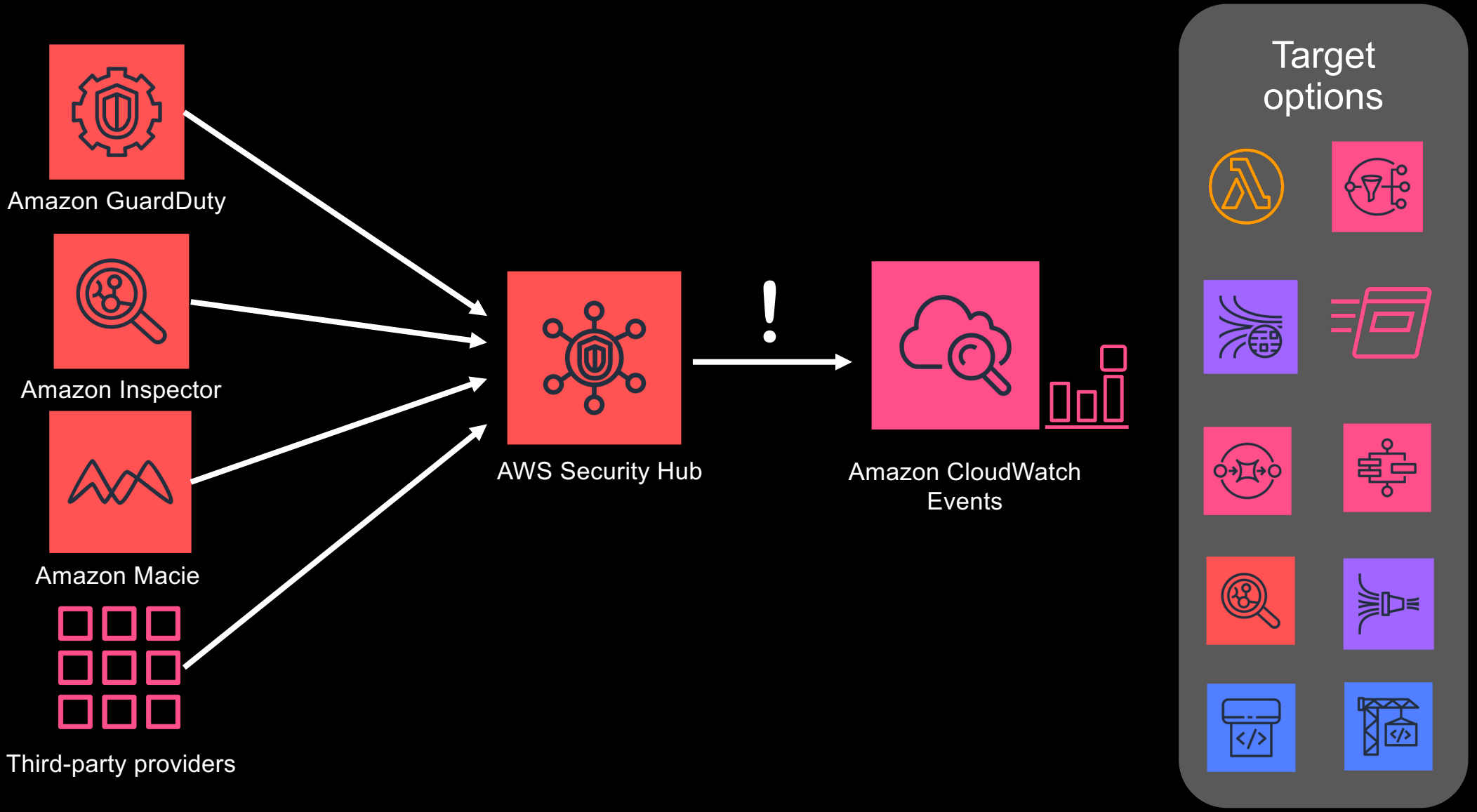
3. Large volume of alerts, and the need to prioritize and take action

Lack of an integrated view

4. Lack of an integrated view of security and compliance across accounts

Security Hub overview

Taking action with AWS Security Hub



Splunk Placeholder Slide

- Splunk to add integration slide

Demo

.conf19

splunk>

Thank You!