

Security Information & Event Management

ArcSight Express – Erstklassiger Schutz für mittelständische Unternehmen

Mittelständische Unternehmen sind einem enormen wirtschaftlichen Druck ausgesetzt, ihre Kundenbasis erweitern, effizienter arbeiten, Kosten zu senken und Prozesse automatisieren zu müssen, um geschäftlich überlebensfähig zu sein. Dieser Druck wird oft durch eine immer komplexere IT-Infrastruktur aufgefangen, was dann aber meist bedeutet, dass die eingesetzten Sicherheitstools und -verfahren nicht mehr angemessen sind. Für Unternehmen, die trotz eines geringeren Budgets und Zeitdrucks ihre Sicherheit und Compliance verbessern möchten, bedarf es einer erstklassigen Sicherheitsüberwachung in Form einer einfachen und kostengünstigen Appliance-Lösung.

ArcSight Express – Erstklassiger Schutz für mittelständische Unternehmen

Wir empfehlen dafür ArcSight Express, eine SIEM-Appliance-Lösung. Mit dieser Lösung werden alle Aktivitäten, die unternehmensweit an den Firewalls, Servern, Desktop-Computern, Antivirenprogrammen, IPS-Systemen, beim Fernzugriff, auf VPN-Geräten, Routern, Switches und anderen Verbindungsgeräten auftreten, erfasst und überwacht und entsprechende Berichte daraus erstellt. Das Produkt ist speziell auf die Bedürfnisse von Unternehmen zugeschnitten, denen nur begrenzte Ressourcen für die Installation und die fortlaufende Verwaltung zur Verfügung stehen. Mit ArcSight Express kann jedes Unternehmen auftretende Probleme einfach erkennen, da die sicherheitsrelevanten Informationen an einem zentralen Ort zusammengefasst werden. In ArcSight Express sind die erforderlichen optimalen Verfahrensweisen (Best Practices) und ein umfassendes Sicherheitswissen integriert. Dieses Wissen liegt in Form von Regeln, Alarmen, Berichten und Dashboards vor, die auf die häufigsten, bereits beschriebenen Risikobereiche ausgerichtet sind. In dem Produkt wird dieses Wissen mit einer auf dem Markt führenden Korrelationsfunktion kombiniert. Auf diese Weise ent-

steht eine umfassende, leicht zu bedienende und wartungsarme Lösung, die sich auf die Aufgaben rund um die Überwachung der Geräte, des Netzwerks, der Infrastruktur und der Einhaltung der Compliance konzentriert, mit denen kleinere Unternehmen am häufigsten konfrontiert werden.

Bei ArcSight Express wird insbesondere die Tatsache berücksichtigt, dass die meisten Unternehmen nicht die Mittel und Ressourcen haben, eine eigene spezialisierte Sicherheitsabteilung aufzubauen. Mit ArcSight Express wird die Erkennung von und die Benachrichtigung über Sicherheitszwischenfälle automatisiert. Die IT-Mitarbeiter müssen sich nur noch darauf konzentrieren, wie sie am besten auf die Sicherheitsvorfälle reagieren. ArcSight Express gibt es als Ein-Box- oder Zwei-Box-Lösung und besteht aus den folgenden Schlüsselkomponenten:

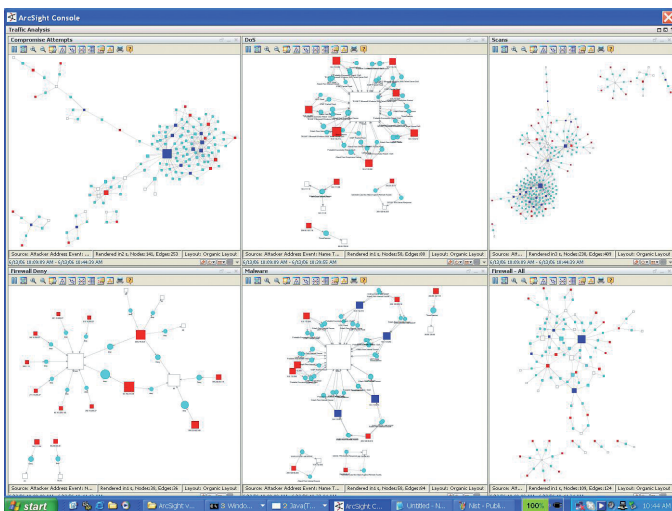
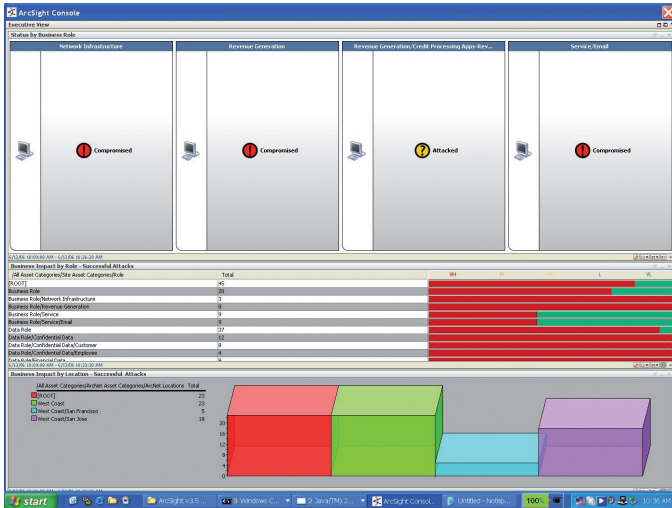
Die Korrelations-Appliance

Herzstück ist eine erstklassige, auf dem Markt führende Korrelations-Engine, bei der eine Vielzahl von Methoden eingesetzt wird, mit denen Ereignisse,



ArcSight Express – Der Sicherheitsexperte «In der Box»

die potenzielle Sicherheitsprobleme darstellen können, schnell erkannt werden. ArcSight Express enthält einen Satz von integrierten Korrelationsregeln, Berichten, Alarmen und Dashboards, mit denen kleinere Sicherheitsteams unmittelbar nach der Installation und ohne Berichtsvorlauf eine umfassende Sichtbarkeit der Systemumgebung erlangen können. Für die ohnehin stark belasteten IT-Teams



entfällt so die Notwendigkeit, den entsprechenden Inhalt definieren und auf einer Entwicklungsplattform bereitstellen zu müssen.

Die ArcSight Express Log-Management-Appliance

Die Log-Daten werden in einem effizienten, komprimierten Format in einer Log-Management-Appliance gespeichert. Sie können jederzeit schnell durchsucht und analysiert werden, ohne dass dazu die gespeicherten Daten wieder entpackt werden müssen. Ausserdem ist für die meisten Compliance-Regelungen keine separate, zusätzliche Speicherinfrastruktur zur Erfüllung der Datenaufbewahrungsanforderungen erforderlich.

Zum besseren Verständnis der gesamten Sicherheitsaufstellung der Organisation ist es notwendig, Logs aller Geräte aus dem Netzwerk zu erfassen.

Veranstaltungshinweis:

ArcSight Express-Lunch
6. Mai 2010 Bern, 11. Mai 2010 Zürich
Mehr Informationen unter www.devoteam.ch

ArcSight Express ermöglicht mit einer integrierten Komponente eine gebrauchsfertige Sammlung von Ereignis-Logs von über 275 Geräten.

Zusammenfassung

Mittelständische Unternehmen haben mit genau denselben Herausforderungen rund um Sicherheit und Compliance zu kämpfen wie grosse Konzerne. Allerdings müssen mittelständische Firmen beim Schutz ihrer Netzwerke mit begrenzten Budgets, eingeschränkten personellen Ressourcen und oft auch geringerem Wissen auskommen. Eine starke SIEM- und Log-Management-Lösung kann helfen, die Analyse der Daten zu sicherheitsrelevanten Ereignissen zu automatisieren. Das macht sich in einer Verringerung der vom IT-Personal benötigten Zeit und Arbeitsleistung bemerkbar. Besonders wichtig ist dies für Organisationen, die nicht über spezialisiertes Sicherheitspersonal verfügen. Möchten Sie mehr über ein ausgereiftes SIEM mit vollem Featureset erfahren, nehmen Sie Kontakt mit uns auf. Als zertifizierter ArcSight-Partner bieten wir Ihnen das gesamte Dienstleistungsangebot rund um SIEM und ArcSight an.

GENESIS DEVOTEAM

Planen Realisieren Betreiben

Lösungen für IT Service Management, IT Security Management, IP Management

Unsere Erfolgsgarantie

Seit 1996 Komplettlösungen aus einer Hand, durchgängige Kompetenz, internationale Ressourcen, Spezialisten-Know-how, Expertise und Erfolg in grossen IT-Umgebungen

Kontakt

Ostermundigen / Zürich / Carouge
Tel. 031 560 35 35 Fax 031 560 35 45
Tel. 044 455 60 81 Fax 044 455 60 85
Tel. 022 732 16 27 Fax 022 732 16 28
info@devoteam.ch

www.devoteam.ch