DATA SHEET

RSA Archer® Security Incident 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 possible security incident are the first line of defense against a significant business event. Many organizations have deployed security information and event management (SIEM) and log collection tools in their infrastructure to track events and provide alerts. Unfortunately, these systems produce an overwhelming amount of data for the security team to review. Lack of a sound process for prioritizing actionable security events, combined with manual, inconsistent response procedures, increases the overall risk that the organization will not effectively respond in time. Poor handoffs to IT operations leave little if any visibility into remediation efforts to close security incidents.

Data breaches, compliance violations and missed threats are some of the more obvious negative consequences of a poorly implemented incident response process. Incomplete documentation of known incidents can lead to missed security events, ongoing unaddressed issues, unclear lines of ownership for remediating gaps and ineffective prioritization for IT operations. The lack of a defined process will consistently lead to higher costs associated with remediating security incidents.

Overview

RSA Archer® Security Incident Management enables you to address security alerts through managed processes designed to effectively escalate, investigate and resolve security incidents. Organizational and IT assets can be centrally cataloged with a full business context overlay to drive appropriate prioritization of security events. Built-in workflows streamline the process and enable teams to work effectively through their defined incident response and triage procedures. Any issues related to incident investigations can be tracked and managed in a centralized portal to enable full visibility and reporting.

With RSA Archer Security Incident Management, security events and incidents are escalated quickly and consistently. Clear process workflow and insight to security incident velocity allow more effective utilization of the security team's time, resulting in faster response, 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, increasing the return on those infrastructure investments while lowering overall security risk.

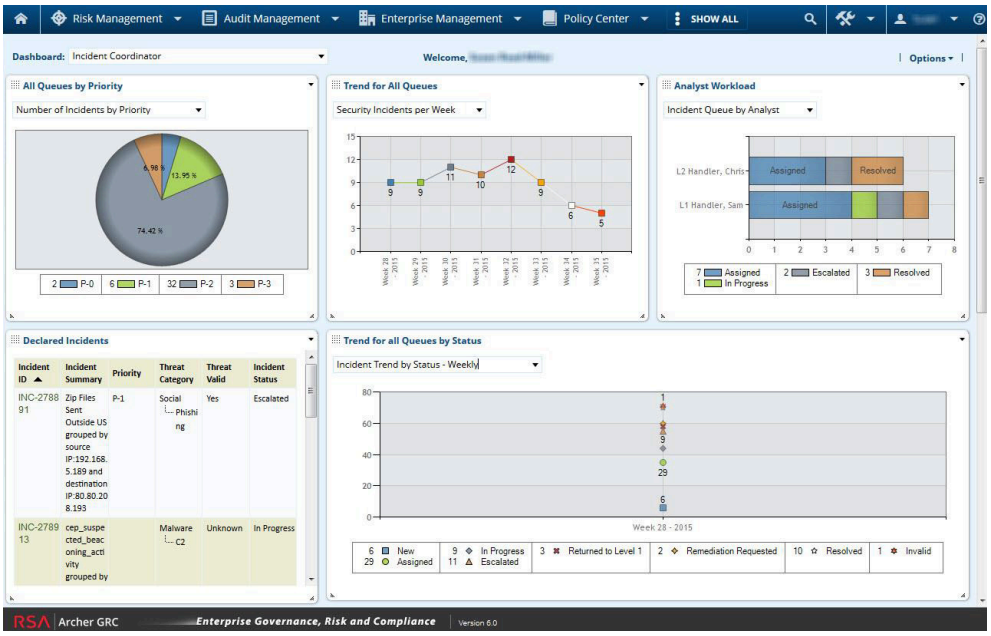
Key Features

- Centralized catalog of organizational and IT assets
- Central repository and taxonomy for security alerts and integration with SIEM/log/packet capture infrastructure
- Full incident response lifecycle support with multiple layers of workflow, escalation and response procedures
- Investigation support including incident journals and forensic analysis tracking
- Issues management for IT operations

Key Benefits

With RSA Archer Security Incident Management, you will see:

- Reduced time to escalate and respond to security alerts
- Less effort to triage and remediate incidents
- Accurate, consolidated incident analysis and reporting



For more information

RSA offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high risk world. For more information, go to rsa.com.