THE CHALLENGE

Cyber and security breaches continue to make front page news. The identification of potential security issues and the response process to a possible cyber incident are the first lines 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. These systems produce an overwhelming amount of data for the security team to review and security response processes that are managed through spreadsheets and email can quickly raise the overall risk that the organization does not respond effectively or in time.

Lack of sound methods to prioritize actionable security events, combined with manual, inconsistent operational response procedures, increases the overall risk that the organization will not effectively respond in time. Poor handoffs between security functions and IT teams leave little visibility into remediation efforts to close declared cyber incidents and can weaken the overall process to the point that it breaks down when needed most, namely during a breach.

OVERVIEW

RSA Archer® Cyber Incident and Breach Response enables you to centrally catalog organizational and IT assets, establishing business context to drive incident prioritization and implement processes designed to escalate, investigate and resolve declared incidents effectively. The use case is designed for teams to work effectively through their defined incident response and triage procedures and prepare for data breaches.

Built-in workflows and reporting are designed for security managers to stay on top of the most pressing issues and streamline processes. Issues related to a declared incident investigation can be tracked and managed in a centralized portal, enabling full visibility and reporting. If an incident escalates into a data breach, prebuilt workflows and assessments are designed to help the broader business team work with your security team to respond appropriately.

With RSA Archer Cyber Incident and Breach Response, declared cyber and security events get escalated quickly and consistently. Advanced workflow and insight to declared cyber and security incidents velocity allow more efficient utilization of security team resources, resulting in faster response, analysis and closure rates for critical security incidents. With improved processes and capabilities, the security team can more effectively leverage existing infrastructure, such as SIEMs, log and packet capture tools, and endpoint security technologies, to focus on the most impactful incidents. These capabilities improve security team preparedness in the case of serious incidents involving potential data breaches, increasing the return on infrastructure investments while lowering overall security risk.
KEY FEATURES

- Centralized catalog of organizational and IT assets
- Defined incident response lifecycle support with advanced workflow, escalation and response procedures
- Central repository and taxonomy to manage processes related to security alerts
- Integration with SIEM/log/packet capture infrastructure
- Investigation support including incident journals and forensic analysis tracking
- Issues management for IT operations
- Breach risk assessments

KEY BENEFITS

RSA Archer Cyber Incident and Breach Response is designed to:

- Reduce effort to triage and remediate incidents
- Improve accuracy of consolidated incident analysis and reporting
- Reduce time and effort for SOC staff to escalate and respond to security alerts
- Improve posture for breach response readiness
- Lower security risk