
AWS
re:Invent

SEC307

Using Amazon GuardDuty and AWS Security Hub to secure multiple accounts

Annam Iyer

Solutions Architect

AWS

AWS re:Invent

Agenda

GuardDuty overview

GuardDuty demo

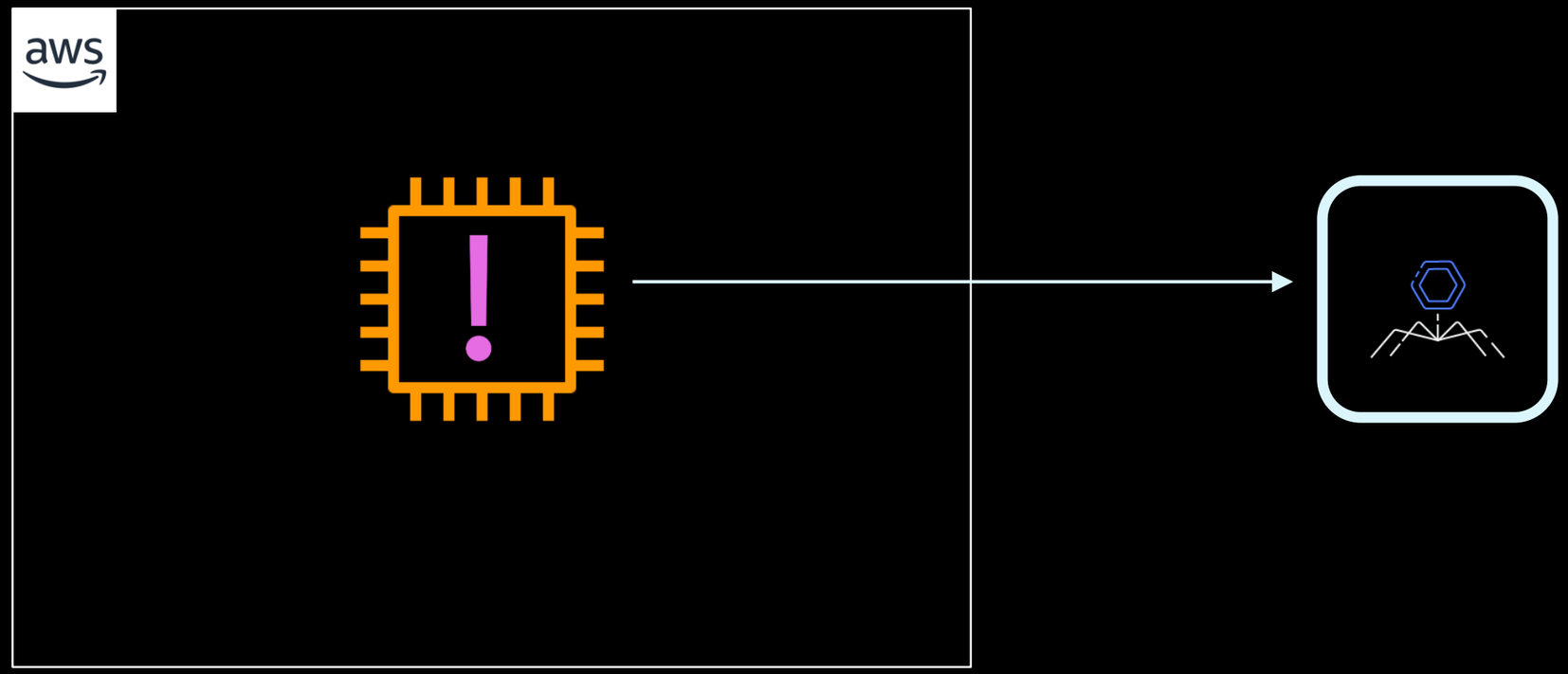
Security Hub overview

Best practices across accounts

Security Hub demo

AWS accounts over time

For example...

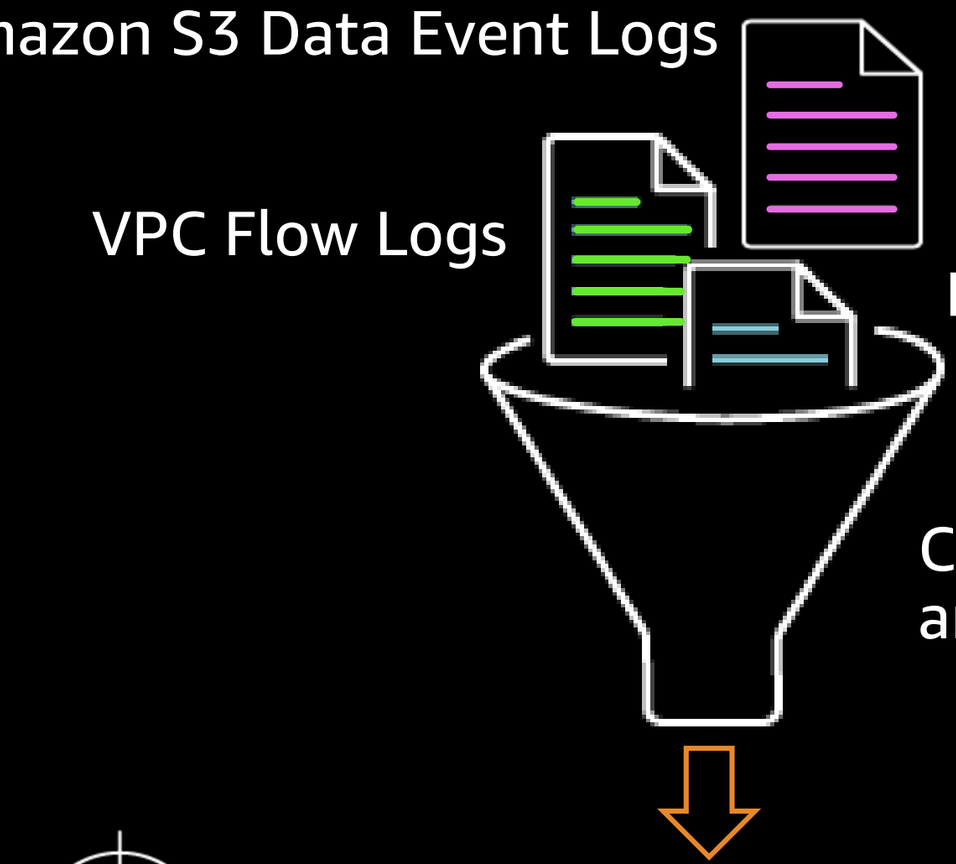


How do you find the anomalous instance?

How do I enable threat detection at scale?

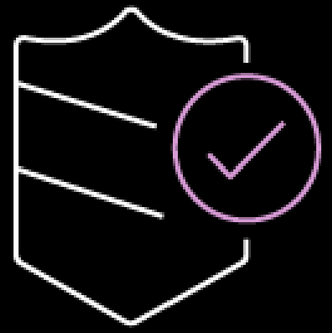
AWS re:Invent

Enable Amazon GuardDuty



Intelligently detect security
risks using machine learning
and anomaly detection

GuardDuty as a threat detection tool



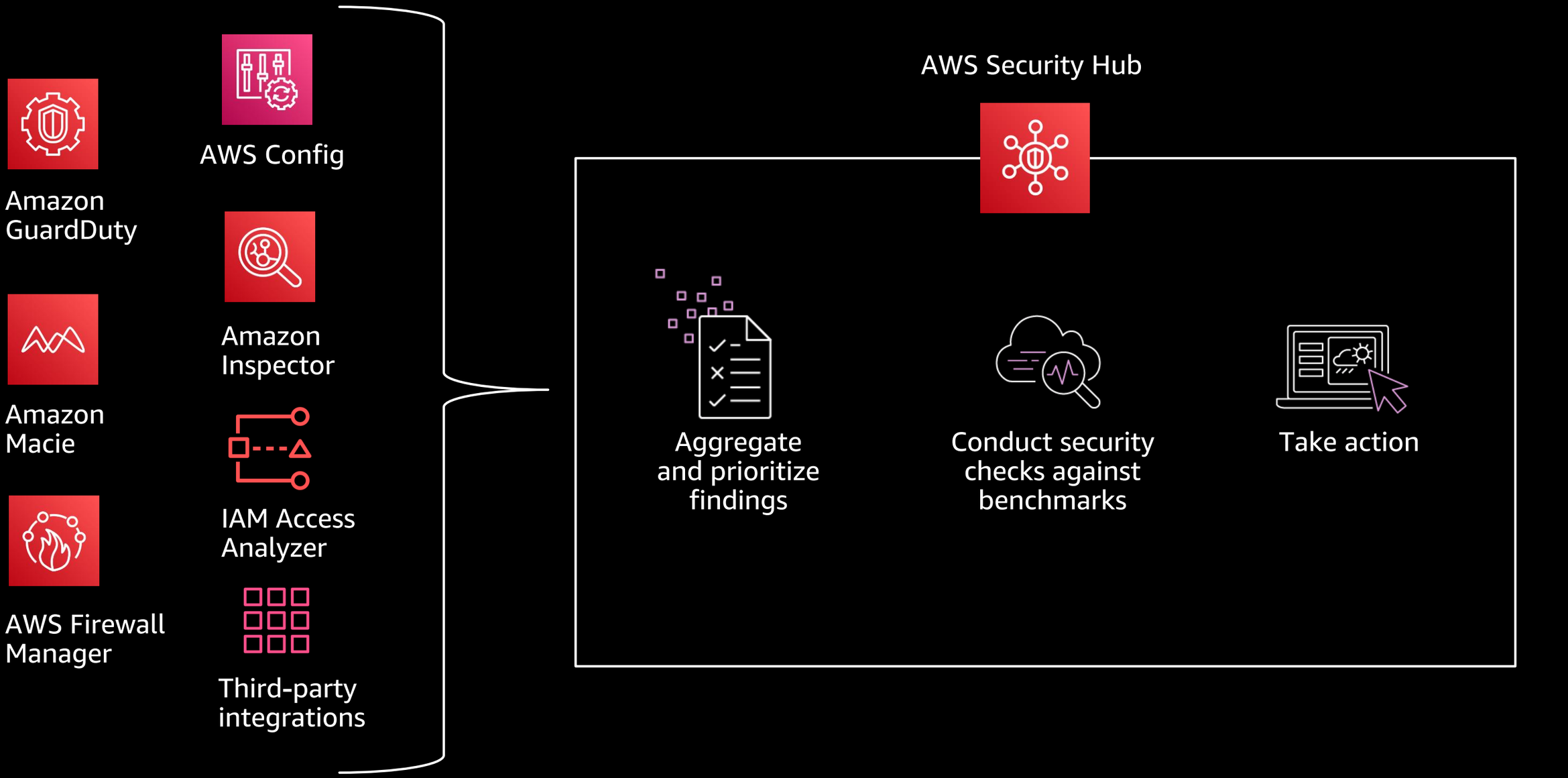
Single-click enablement and fully managed

Continuously monitors account usage and behavior

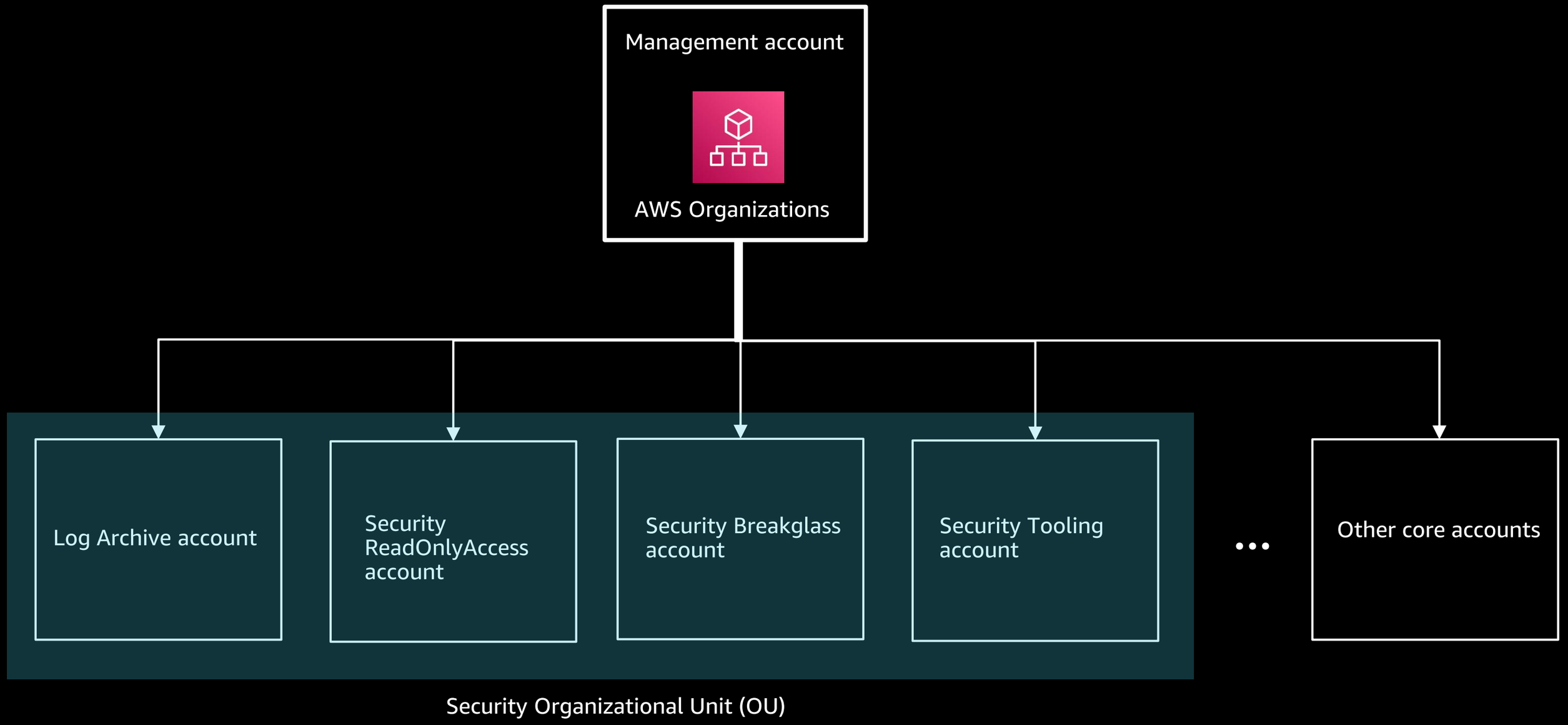
Uses ML to learn and evolve

How do I monitor threat detection with a single pane of glass?

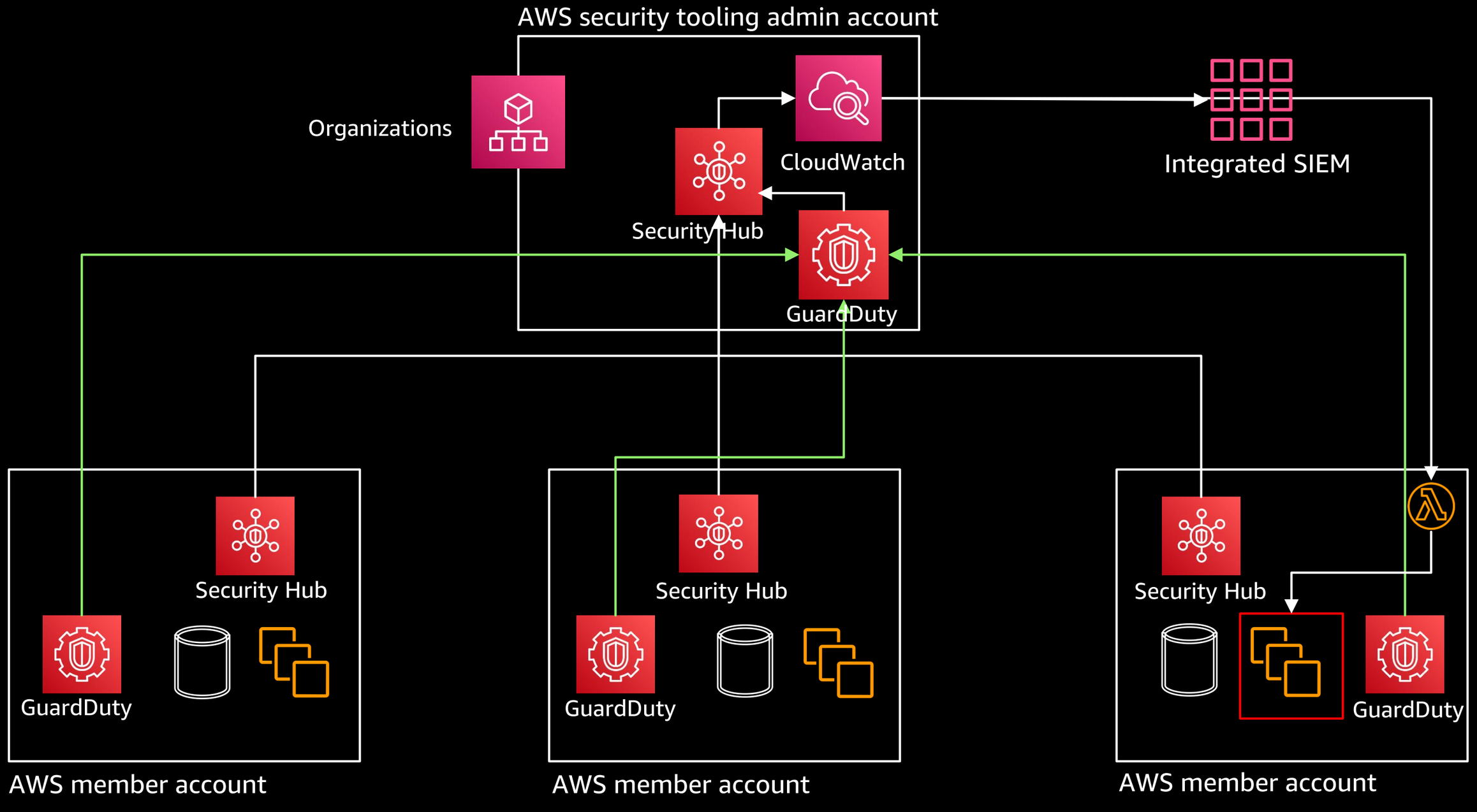
Enable Security Hub



Multi-account strategy with Security OU



Architecture with multi-account strategy



Security Hub as a central dashboard

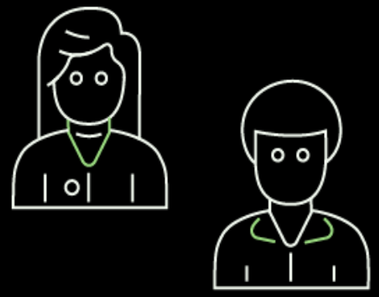
Centralize and prioritize findings without needing to normalize

View security and compliance posture against key standards

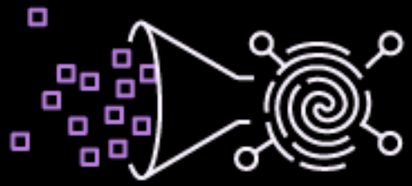
Take automated action on findings through CloudWatch Events

Key takeaways

Security tools available
in a singular destination



Decrease the burden
for the security team



Services work at scale
with a click of a button

Thank you!

AWS re:Invent

Please complete the session survey

AWS re:Invent