Top 5 use cases of AWS detection and response services

1. Threat detection and workload protection
   - Protect your workloads, applications, and data against security risks—equip your organization with security solutions that continuously detect and respond to security risks. Enlist Amazon Web Services (AWS) detection and response services to manage and mitigate security risks so you and your teams can focus on accelerating innovation.

2. Automated and continual vulnerability management at scale
   - Discover and protect workloads and data to meet your compliance obligations.

3. Unified security data management
   - Leverage AWS to consolidate and analyze security-related data and facilitate broader visibility. IPG created a security data lake to centralize security-related data from AWS and third-party sources while retaining full control and ownership over data.

4. Risk management
   - Continuously detect and remediate cloud resource misconfigurations and compliance risks to achieve continuous cloud security posture management (CSPM). Southwest Airlines successfully deployed AWS detection and response services to gain higher visibility into the airline’s security operations.

5. Threat intelligence
   - Enable immediate action on vulnerability findings—automate patch management to quickly route issues to appropriate teams. HelloSign upgraded its security with AWS and saved $1 million annually in triage time for security operations, staffing, and licensing costs.

Protect your workloads against security risks with AWS

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.