IBM Security QRadar SOAR

Automated intelligent security response across your hybrid environment

Challenges of securing a hybrid infrastructure

As a business grows, it's essential that cyber security scales accordingly. This becomes increasingly important as a company begins their cloud migration journey. As more users and systems are added to the infrastructure, having visibility into all the endpoints becomes more important, and more challenging.

Adding new security tools to the mix can offer some short-term relief, but without a centralized solution that works across the entire IT landscape, it becomes difficult to manage. With so much incoming information from the various tools, it's harder to filter out the noise to discern where and how actions need to be taken. Meanwhile, new regulatory deadlines for incident reporting are shorter than ever. Organizations need to respond quickly and decisively when security breaches occur.

60% of security leaders don't have a holistic, well documented cloud strategy

Source: Forrest Opportunity Snapshot

$4m Is the average cost of a data breach

Source: 2021 Cost of a Data Breach Report from IBM and Ponemon Institute

Work smarter and faster with automation

With IBM Security QRadar Security Orchestration, Automation and Response (SOAR), security teams can increase efficiency with a security automation and response solution that integrates tightly with existing security tools across the hybrid IT infrastructure. This integration helps mitigate the duration and impact of cyberattacks with intelligent automation, enabling immediate analyzation and automated responses that get the right team involved to quickly resolve it. IBM Security QRadar SOAR gives the security team flexibility to assign cases to the right members of the security team, while other analysts remain focused on higher priority investigations. Detailed information about the alert is then saved for further analysis and refinement of incident playbooks.

Respond

Accelerate Incident Response
Industry and organizational knowledge is combined into incident playbooks, ensuring rapid response by an empowered security team.

Automate

Orchestrate Responses to automate manual tasks, prioritize analyst workload and reduce remediation time of complex security threats.

Collaborate

Coordinate Information Sharing across the organization, ensuring optimal use of resources and full visibility for all stakeholders.

Respond confidently to cyber threats

IBM Security QRadar SOAR helps guide and empower security teams with knowledge and automation. Analysts can respond rapidly to security incidents, armed with the information and tools to resolve and learn from each incident. Custom integration with your existing infrastructure consolidates incident response to a single pane of glass, dramatically improving response times and easing the sharing of information.

Optimize response protocols

Leverage orchestration to enable quick responses to security alerts, thereby mitigating the impact of cyberattacks. Reduce response times by replacing menial tasks with automation.

Collaborate with consistency

Get the right information to the right people at the right time. Robust case management enables end-to-end visibility and information sharing across the organization.

Initiate more dynamic responses

Codify established incident response processes into dynamic playbooks, enabling consistent responses to threats such as malware, ransomware and phishing. Processes can be built upon and updated as new cyberattacks emerge.

Customer success story: TalkTalk

Challenges

A large broadband provider with disparate legacy applications needed to consolidate and bolster its security infrastructure as the business continued to grow.

Solution

Working with IBM, TalkTalk integrated the IBM Security QRadar SOAR platform with their existing infrastructure, centralizing their incident response.

Results

8x faster resolution time for security incidents, along with a centralized hub affording greater transparency across their organization and stakeholders.

IBM Security QRadar SOAR on the AWS Cloud

IBM Security QRadar SOAR offers a growing list of integrations with services on the AWS Cloud, including Amazon GuardDuty, Amazon CloudWatch, Amazon Elastic Compute Cloud (Amazon EC2), AWS Security Hub, Amazon Simple Storage Service (Amazon S3), Amazon Route 53 and AWS CloudTrail.

Whether you are migrating to the AWS Cloud or are already operating in the AWS Cloud, IBM Security® is trusted in cloud security, delivering not only leading solutions to secure the AWS Cloud or hybrid deployments but expert services to develop, implement and scale lasting security strategies, while complementing AWS-native controls and services.

Get started with IBM Security QRadar SOAR on the AWS Cloud

Learn more at https://www.ibm.com/qradar/security-qradar-soar or on the AWS Marketplace