

Kurzdarstellung des Produkts: ArcSight™ ESM

Für umfassendes Monitoring und Schutz Ihres Unternehmens

Hochentwickelte Lösungen für Compliance-Anforderungen und Schutz gegen externe sowie interne Bedrohungen

Höhepunkte

- Umfassendes Monitoring und Schutz für alle IT Hardware- und Software-Assets
- Fertige Vorlagen erlauben schnellere Umsetzung von Compliance-Anforderungen
- Einheitliche Plattform für Sicherheits- und Compliance-Berichte für alle Assets und Benutzer

Die Lösung zum Sicherheits- und Ereignismanagement ArcSight ESM wird von den weltweit renommiertesten Unternehmen zur Sicherung ihrer geschäftlichen Tätigkeit eingesetzt. Mit ArcSight ESM lassen sich alle Ereignisse im gesamten Unternehmen überwachen, und auf der Basis einer leistungsfähigen Korrelation und Analyse können geschäftliche und technologische Bedrohungen rasch identifiziert werden. ESM baut auf einer flexiblen, erweiterbaren Plattform auf und ermöglicht unternehmensweit wie auch zwischen mehreren Unternehmen eine Portabilität von Inhalten, als auch zwischen unterschiedlichen technologischen Produkten.

Reduzieren Sie die geschäftlichen Risiken für Ihr Unternehmen

ArcSight ESM liefert die Korrelationsinfrastruktur, mit der die Bedeutung eines beliebigen Ereignisses besser identifiziert werden kann, indem dieses in den entsprechenden Kontext eingeordnet wird: bei wem ist welches Ereignis wo, wann und unter welchen Umständen aufgetreten, und welche Auswirkungen hat dieses Ereignis auf das geschäftliche Risiko. Die Korrelation in ArcSight ESM liefert eine genaue und automatisierte Priorisierung von Sicherheitsrisiken und Compliance-Verletzungen in einem geschäftsrelevanten Zusammenhang. Die Sammlungsinfrastruktur in ESM bietet eine hochentwickelte Sammlungsfunktion für die umfangreichste Zusammenstellung von Ereignisquellen – Logs von über 275 Geräten und Ereignisquellen werden gesammelt, darin eingeschlossen Betriebssysteme, Netzwerkgeräte (Router, Switches), Netzwerk-Analyzer (Netzwerküberwachungseinrichtungen und Traffic-Analyzer,

NAC, NBA), Sicherheitslösungen (IPS/IDS, Firewalls, VPNs, Schwachstellen-Scanner) sowie Logs von Anwendungen, Datenbanken, Lösungen für das Identitätsmanagement und webserver- bzw. webbasierte Anwendungen. Ereignisse von unterschiedlichen Geräten derselben Familie (z. B. Router) werden normalisiert, damit sie einfach geräteübergreifend beobachtet und analysiert werden können. Optionale Lösungspakete können hochrangige Probleme und Initiativen wie SOX, PCI, HIPAA, GLBA, Benutzerüberwachung und IT-Governance unterstützen und verwalten.



ArcSight ESM kann viele Probleme für mehrere Benutzer und Rollen lösen.

Leistungsstarke Korrelation und Analyse zur Erkennung von Risiken

Die leistungsstarke Korrelations-Engine in ArcSight ESM ermöglicht Unternehmen, ein kontinuierliches situationsabhängig hohes Sicherheitsniveau aufrechtzuerhalten, indem sie Millionen von Ereigniseinträgen in Echtzeit verarbeitet. ESM konzentriert sich dann auf die wenigen kritischen Ereignisse, die vom Sicherheitsadministrator überprüft werden sollten. Durch die Integration von Netzwerkelementen und von Benutzermodellen ist ArcSight ESM in einzigartiger Weise dazu in der Lage zu verstehen, wer sich im Netzwerk befindet, welche Daten abgerufen werden und welche Aktionen mit diesen Daten durchgeführt werden. Echtzeitalarne zeigen Administratoren die kritischsten Sicherheitsereignisse in der Umgebung, zusammen mit dem gesamten notwendigen Kontext, damit die damit verbundene Sicherheitsverletzung weiter analysiert und minimiert werden kann.

Flexible Dashboards, robustes Reporting

ArcSight ESM bietet eine Reihe von Funktionen, die einen schnellen, bequemen und intuitiven Zugang zu Informationen gewährleisten. Anpassbare und grafisch umfangreiche Dashboards gewährleisten geschäftliche und technische Ansichten, über die einzelne Personen den entsprechenden Einblick in ein Unternehmen erhalten können. Über die ESM-Konsole wird der Sicherheitsstatus eines Unternehmens basierend auf validierten Angriffen und geschäftlichen Risiken auf einen Blick dargestellt, und geografische und Netzwerkansichten ermöglichen den Benutzern, die Aufmerksamkeit in bestimmten Bereichen ihrer Verantwortung im Unternehmen hoch zu halten.

ArcSight ESM bietet umfassende technische, betriebliche und Trendberichte, die Informationen zum Sicherheitsstatus enthalten und den gesetzlichen Anforderungen bezüglich des Berichtswesens genügen. Das Reporting-Framework vereinfacht das Berichtswesen auf Unternehmensebene dadurch, dass sowohl standardisierte als auch anpassbare Vorlagen für den Compliance-Status, geschäftliche Risiken und Benutzerprofile angeboten werden. Zusätzlich zu den vorgefertigten Berichten und Vorlagen wird Benutzern durch das Framework ermöglicht, neue Berichte und Vorlagen für unmittelbare oder geplante Berichtsansforderungen zu erstellen. Im Framework werden hochgradig korrelierte Information in umfassenden Ansichten gebündelt, die

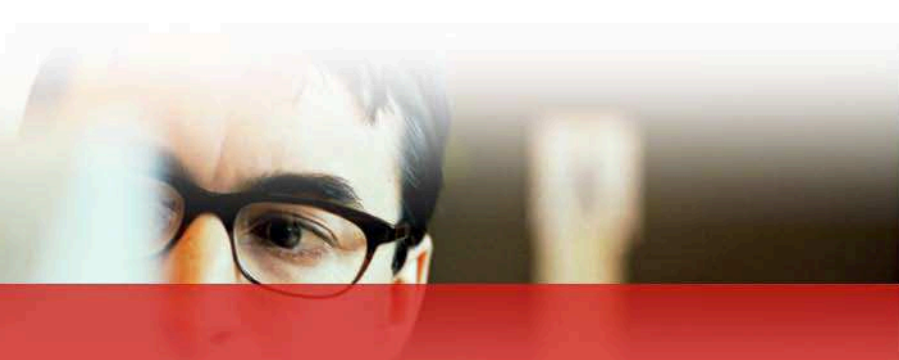
alle Beteiligten in die Lage versetzen, Risikobereiche zu identifizieren, den Wert und die Effektivität von Sicherheitsoperationen zu erkennen und unkompliziert wichtige Geschäftsfragen zu beantworten. Trend-Reporting macht das Verfolgen von Ereignissen und ihren zeitlichen Auswirkungen möglich. Mittels Korrelationstechnologie kann das Trend-Reporting auch dazu benutzt werden, „was-wenn“-Szenarien zu simulieren und zu zeigen, welche Auswirkungen solche Richtliniwechsel möglicherweise auf die globale Sicherheits- und Risikoaufstellung eines Unternehmens haben können.

Modell	E7100
EPS (Peak Sustained)	5000 EPS/3000 EPS
Betriebssystem	Oracle Linux (Variante von RedHat)
CPU	2x Quad-Core Intel Xeon (2,0 GHz)
RAM	16 GB
Schnittstellen	2 x 10/100/1000 CX
Speicher	6x SAS-Laufwerke (Serial Attached SCSI) mit je 400 GB in RAID-10
Gestell	2U Rack-Mountable-Appliance
Stromversorgung	2x 750 W redundant
Thermische Leistung	2700 BTU/h (791,1 W)
Gewicht	27 kg
Abmessungen (TxBxH)	74,4 cm x 43,7 cm x 8,6 cm

ArcSight ESM ist entweder als Software oder als Rack-Mountable-Appliance erhältlich.

Über ArcSight

ArcSight ist ein führender Anbieter von Sicherheits- und Compliance-Lösungen für Unternehmen, MSSPs (Managed Security Service Provider) und Regierungsbehörden. Die Lösungen von ArcSight identifizieren und entschärfen geschäftliche Risiken auf intelligente Weise, indem sie einen zentralen Überblick aller Ereignisse bieten, die in heterogenen Infrastrukturen aufgetreten sind. Die Echtzeit- und historische Darstellung von externen Angriffen, Bedrohungen von innen und Compliance-Verletzungen geben dem Kunden genau die Intelligenz an die Hand, die sie zu einem wirksamen Schutz ihres Unternehmens benötigen.



ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com
 E-Mail: info@arcsight.com

Konzernzentrale: +1 408 864 2600
 Zentrale für den EMEA-Raum:
 +44 870 351 6510
 Zentrale für den asiatisch-pazifischen
 Raum: +852 2166 8302

© 2008 ArcSight, Inc. Alle Rechte vorbehalten.
 ArcSight and ArcSight ESM sind Handelsmarken von
 ArcSight, Inc. Alle anderen hier erwähnten Produkt- und
 Firmennamen sind möglicherweise Handelsmarken
 oder registrierte Handelsmarken ihrer jeweiligen
 Eigentümer. P/N PB04a 6/06