Datenblatt

Computer Associates®

*e*Trust® Security Command Center r8

Mit *e*Trust® Security Command Center r8 können Sie relevante Sicherheitsdaten erkennen und ihnen Prioritäten zuordnen, was eine effektive Verwaltung von Sicherheitsrisiken in Echtzeit ermöglicht. Wenn Sie Sicherheitsrisiken und Assets zueinander in Beziehung setzen, können Unternehmen korrigierend eingreifen und Sicherheitsverletzungen über eine zentrale Überwachungs- und Steuerungskonsole untersuchen. Als Bestandteil der Enterprise Infrastructure Management-Strategie von Computer Associates International, Inc. (CA) unterstützt Sie *e*Trust Security Command Center beim Zusammenstellen von Business Intelligence-Daten, mit denen Sie Risiken minimieren, die Business Continuity gewährleisten und die Einhaltung von gesetzlichen und anderen Bestimmungen sicherstellen können.

Wichtige Leistungsmerkmale im Überblick

- Zentralisierte Überwachung und Steuerung
- Überprüfungsengine
- Fortschrittliche Korrelation von Ereignissen
- Korrelation über mehrere Software- und Hardwareplattformen hinweg
- Assetbasierte Einordnung von Ereignissen nach Priorität
- Fortschrittliche Visualisierung
- Incident-Management
- Problembehebung
- Richtlinienbasierte Benachrichtigung bei Ereignissen
- Fortschrittliches Reporting

Neues in r8.1

- Sofort einsatzfähige Tools zur Korrelation
- Incident-Management-Workflow
- Erweiterte Integration von Unicenter® Network and Systems Management
- Neue Arbeitsbereiche und Visualisierung
- Lokalisierungsunterstützung

Sicherheitsinformationsflut

Da immer mehr traditionelle Unternehmen Technologien auf Basis des Internets übernehmen, ist die Verwaltung von IT-Sicherheit extrem komplex geworden. Viele Unternehmenssysteme erfassen Daten über sicherheitsbezogene Ereignisse und geben Warnungen aus. Diese beziehen sich auf Betriebssysteme, Anwendungen, Sicherheitssoftware und Sicherheitshardware, Kommunikationssysteme, physikalische Kontrollsysteme und andere Infrastrukturkomponenten. Ohne eine intelligente Korrelation dieser wichtigen und umfangreichen Daten fehlen Ihrem Unternehmen die Steuerelemente und Managementfunktionen, um angemessen auf die Situationen reagieren zu können, die möglicherweise die Sicherheit gefährden. Das kann entscheidende Geschäftsprozesse und Assets sowie den alltäglichen Geschäftsbetrieb beeinträchtigen.

Hinzu kommt, dass Sicherheitsadministratoren, die ihre Unternehmen schützen und stärken sollen, von Meldungen und Ereignissen überschwemmt werden – oft Millionen pro Tag. Ein einziger Vorfall kann Tausende von Meldungen nach sich ziehen. Das macht es fast unmöglich, die Ereignisse nach Priorität zu gewichten und zu entscheiden, welchen Grad an Aufmerksamkeit sie erfordern, was die Arbeit der IT-Abteilung in Hinblick auf die Sicherheit erschwert.

Die Sicherheitsdatenflut stammt aus einem Array von Software- und Hardwareplattformen, darunter Virenschutzsoftware, Firewalls, Webanwendungen, Warnsysteme gegen Angriffe von außen, Zugriffssteuerung, Identity Management, Einzelanmeldung, Authentifizierungssysteme usw. In der Regel setzt ein Unternehmen mindestens eine dieser Lösungen ein, die auf zahlreichen Hardwareplattformen und unter verschiedenen Betriebssystemen ausgeführt werden können. Diese Sicherheitslösungen dürfen aber nicht isoliert eingesetzt werden, sondern müssen miteinander verbunden und in die wichtigsten Unternehmensanwendungen integriert werden, darunter Lohnbuchhaltung, Personalwesen und Produktion. Dies erfordert einen offenen Austausch und eine intelligente

Datenfilterung sowie die Korrelation der unterschiedlichen Systemen.

Die Führungskräfte von heute müssen die Kontinuität aller Geschäftsprozesse gewährleisten, Kosten in Grenzen halten und die Einhaltung von Vorschriften überwachen. In Hinblick auf die Sicherheit bedeutet dies, dass die wichtigsten Ressourcen geschützt werden müssen. In einer On-Demand-Computing-Umgebung, in der Systeme dynamisch konfiguriert und bereitgestellt werden, ist eine zentrale Überwachungs- und Steuerungskonsole erforderlich, um in Echtzeit auf geschäftliche Prioritäten reagieren zu können und laufende Geschäftsprozesse sowie eine ständige Kontrolle sicherzustellen. Hierfür ist eine echte Sicherheitsmanagementlösung unerlässlich, die sämtliche Rohdaten aus den verschiedenen sicherheitsbezogenen Lösungen in intelligente Informationen umwandelt, die in Echtzeit abgerufen und bearbeitet werden können.

Sicherheitsinformationsmanagement von der Erkennung bis zur Behebung

*e*Trust Security Command Center von Computer Associates ist eine leistungsstarke Lösung zum Management von Sicherheitsinformationen. Sie trägt durch die Überwachung und Verwaltung aller Aspekte der Unternehmenssicherheit dazu bei, das „Übermaß an Sicherheitsinformationen“ zu bewältigen – von der Erkennung bis zur Behebung – und das in Echtzeit. *e*Trust Security Command Center stellt Business Intelligence-Daten durch das Aggregieren, Reduzieren, Korrelieren und Erteilen von Prioritäten verschiedenster Sicherheitsdaten, die von Sicherheitsmedien, Softwaretechnologien und Assets in einem Unternehmen stammen, zusammen. Anschließend werden den großen Mengen Daten Prioritäten zugeordnet, die danach in intelligente, nützliche Informationen umgewandelt werden, die von einer einzigen zentralen Konsole aus verwaltet werden. Sie werden gespeichert, damit sie auch in Zukunft für Berichte, Analysen und zur Verwaltung genutzt werden können.

*e*Trust Security Command Center zeigt Sicherheitsdaten in einem leicht verständlichen visuellen Format an, das die Informationen in den Kontext der Unternehmensprioritäten stellt. Dank der zentralen Überwachungs- und Steuerungskonsole sowie der Warnfunktionen der Lösung können Unternehmen schnell aktiv werden und Bedrohungen entschärfen, die Gefährdung wichtiger Geschäftssysteme vermeiden, Ausfallzeiten minimieren und Business Continuity gewährleisten. Darüber hinaus bietet *e*Trust Security Command Center die Tools, die erforderlich sind, um die einem Vorfall vorausgehenden Ereignisse zu untersuchen. Auf diese Weise können Unternehmen verfolgen, welche Schritte zu einer Sicherheitsverletzung geführt haben, und erarbeiten, welche Maßnahmen sie zur Einhaltung ihrer Sicherheitsrichtlinien ergreifen müssen.

Als Bestandteil der Enterprise Infrastructure Management-Strategie von Computer Associates leistet *e*Trust Security Command Center eine proaktive Verwaltung von komplexen Sicherheitsumgebungen. Vorfälle werden nicht nur erkannt, sondern auch bewältigt, was die Investitionsrentabilität steigert und das Risikomanagement auf ein bislang unerreichtes Niveau anhebt.

Besondere Merkmale und Funktionen

Erkennung, Zusammenstellung und Überwachung. Durch automatische Erkennung in Echtzeit, das Zusammenstellen von Informationen und Überwachen des betrieblichen Status verbessern Sie die geschäftliche Effizienz und maximieren Ihre Investitionen in die Sicherheit.

- **Erkennung.** Lernen Sie Ihre Umgebung kennen, und zentralisieren Sie die Verwaltung eindeutiger Ereignisse aus verschiedenen Quellen über eine zentrale Steuerungskonsole.
- **Statusüberwachung.** Überwachen Sie die betrieblichen Meldungen und Warnungen in Ihrer Umgebung in Echtzeit, und zeigen Sie die auf diese Weise ermittelten Intelligencedaten bedarfsgerecht den Benutzern an, die darauf reagieren müssen. Mithilfe der Statusüberwachung erhalten die richtigen Personen die richtigen Informationen über die Sicherheit in Ihrem Unternehmen, und das zur richtigen Zeit.
- **CA Security Advisor.** Dieses Tool stellt eine Weiterentwicklung von *e*Trust Security Command Center dar. Das Forschungsteam von CA versetzt Sie in die Lage, durch Web-Update-Services von aktuellen, aus Korrelationen gewonnenen Intelligencedaten, von Berichten, Visualisierungen und von Arbeitsbereichen zu profitieren.

Korrelation und Analyse. Der sofortige Nutzen, den umfassende Tools zur Korrelation und zur Analyse bieten, ermöglicht eine beschleunigte Implementierung von Sicherheit und eine gesteigerte Investitionsrentabilität. Mit diesen anpassbaren Tools können Sie die Regeln für die Korrelation und die Analyse in Hinblick auf die Sicherheit an Ihre Website anpassen.

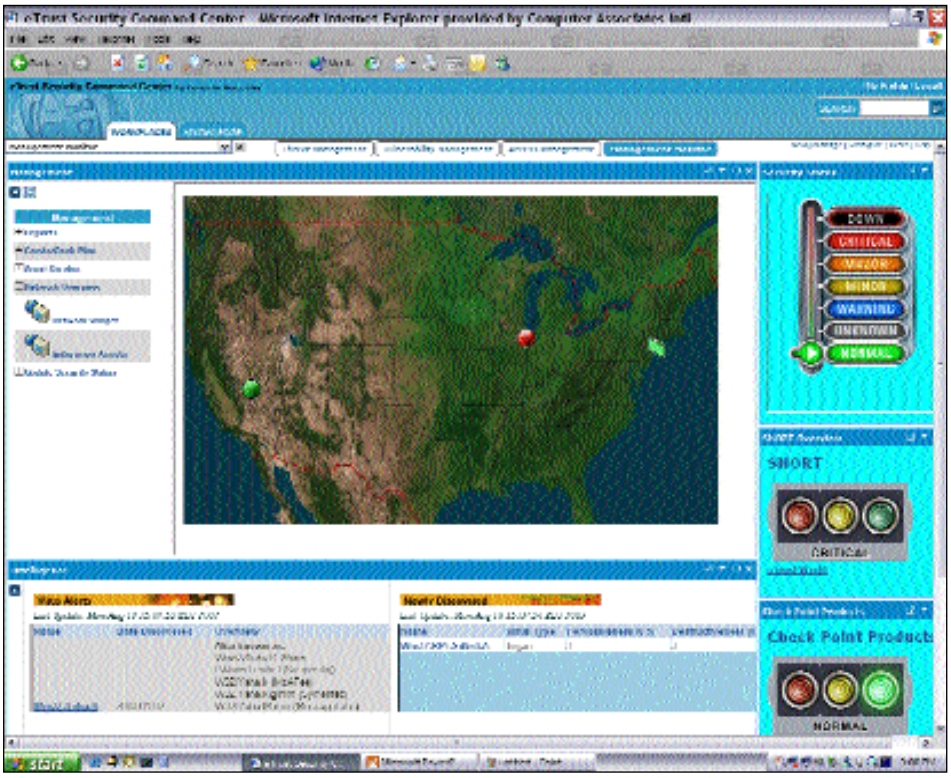

Abbildung 1.
Webgestützte Ansichten zeigen nur die für Ihre Rolle relevanten Informationen an und bieten Drilldownfunktionen, um sofortige Maßnahmen zu ergreifen.

- **Richtlinienbasierte Korrelation.** Verwenden Sie zur Überwachung von Ereignissen in Ihrer Umgebung Regeln, die Sie einfach herunterladen, bereitstellen und konfigurieren können. Die Regeln für die Korrelation können Sie mit intuitiven, benutzerfreundlichen Vorlagen und Assistenten selbst erstellen. *e*Trust Security Command Center kann Tausende von Regeln gleichzeitig verwalten. Durch die fortschrittliche Automatisierung können vorab Scripts für die richtigen Reaktionen erstellt werden, abhängig von Ihren Sicherheitsanforderungen.
- **Korrelation von Sicherheitssoftware und Sicherheitshardware.** Daten aus unterschiedlicher Sicherheitssoftware und Sicherheitshardware werden in einer konsolidierten und normalisierten Datenstruktur zueinander in Beziehung gesetzt, was eine leistungsfähige Klassifizierung der Sicherheitsdaten von Ereignissen aus sämtlichen Quellen ermöglicht. Die Korrelation von Sicherheitssoftware und Sicherheitshardware beinhaltet Anwendungen wie Warnsysteme gegen Angriffe von außen, Firewalls, Router, Protokolldateien von Betriebssystemen, Virenschutzsysteme, Web-Server, drahtlose Geräte, Netzwerkgeräte und vieles mehr.
- **Korrelation von Schwachstellen.** Nutzen Sie *e*Trust® Vulnerability Manager, um potenzielle Bedrohungen mit Schwachstellen und anfälligen Assets zueinander in Beziehung zu setzen, damit die wichtigsten Warnungen die nötige Aufmerksamkeit bekommen.
- **Korrelation von Netzwerkvorgängen.** Die bidirektionale Korrelation der Sicherheitsereignisse und des Netzwerkverkehrs aus Systemen zur Netzwerk- und Systemverwaltung verbessert nicht nur die Netzwerk- und Sicherheitsvorgänge, sondern auch die Reaktionen.
- **Korrelation des Zugriffsmanagements.** Erfolgreiche und fehlgeschlagene Anmeldungen werden zueinander in Beziehung gesetzt und Muster aufgedeckt. *e*Trust Security Command Center erlaubt den Zugriff auf Ressourcen, damit sie verfolgt werden können, sowie auf Muster, um diese hervorzuheben, zu verwalten und bei Bedarf Berichte darüber zu erstellen.
- **Korrelation von Datenbank-, Mainframe- und Unternehmensanwendungen.** Datenbank-, Mainframe- und Anwendungsdaten werden mit einer einzelnen leistungsfähigen Engine analysiert und korreliert. Wenn Sie Ihre Sicherheitsdaten und die ermittelten Informationen bestmöglich nutzen möchten, ist es wichtig, dass Sie in älteren Anwendungen sowie entscheidenden Geschäftsprozessen und Plattformen Muster aufdecken.
- **Korrelation der physikalischen Sicherheit.** Die Achillesferse bei der Sicherheit ist oftmals der physikalische Zugriff und die physikalische Sicherheit – ist eine erfolgreiche Anmeldung signifikant, wenn ein Benutzer physisch nicht anwesend ist? Die Korrelation der physikalischen Zugriffsprotokolle mit IT-Zugriffsprotokollen ist eine bedeutende Komponente, wenn es darum geht, die Integrität eines Unternehmens zu wahren.
- **Klassifizierung von Ressourcen und Erteilung von Prioritäten.** Zur Risikominimierung ist es unerlässlich, Bedrohungen und Schwachstellen mit wichtigen Geschäftsprozessen und Assets zu korrelieren. *e*Trust Security Command Center versetzt Ihr Unternehmen in die Lage, kritische Assets zu klassifizieren, damit Sie diesen erste Priorität erteilen und sie von Problemen befreien können.

Warnung, Kontrolle und Aktion. Mit den fortschrittlichen Funktionen für Warnungen, Visualisierung, Incident-Management und Problembehebung können Sie Sicherheitsbedrohungen

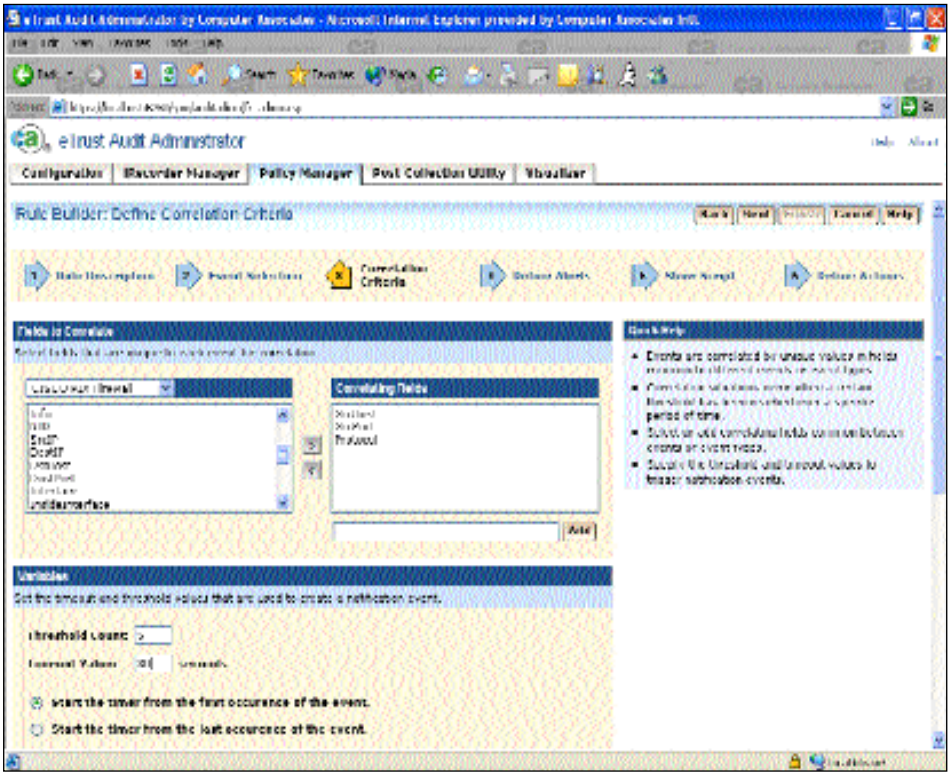

Abbildung 2.
Mit dem flexiblen Rule Policy Wizard können Sie schnell und einfach richtlinienbasierte Regeln für das Aggregieren, Reduzieren, Korrelieren und anderes für Ihre Umgebung erstellen.

schnell erkennen und beheben – und Ausfallzeiten sowie Serviceunterbrechungen direkt verhindern.

- **Richtlinienbasierte Benachrichtigung bei Ereignissen.** Die Richtlinienengine, die zur Korrelation verwendet wird, erstellt auch Scripts für angemessene Reaktionen, die an bestimmte Rollen in Unternehmen angepasst sind – das Aufrufen von Anwendungen, Auslösen von Warnungen, Benachrichtigen von wichtigen Mitarbeitern per Paging oder E-Mail usw.
- **Visualisierung.** Webgestützte visuelle Tools mit rollenbasiertem Zugriff ermöglichen Benutzern neue und sinnvolle Ansichten ihres Arbeitsbereichs. Mit *e*Trust Security Command Center Visualizer können Sicherheitsbeauftragte leistungsfähige visuelle Darstellungen der Ereignisse in ihrer Umgebung erstellen und damit arbeiten (siehe Abbildung 1).
- **Incident-Management.** Incident-Management und fortschrittliche Workflowfunktionen ermöglichen ein schnelles und effektives Reagieren auf Vorfälle. Mithilfe von Arbeitsbereichen, die das Gruppieren und Kommentieren von Ereignissen bzw. das Feststellen und Bestätigen von Vorfällen ermöglichen, können Sicherheitsbeauftragte die Hintergründe eines Vorfalls feststellen, Ereignisse verwalten und entsprechend reagieren.
- **Problembehebung.** Ein Problem zu kennen, aber keine Lösung dafür zu finden, ist nicht sehr hilfreich. Mit *e*Trust Security Command Center können Benutzer wichtige Sicherheitsinformationen mit den Mechanismen zur automatisierten oder manuellen Behebung von Problemen verbinden, darunter Trouble-Ticket-Systeme, Patching-Tools, Systeme zur Verwaltung von Schwachstellen, Netzwerk- und Systemmanagement u. a.

Berichterstellung und Untersuchung. Zentrale, sofort einsatzfähige Berichte sind bei Bedarf verfügbar. Anpassbare Abfragetools und stabile Visualisierungen bieten einen bequemen Drilldown auf gewünschte Informationen. All diese Bemühungen schärfen Ihr Sicherheitsbewusstsein und unterstützen Sie bei Ihren Untersuchungen, Überwachungen und der Einhaltung von Vorschriften.

Sofort einsatzfähige Berichte. Mit Ihren Geräten und Systemen erstellen Sie wertvolle Berichte. *e*Trust Security Command Center stellt Berichte zusammen, die eine zentrale Archivansicht und Verteilung ermöglichen, damit Sie Sicherheitsrisiken schnell erkennen.

- **Anpassbare Abfragetools und Visualisierungen.** Ein Tool für Ad-hoc-Abfragen erstellt Berichte und liefert die Eingaben für *e*Trust Security Command Center Visualizer über eine einzelne Schnittstelle. Als ständiger Service für die Kunden von *e*Trust Security Command Center können neue Abfragen und Visualisierungen im Internet heruntergeladen werden.
- **Tools zur Überprüfung und zur Überwachung der Einhaltung unternehmensinterner oder gesetzlicher Vorschriften.** Dass Sie die Anforderungen an die Überwachung und Einhaltung von gesetzlichen Vorschriften erfüllen, ist wichtig, um die Haftung zu beschränken und sicherzustellen, dass der Datenschutz für Mitarbeiter, Partner und Kunden gewährleistet ist. *e*Trust Security Command Center bietet alle Arten von Korrelation, Berichten und Arbeitsbereichen, die der Erfüllung von Richtlinien dienen. So können Sie sich darauf konzentrieren, die Sicherheit mithilfe möglichst vollständiger und umfassender Informationen zu verwalten.

Flexible Architektur. Maximieren Sie Ihre aktuellen und zukünftigen Investitionen in die Sicherheit durch eine skalierbare und offene Architektur, die eine Bereitstellung mit oder ohne

Agent bietet, laufende Updates für Regeln zur Korrelation, Filterung auf Agentenebene und Kits zur Produktintegration.

- **Skalierbarkeit.** Durch die Architektur von *e*Trust Security Command Center ist sichergestellt, dass IT-Infrastrukturen von Unternehmen sowohl in die Breite als auch in die Tiefe skaliert werden können. Diese Skalierbarkeit ermöglicht eine dezentrale Bereitstellung von Tools zur Aggregation, Reduzierung, Erfassung und zur Korrelation von Ereignissen in unterschiedlichen Netzwerkbereichen sowie von ausgereiften Daten durch aufeinander folgende Repositorys, die von jeder Stelle im Netzwerk aus angezeigt werden können.
- **Bereitstellung mit und ohne Agent.** *e*Trust Security Command Center unterstützt die Ereignisweiterleitung an Dritte und die Datenerfassung ohne Agenten. Daneben wird die üblichere Bereitstellung über Agenten unterstützt, die Verschlüsselung, Sicherung im Store-and-Forward-Verfahren, Normalisierung und die Korrelation „an der Quelle“ ermöglicht.
- **Filterung auf Agentenebene.** Optional können Sie mit *e*Trust Security Command Center auf Agentenebene aggregieren, reduzieren und filtern und so die Menge über das Netzwerk gesendeter Daten verringern.
- **Online-Updates für Regeln zur Korrelation.** Als Teil des Kundendiensts werden die vom CA Security Advisory Team ermittelten neuen Regeln zur Korrelation und Richtlinien ständig über die Web-Update-Services bereitgestellt.
- **Kits zur Produktintegration.** Bei der Verwaltung von Sicherheitsinformationen geht es nicht nur um Sicherheitsereignisse. Verwaltet werden müssen auch der Status von Systemen und Anwendungen, die zu erfassenden und zu erstellenden Berichte sowie die Tools, die systemintern aufgerufen werden müssen, um Vorfälle erfolgreich beheben zu können. Damit all diese Aspekte berücksichtigt werden können, wurden stabile Kits zur Produktintegration entwickelt.
  Weitere Informationen über zertifizierte Integrationslösungen bietet die Liste mit zertifizierten Geräten für *e*Trust Security Command Center, die Sie unter ca.com abrufen können.

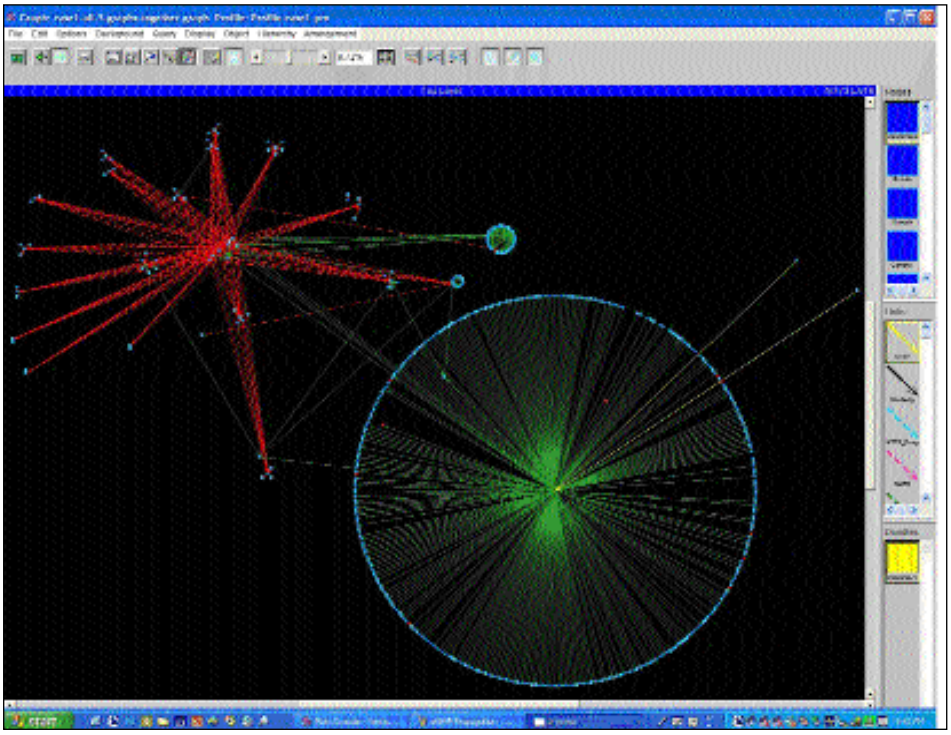

Abbildung 3. Leistungsfähige Visualisierungen ermöglichen das Analysieren und Untersuchen von Vorfällen und Mustern in Ihrer Sicherheitsinfrastruktur.

Neues in r8

Sofort einsatzfähige Tools zur Korrelation. *e*Trust Security Command Center bietet eine umfassende, sofort einsatzfähige Bibliothek mit Regeln für die Korrelation, die eine schnelle Korrelationsanalyse in der gesamten Unternehmensumgebung ermöglicht. Zusätzlich stehen der Regelassistent für die Korrelation und Vorlagen zur Verfügung, mit denen Sie neue Regeln erstellen oder bereits vorhandene ganz einfach anpassen können (siehe Abbildung 2).

- **Regelassistent für die Korrelation.** Eine leistungsstarke Richtliniensprache erleichtert Funktionen wie Aggregation, Reduzierung, Manipulationsbeweise, Datenverwaltung und Korrelation. All dies ist für den Endbenutzer nicht sichtbar. Er arbeitet mit einem webgestützten Regelassistenten für die Korrelation, der sich durch einfache Menüs und Bedingungen auszeichnet sowie durch Scripts für Aktionen, die ganz einfach erstellt, bereitgestellt und umgesetzt werden können.
- **Regelbibliothek für die Korrelation.** Neue Regeln für die Korrelation spiegeln wider, auf was Sicherheitsorganisationen heutzutage achten müssen. *e*Trust Security Command Center, unterstützt von CA Security Advisor, umfasst Hunderte von Regeln für die Korrelation und stellt rund um die Uhr über die Web-Update-Services vorhandene und neue Regeln zur Verfügung.
- **Regelvorlagen für die Korrelation.** Umfassende Regeltypen, die zu über 90 % fertig gestellt sind, können als Vorlagen verwendet und ganz einfach geändert und bereitgestellt werden.

Incident-Management. Mit den fortschrittlichen Tools für das Incident-Management und die Visualisierung von *e*Trust Security Command Center

verringern Sie das Risiko betrieblicher Beeinträchtigungen oder finanzieller Verluste aufgrund von Ausfallzeiten oder Diebstahl.

- **Verbesserungen bei der Visualisierung.** Die leistungsfähige Visualisierungsengine von *e*Trust Security Command Center kann Ereignisse und Vorfälle aus dem Ereignisrepository extrahieren, anzeigen und ändern. Im Rahmen der Funktionen für Untersuchungen und Reporting können Muster und Abweichungen aufgedeckt werden (siehe Abbildung 3).
- **Gruppieren von Vorfällen.** Mehrere Ereignisse können zu Vorfällen gruppiert werden, woraufhin sie besser verarbeitet und verfolgt werden können, ohne dass Ereignisse im Ereignisrepository geändert werden müssen. Auf diese Weise wird die Datenintegrität gewahrt, und Ereignisse sowie Vorfälle können bestmöglich verwaltet werden.
- **Incident-Management, Zuweisung und Kommentierung.** Unabhängig von der Integration von Problem-Ticket-Systemen können Ereignisse und Vorfälle von Sicherheitsbeauftragten bestätigt, zugewiesen und kommentiert werden, um ihre Verfolgung und Verwaltung zu vereinfachen.

Integration von Unicenter® Network and Systems Management.
*e*Trust Security Command Center bietet die erweiterte Integration von Unicenter Network and Systems Management-Lösungen, was eine Verwaltung von Sicherheitsobjekten aus der Network and Systems Management-Umgebung heraus ermöglicht.

- **Unicenter® Network and Systems Management Integration Kit.** Fortschrittliche bidirektionale Kommunikationen über Ereignisse und Warnungen werden zwischen Unicenter Network und Systems Management-Lösungen und *e*Trust Security Command Center versendet, sodass Sie die Netzwerksicherheit über eine zentrale Konsole gewährleisten können.
- **Unicenter® Management für *e*Trust Security Command Center.** Der Status vollständiger Vorgänge kann nun genauer betrachtet werden, da der Unicenter® Network and Systems Manager nicht mehr nur Einblick in Netzwerk- und Systemprozesse hat, sondern auch in die Sicherheitsprozesse und Sicherheitsservices, und zwar von einer zentralen Konsole aus.
- ***e*Trust Security Command Center Service Management.** Die erweiterte Integration in Unicenter® ServicePlus Service Desk sorgt dafür, dass sicherheitsbezogene Probleme schnell an die zuständigen Techniker weitergeleitet werden.

Neue Arbeitsbereiche. Durch rollenbasierte Arbeitsbereiche verbessert *e*Trust Security Command Center Ihre geschäftliche Effizienz. Verwenden Sie vordefinierte Arbeitsbereiche wie SANS Top 20, oder passen Sie sie an Ihre Rolle an. Sie können sie auch dahingehend ändern, dass sie den Zielen für die IT-Sicherheit entsprechen oder die Einhaltung gesetzlicher Vorschriften gewährleisten.

- **SANS Top 20 Workspace.** SANS Top 20 Workspace zählt zu den aktuellsten Arbeitsbereichen und versetzt Führungskräfte und IT-Mitarbeiter in die Lage, Bedrohungen zu erkennen und Schwachstellen von *e*Trust-Produkten, Open Source-Lösungen und herstellerspezifischen Sicherheitssystemen in Form von Webansichten aufzudecken. Auf Basis der vierteljährlich vom SANS Institute veröffentlichten Kategorien werden die in den Webansichten gezeigten Informationen sortiert, verwaltet und zur Berichterstellung verwendet (siehe Abbildung 4).

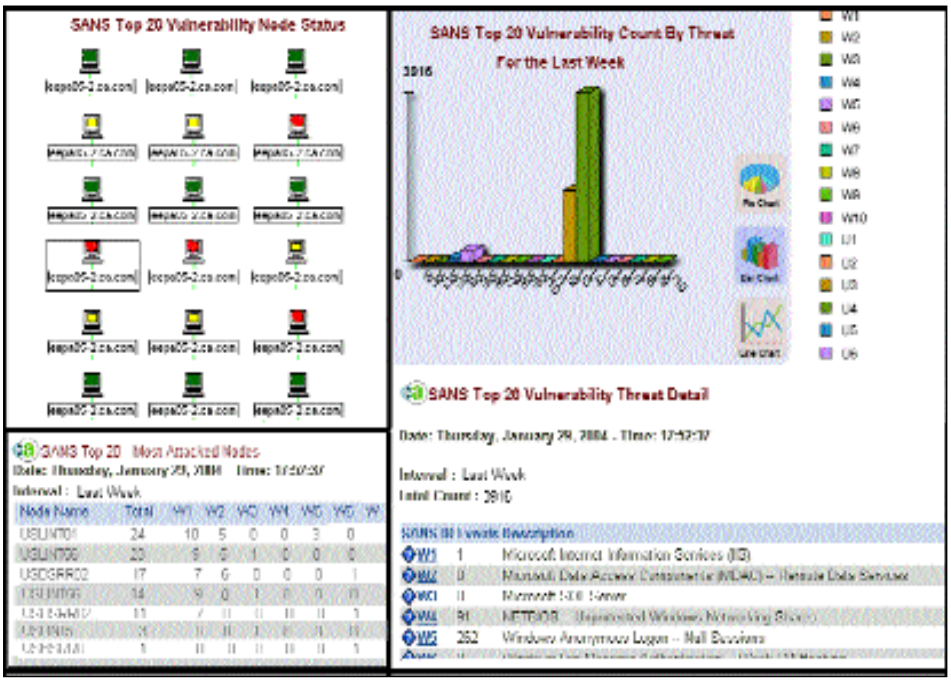

Abbildung 4. SANS Top 20 Workspace ist in *e*Trust Security Command Center integriert und verschafft Ihnen mithilfe der SANS Top 20-Kategorisierung einen Überblick über sämtliche Bedrohungen und Schwachstellen.

- **Rollenbasierte Arbeitsbereiche.** Arbeitsbereiche können auf die Rollen und Funktionen in einer Organisation abgestimmt werden. Neue Ansichten werden laufend aktualisiert und über die Web-Update-Services zur Verfügung gestellt.

Sprachunterstützung. *e*Trust Security Command Center bietet neben Internationalisierungsunterstützung erweiterte Sprachunterstützung für Englisch, Spanisch, Französisch, Deutsch, Italienisch, Japanisch, Koreanisch, Chinesisch (Traditionell) und Chinesisch (Vereinfacht).

Weitere Informationen

CA Computer Associates GmbH
D-64243 Darmstadt
Telefon 0049 / 61 51 / 9 49-0
ca.com/de

Computer Associates AG
CH-8302 Kloten
Telefon 0041 / 1 / 804 78 78
ca.com/ch

Computer Associates International
Ges.m.b.H.
A-1100 Wien
Telefon 0043 / 1 / 917 79-0
ca.com/at

Quality System
Quality Endorsed Company
ISO 9001
Lic. 2443

Computer Associates®

MP278181005