DATA SHEET

RSA Archer® Security Operations & Breach Management

Use case for IT & Security Risk Management

The challenge

Security breaches continue to make front page news. The identification of and response to a security incident are the first line of defense against a significant business event. Many organizations have deployed security operations that are managed through spreadsheets, email, and intranets or other shared portal solutions. Inconsistent operational procedures for handling security incidents and manual processes for managing shifts in the security operations center (SOC) can weaken the overall process to the point that it breaks down when you need it most, namely, during a breach.

Data breaches, compliance violations, and missed threats are some of the more obvious negative consequences of poorly executed security operations. Mismanaged processes and procedures within the operations center can lead to missed security events, outstanding issues, unclear lines of ownership for remediating gaps, and ineffective prioritization IT operations. The lack of a defined process will consistently lead to higher costs associated with remediating security incidents. In addition, when there is a significant breach or data compromise, the impact of that incident must be analyzed and escalated appropriately to ensure the right people are engaged. Effective breach management involves multiple parties working together to handle the event. Without a clear plan, a serious event can turn into a catastrophe.

Overview

RSA Archer Security Operations & Breach Management enables you to centrally catalog organizational and IT assets, to establish a full business context overlay to drive incident prioritization. Built-in workflows and reporting for security incidents enable security managers to stay on top of the most pressing issues. Best practices and procedures for incident handling help security analysts effectively and efficiently triage alerts. Any issues related to incident investigations can be tracked and managed in a centralized portal, enabling full visibility and reporting. Finally, the security operations manager can effectively monitor key performance indicators, measure control efficacy, and manage the overall SOC team.

With RSA Archer Security Operations and Breach Management, the incident response process to address security events and incidents is integrated into a broader, more mature approach to managing security operations. Clear process workflow and insight into security incident velocity allows the SOC manager to better utilize the security team's time and resources, resulting in faster response,

Key features

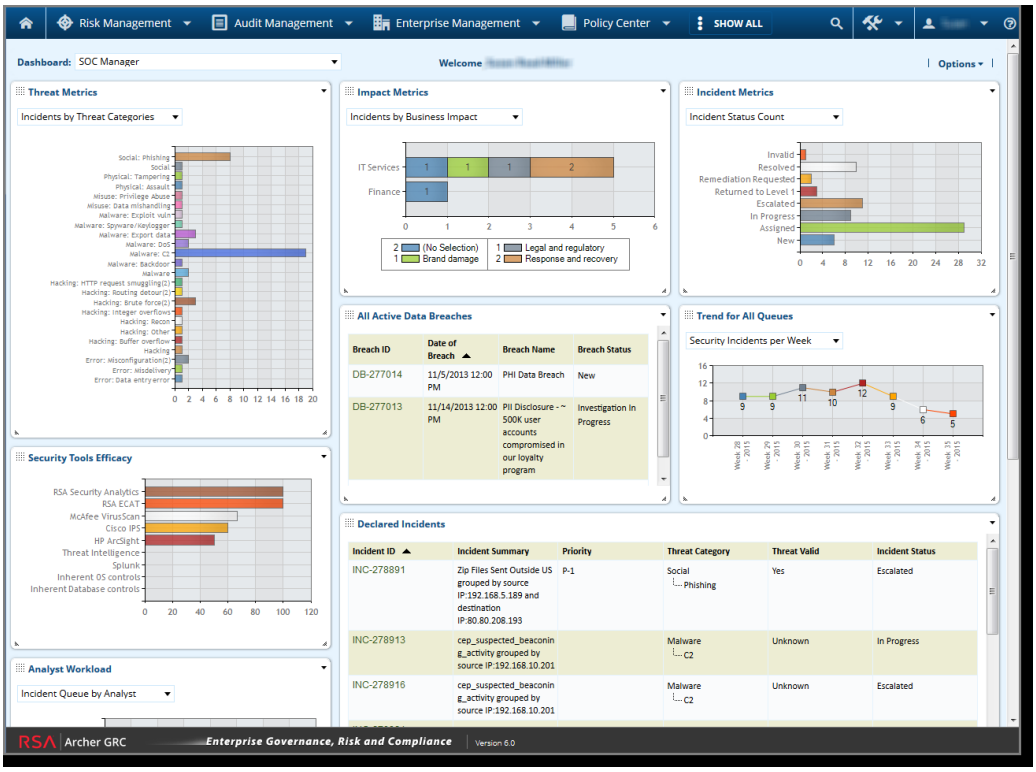
- Centralized catalog of organizational and IT assets
- Central repository and taxonomy for security alerts and integration with SIEM/log/packet capture infrastructure
- Breach risk assessments
- Defined security incident response procedures
- SOC management tools including notifications, control efficacy monitoring, key performance indicators (KPIs), staffing management and shift turnover
- Issues management for IT operations

Key benefits

With RSA Archer Security Operations and Breach Management, you will see:

- Reduced time and effort for SOC staff to escalate and respond to security alerts
- Stronger posture for breach response readiness
- Lower security risk

analysis, and closure rates for critical security incidents. With improved processes and capabilities, the security team can leverage existing SIEM / log / packet capture resources to focus on the most impactful incidents. It also strengthens the ability to respond effectively to potential data breaches, increasing the return on those infrastructure investments while lowering overall security risk.



For more information

To learn more about how RSA products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at **www.rsa.com**. If you are an existing RSA Archer customer and have questions or require additional information about licensing, please contact RSA Archer at **archersupport@rsa.com** or call 1-888-539-EGRC.

About RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to **rsa.com**.