RSA® ARCHER® SICHERHEITSABLÄUFE UND MANAGEMENT VON SICHERHEITSVERLETZUNGEN

Anwendungsbeispiel für IT- und Sicherheitsrisikomanagement

Die Herausforderung

Sicherheitsverletzungen sorgen immer wieder für Schlagzeilen. Die Identifizierung von und Reaktion auf Sicherheits-Incidents stellen die erste Verteidigungslinie gegen ein bedeutendes Geschäftsereignis dar. Viele Unternehmen haben Sicherheitsabläufe eingeführt, die über Tabellen, E-Mails, das Intranet oder andere gemeinsam genutzte Portale verwaltet werden. Inkonsistente Betriebsverfahren zur Handhabung von Sicherheits-Incidents und manuelle Prozesse für das Management von Veränderungen im SOC (Security Operations Center) können den Gesamtprozess derart schwächen, dass er im Notfall – also während einer Sicherheitsverletzung – versagt.

Datenschutzverletzungen, Verstöße gegen Compliancevorschriften und übersehene Bedrohungen sind nur einige der auf der Hand liegenden negativen Konsequenzen von mangelhaften Sicherheitsabläufen. Schlecht ausgeführte Prozesse und Verfahren im Operations Center können zu übersehenen Sicherheitsereignissen, offenen Punkten, unklaren Verantwortlichkeiten für die Schließung von Lücken und einer ineffektive Priorisierung von IT-Abläufen führen. Das Fehlen eines festgelegten Prozesses wird konsequenterweise zu höheren Kosten bei der Behebung von Sicherheits-Incidents führen. Darüber hinaus muss, sofern keine ernsthafte Verletzung oder Datenkompromittierung stattgefunden hat, die Auswirkung dieses Incident entsprechend analysiert und eskaliert werden, damit der Fall an die geeigneten Personen weitergeleitet werden kann. Am effektiven Management von Sicherheitsverletzungen sind mehrere Parteien beteiligt, die dieses Event gemeinsam bearbeiten. Ohne einen klaren Plan kann sich ein Event zu einer echten Katastrophe auswachsen.

Übersicht

RSA® Archer® Sicherheitsabläufe und Management von Sicherheitsverletzungen ermöglicht Ihnen die zentrale Katalogisierung von Unternehmensressourcen und IT-Ressourcen, damit Sie den vollständigen Unternehmenskontext bestimmen und Incidents priorisieren können. Integrierte Workflows und Reportingfunktionen für Sicherheits-Incidents geben Sicherheitsmanagern die Möglichkeit, den Überblick über die dringendsten Probleme zu behalten. Best Practices und Verfahren für den Umgang mit Incidents helfen Sicherheitsanalysten dabei, Warnmeldungen effektiv und effizient zu sichten. Probleme im Zusammenhang mit der Untersuchung von Incidents lassen sich in einem zentralen Portal nachverfolgen und managen, was vollständige Transparenz und umfassendes Reporting ermöglicht. Schließlich können Sicherheitsbetriebsleiter Key-Performance-Indikatoren effektiv überwachen, die Wirksamkeit von Kontrollen messen und das gesamte SOC-Team managen.

Mithilfe von RSA Archer Sicherheitsabläufe und Management von Sicherheitsverletzungen wird der Prozess für die Reaktion auf Incidents, mit dem Sicherheitsereignisse und Incidents behandelt werden, in einen weiter gefassten,

ausgereifteren Ansatz für das Management von Sicherheitsabläufen integriert. Dank eines eindeutigen Prozessworkflows und Einblicken in die Dynamik von Sicherheits-Incidents können SOC-Manager die Arbeitszeit und Ressourcen im Sicherheitsteam besser ausnutzen und dadurch ihre Reaktion, Analysen und die Behebung kritischer Sicherheits-Incidents beschleunigen. Das Sicherheitsteam kann mit verbesserten Prozessen und Funktionen vorhandene SIEM-/Protokoll-/Paketerfassungsressourcen nutzen, um sich auf die gravierendsten Incidents zu konzentrieren. Die Lösung stärkt die effektive Reaktion auf potenzielle Datenschutzverletzungen, steigert die Rendite von Infrastrukturinvestitionen und senkt das Sicherheitsrisiko insgesamt.

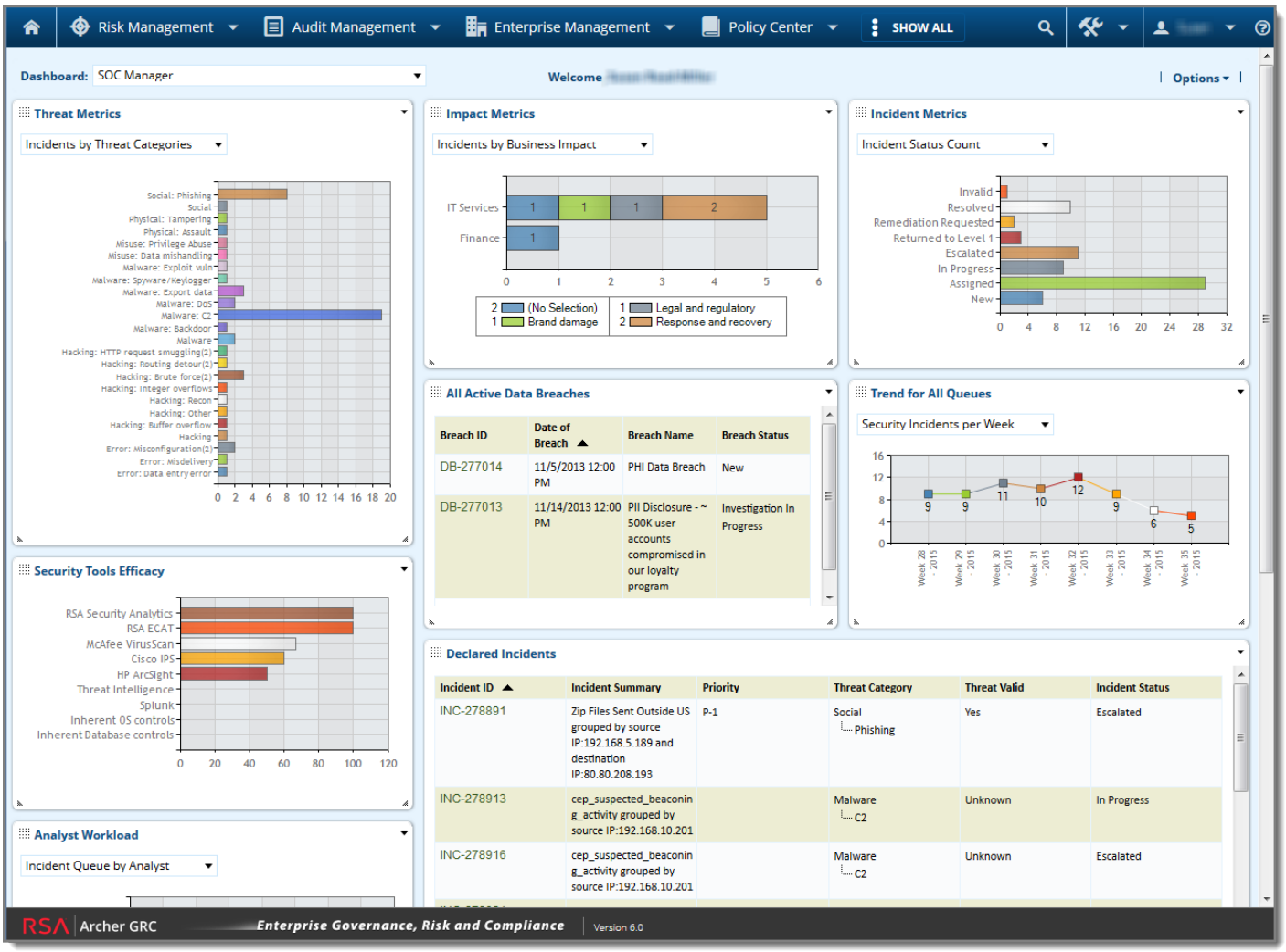
Hauptmerkmale

- Zentralisierter Katalog für Unternehmensressourcen und IT-Ressourcen
- Zentrales Repository und Taxonomie für Sicherheitswarnungen und Integration in SIEM-/Protokoll-/Paketerfassungsinfrastruktur
- Risikobewertungen von Sicherheitsverletzungen
- Festgelegte Verfahren für die Reaktion auf Sicherheits-Incidents
- SOC-Managementtools, wie Benachrichtigungen, Monitoring der Wirksamkeit von Kontrollen, KPIs, Personalmanagement und Schichtwechsel
- Problemmanagement für den IT-Betrieb

Die wichtigsten Vorteile

Vorteile von RSA Archer Sicherheitsabläufe und Management von Sicherheitsverletzungen:

- Geringerer Zeit- und Arbeitsaufwand für das SOC-Personal bei der Eskalation von und Reaktion auf Sicherheitswarnmeldungen
- Günstigere Ausgangslage für eine Reaktion auf Sicherheitsverletzungen
- Geringeres Sicherheitsrisiko



Weitere Informationen

Weitere Informationen darüber, wie Produkte, Services und Lösungen von EMC Sie bei der Bewältigung Ihrer Geschäfts- und IT-Herausforderungen unterstützen, erhalten Sie von Ihrem Vertriebsmitarbeiter oder autorisierten Reseller vor Ort oder auf unserer Website unter www.rsa.com. Wenn Sie bereits Kunde von RSA Archer sind und Fragen haben oder zusätzliche Informationen zur Lizenzierung wünschen, wenden Sie sich bitte an RSA Archer unter archersupport@rsa.com oder rufen Sie die Nummer 00800 772 49000 an.

RSA
www.RSA.com