SIEM Dashboards

Analyse typischer Dashboards führender Security Information and Event Management Systeme

SaSER Milestone 1.5

FH Potsdam | IDL
Jan-Erik Stange

Einleitung

Größere Netzwerke sind aus einer extrem großen Anzahl unterschiedlicher Komponenten zusammengesetzt. Bei den Komponenten kann es sich zum Beispiel um Server, Firewalls, Router, Switches handeln. Zur Überwachung solch großer Netzwerke ist es erforderlich, dynamische (zeitbasierte) Daten, wie z.B. Log Entries, die diese Komponenten erzeugen, zusammen mit anderen statischen (nicht zeitbasierten) Daten zu sammeln, wie z.B. Identitätsdaten von Nutzern oder externen Bedrohungsdaten (Signaturen) (Marty 2008: 42). Häufig bedingen sich die Daten der verschiedenen Quellen gegenseitig, so dass sie nicht isoliert betrachtet werden sollten, um Sicherheitslagen zu beurteilen. Die Daten manuell miteinander zu korrelieren ist allerdings aufgrund der unterschiedlichen Formate äußerst aufwändig.
Sogenannte *SIEM*-Systeme *(Security and Information Management)* aggregieren diese Daten unterschiedlichen Formats, normalisieren sie und machen sie damit miteinander vergleichbar. In der Regel werden die Daten dann innerhalb einer Software-Oberfläche zusammengeführt. Der Nutzer eines *SIEMs* kann nun vordefinierte Regeln nutzen oder selber festlegen, bei denen das System Ereignisse auslöst. Diese Regeln lassen sich mithilfe von häufig einfach *Suchen* genannten Suchstrings beschreiben und speichern. Diese können als Grundlage für die im Dashboard der Software dargestellen Visualisierungen dienen oder einfach dazu, beim Überschreiten bestimmter Schwellenwerte, Alarme zu generieren, die dem Sicherheits-Administrator über weitere Kommunikationskanäle kommuniziert werden, z.B. über E-Mail oder SMS.
Das folgende Kapitel beschreibt die einzelnen Bestandteile und Funktionalitäten von *SIEMs* im Detail.

Bestandteile von SIEMs

Im Folgenden werden die charakteristischen Bestandteile/ Funktionen eines SIEM kurz vorgestellt.

Echtzeitanalyse und Alarme

Ein wichtiges Feature bestehender Systeme ist die Analyse von Netzwerkaktivitäten in Echtzeit. Alarme werden entweder dann ausgelöst, wenn Muster im Netzwerk vom System entdeckt werden, die vorher festgelegten Regeln entsprechen oder wenn Anomalien mittels statistischer Analyse identifiziert werden. Die Benachrichtigungen über potentiell bedrohliche Aktivitäten im Netzwerk können dem Nutzer, wie bereits beschrieben, über verschiedene Kanäle zugestellt werden. In einer Untersuchung der Zeitschrift *Information-Week* wurden 322 Nutzer zu verschiedenen Aspekten von SIEMs befragt. Echtzeitanalyse wurde als wichtigste Funktionalität angegeben (Francis 2012)

Forensische Analyse in archivierten Logs

Während des Netzbetriebs werden kontinuierlich Daten gesammelt und in großen Datenbanken über längere Zeiträume archiviert. Häufig lassen sich aus Angriffen, die nicht erkannt wurden, zu einem späteren Zeitpunkt durch die Analyse nützliche Erkenntnisse ziehen, die die Organisation dabei unterstützen, in Zukunft besser vorbereitet zu sein auf ähnliche Angriffe, indem entsprechende Vorkehrungen getroffen werden.

Datenaggregation und Normalisierung

SIEMs sind in der Lage aus unterschiedlichsten Quellen Daten zusammenzuführen. Da bezüglich der generierten Daten von Netzwerkgeräten keine einheitlichen Standards existieren, hat jeder Hersteller sein eigenes Datenformat. Diese Datenformate werden innerhalb des *SIEMs* normalisiert und damit miteinander vergleichbar gemacht. Grundsätzlich lassen sich zwei Grundkategorien von Daten unterscheiden: dynamische (zeitbasierte) Daten, wie die Event Logs der verschiedenen Netzwerkgeräte, und statische Daten, wie z.B. Dateien oder Informationen zu Usern im Netzwerk. (Marty 2008: 42). Typische, überwachte Datenquellen sind z.B.: Firewalls, *Intrusion Detection/ Prevention Systeme*, *NetFlow*-Daten, Geräte-Logs, Content (z.B. E-Mails), Betriebssystem-Logs, Anwendungs-Logs, Konfigurationsdateien [Rothmann 2010).

Suche/ Filter

In vielen SIEMs bilden durch den Admin erstellte Suchen/Filter die Grundlage für die Darstellung der Diagramme und Tabellen im Dashboard. Meist existieren auch bereits vorgefertigte Suchstrings, die vom Nutzer als Grundlage verwendet werden können. Häufig benötigte Suchen/Filter können gespeichert werden und mit einer bestimmten Visualisierungsart im Dashboard verknüpft werden. Typische Filter, die in solche Suchstrings eingefügt werden, sind z.B. Zeitangaben, also nur ein bestimmter Zeitabschnitt („Letzte 10 Minuten"), bestimmte Quellen (z.B. nur Firewall-Logs) oder z.B. auch ganz spezifisch bestimmte IP-Source-Adressen, um den von dort ausgehenden Traffic isoliert betrachten zu können.

Korrelation

Mithilfe einer sogenannten *Correlation Engine*, eines der Alleinstellungsmerkmale eines *SIEMs* lassen sich vom Hersteller bereits definierte oder selber angelegte Regeln nutzen, um Muster zu identifizieren, die sich über mehrere Datenquellen erstrecken. Das System bündelt miteinander verknüpfte Events aus diesen unterschiedlichen Quellen zu zusammenhängenden Paketen, die für den Sicherheitsexperten leichter zu untersuchen sind. Die Korrelations-Regeln sollten der speziellen Situation, in der das Netzwerk Verwendung findet, angepasst werden, in der Regel reichen die vordefinierten Regeln nicht aus. Die spezielle Bedrohungslage eines Netzwerkes lässt sich häufig nur aus den Angriffen und Bedrohungen, die in der Vergangenheit aufgetreten sind, ableiten (Rothmann 2010)

Zusammenfassung und Überblick (Dashboard)

Das Dashboard bietet einen Überblick über verschiedene für den Administrator relevante Ereignisse im Netzwerk. Normalerweise setzt es sich zusammen aus einer Sammlung unterschiedlicher Diagramme, die, wie unter Suche/ Filter bereits beschrieben, häufig auf vorher erstellten Suchenstrings basieren. Die Diagramme sind meist in sogenannten Widgets oder Panels untergebracht, kleinen verschieb- und skalierbaren Fenstern. Gängige Visualisierungsarten sind z.B. Tortendiagramme, Säulendiagramme, Liniendiagramme, Kartendarstellungen, häufig auch abstrahierte „Messgerätanzeigen", ähnlich eines Tachometers. Seltener findet man auch komplexere Diagramme wie Netzwerkvisualisierungen, Treemaps, Word Clouds vor. Häufig dient das Dashboard als Ausgangspunkt für eine ausgedehntere Suche bzw. Analyse.

Kompression und Speicherung

Die Speicherung im Netzwerk angefallener Daten dient unterschiedlichen Zwecken. Einerseits ermöglicht sie die nachträgliche forensische Analyse nach erfolgten Angriffen, wie oben beschrieben, andererseits treten aber auch Fälle auf, in denen Angriffe auf ein Netzwerk sich über längere Zeiträume langsam aufbauen, so dass zur Identifizierung eine langfristige Betrachtung der verschiedenen Datenquellen erforderlich ist (Rothmann 2010). Wichtig ist die Archivierung auch gerade in Hinblick auf das weiter unten beschriebene *Compliance-Management*. Mit den gesammelten Daten lassen sich Berichte erstellen (*Compliance Reports*), die zusammenfassend zeigen, dass das Unternehmen bzw. die Organisation bestehenden Richtlinien gefolgt ist.

Compliance-Management

Eine weitere, gerade für Unternehmen wichtige Funktionalität, die *SIEMs* bieten, ist das Compliance-Management. Hiermit ist in erster Linie das Einhalten gesetzlicher und unternehmensinterner Richtlinien in den Bereichen Informationssicherheit, Verfügbarkeit, Datenaufbewahrung und Datenschutz gemeint.

Analyse SIEM Dashboards

Im Folgenden werden die Dashboards vier verschiedener *SIEM*-Lösungen miteinander verglichen, um einen groben Überblick über verbereitete Visualisierungen und Funktionalitäten zu erhalten.
Bei der Auswahl der Software-Lösungen für diese Studie diente eine von *Gartner* im Mai 2012 durchgeführte Studie als Ausgangspunkt (Nicolett and Kavanagh 2012)). Diese ordnet aktuelle Marktlösungen in einen sogenannten *Magic Quadrant* ein. Im *Magic Quadrant* werden Produkte den vier verschiedenen Bereichen *Leaders*, *Challengers*, *Visionaries* und *Niche Players* zugeordnet. Mit *Leaders* werden hierbei die Hersteller von Softwareprodukten bezeichnet, die generell am besten den aktuell existierenden Wünschen der Kunden nachkommen, einen hohen Marktanteil haben, aber auch in der Lage sind, neue Bedürfnisse vorauszuahnen und diese in die Produkte zu integrieren. Im Quadranten *Challengers* werden *SIEMs* von Firmen verortet, deren Marktanteil ebenfalls hoch ist, die jedoch mit ihrer Software eine geringere Bandbreite an Funktionalität anbieten und in geringerem Maße schritthalten mit den Erfordernissen des Marktes. Zu den *Visionaries* werden diejenigen *SIEMs* gezählt, die am Markt orientierte Lösungen anbieten mit einem großen Funktionsumfang, aber nur über einen geringeren Marktanteil verfügen. *Niche Players* sind auf dem Markt weniger stark etabliert und bieten *SIEMs* an, die in der Regel weniger Use Cases abdecken, also ebenfalls über einen geringeren Funktionsumfang verfügen.
Diese Analyse soll einen Überblick vermitteln über die in Dashboards verwendeten Darstellungen und Interaktionen und verbreitete Probleme identifizieren. Hierzu werden typische *SIEMs* aus allen drei Bereichen *Leaders*, *Visionaries* und *Challengers* untersucht, der vierte Bereich soll hier aufgrund seiner geringeren Relevanz vernachlässigt werden. Betrachtet werden im Quadranten *Leaders* zwei der drei mit Abstand führenden *SIEM*-Systeme (*NitroView* und *QRadar*). Sowie jeweils ein *SIEM*-System aus dem Quadranten *Visionaries* (*AlienVault*) und eines aus dem Quadranten *Challengers* (*Splunk*).
Natürlich kann hier nur ein Bruchteil der auf dem Markt vertretenen Lösungen untersucht werden, denn es existieren zur Zeit etwa um die achtzig verschiedene Produkte. Deshalb wurde versucht, Produkte auszuwählen, die als stellvertretend gelten können für die anderen Produkte im gleichen Quadranten.
Die Betrachtung wird hinsichtlich der drei sich bisweilen überschneidenden Bereiche *Information Design, Interface Design* und *Usability* geschehen. Für die Evaluation werden in erster Linie Guidelines aus dem Buch *Information Dashboard Design* (Few 2006), sowie die Bücher *The Visual Display of Quantitative Information* und *Envisioning Information* von *Edward Tufte* für den Bereich *Information Design* dienen (Tufte 2001; Tufte 1990), sowie etablierte Heuristiken aus dem Bereich *User Interface Design* und *Usability* (Nielsen 1994.) Nicht alle der in diesen Werken aufgeführten Prinzipien sind für diese Evaluation relevant, in der es ausschließlich um Dashboards geht.

Desweiteren sei an dieser Stelle angemerkt, dass die Evaluation sich in erster Linie auf Videovorführungen und Demos der Software stützt, ergänzt durch die in zwei Interviews mit Mitarbeitern des *Leibniz-Rechenzentrums* gewonnenen Erkenntnisse. Ein direktes Testen der Software gestaltet sich schwierig, da etwaige Testversionen der Software nicht einfach ohne das Vorhandensein einer entsprechenden Netzwerkinfrastruktur installiert werden können bzw. das Testen ohne die in das System einfließenden Datenquellen auch nicht sinnvoll durchzuführen ist. Auch die Evaluation am Arbeitsplatz eines Netzwerksicherheitsexperten ergab sich bisher nicht, da kaum Sicherheitsexperten dazu bereit sind, die Zeit zur Verfügung zu stellen bzw. hier auch Bedenken hinsichtlich des Datenschutzes bestehen.

Im Folgenden werden die oben beschriebenen Guidelines und Heuristiken kurz vorgestellt:

Information Design Guidelines

Fokussierung auf die Daten

Bei der Darstellung von Visualisierungen im Dashboard sollte darauf geachtet werden, die Visualisierung der Daten in den Vordergrund zu stellen. Zusätzliche rein schmückende Bestandteile sollten möglichst vermieden werden oder, falls dies nicht möglich sein sollte, auf ein Minimum reduziert werden. (Dies bedeutet nicht, dass Graphen keine ästhetische Qualität besitzen dürfen.) Auch sollten strukturierende Elemente wie beispielsweise Skalen oder Gitternetze nicht die gleiche visuelle Gewichtung erhalten wie die Daten selbst. (HIER TUFTE-ZITAT ZU DATA-INK RATIO)

Hervorheben wichtiger Informationen

Nicht alle dargestellten Informationen im Dashboard sind gleich wichtig. Nach Few (Vgl. Few 2006: 113ff.) ist außerdem zu unterscheiden zwischen immer wichtigen und nur zu einem bestimmten Zeitpunkt wichtigen Informationen. Für die erste Kategorie bietet sich in erster Linie die Positionierung auf dem Dashboard an. Grundsätzlich werden Informationen in der linken, oberen Ecke und im Zentrum als wichtiger wahrgenommen als an anderen Positionen. Informationen in der unteren, rechten Ecke werden als am wenigsten wichtig empfunden. Weitere Möglichkeiten des Hervorhebens sind z.B. Farbintensität, Größe oder Linienstärke. Attribute wie Farbton, Ausrichtung, Umrahmung, oder Markierung eines Elements mit einem Symbol eignen sich besonders, um einzelne gleichförmige Elemente in einer größeren Menge zu betonen. Die nur zu einem bestimmten Zeitpunkt wichtigen Informationen sollten dynamisch ihr Erscheinungsbild ändern und sich noch einmal stärker abgrenzen von den dauerhaft wichtigen Informationen.

Vergleiche ermöglichen

Häufig lassen sich dargestellte Daten nur in Relation beurteilen. Der Nutzer sollte die Möglichkeit haben, sowohl verschiedene Daten innerhalb eines Diagrammes miteinander vergleichen zu können, als auch über verschiedene Visualisierungen hinweg. Letzteres kann beispielsweise durch gleiche Farben erreicht werden, durch räumliche Nähe zueinander oder durch die Verwendung identischer Skalen. Hier kann man sich Erkenntnisse aus dem Bereich der Gestaltpsychologie zunutze machen. Im Gegensatz dazu sollte bei der Gestaltung darauf geachtet werden, dass unerwünschte Vergleiche nicht versehentlich stattfinden, weil Diagramme zu nah beieinander angeordnet sind oder eine Farbe unterschiedlichen Daten zugewiesen wird.

Übersicht ohne Details

Im Dashboard sollten nur die wirklich relevanten Informationen dargestellt sein. Detailinformationen lenken vom Wesentlichen ab. Das Dashboard sollte jedoch als Startpunkt dienen für eine genauere Analyse von im Dashboard sichtbaren Ereignissen.

Ästhetische Qualität

Es gilt mittlerweile als gesicherte Erkenntnis, dass Ästhetik in User Interfaces dazu beiträgt, die User Experience zu verbessern. Laut Norman fördern ästhetisch ansprechend gestaltete Interfaces die Toleranz gegenüber kleinen Fehlern, und erlauben den Nutzern, kreativer mit dem Produkt umzugehen. „*Positive affect makes people more tolerant of minor difficulties and more flexible and creative in finding solutions. Products designed for more relaxed, pleasant occasions can enhance their usability through pleasant, aesthetic design. Aesthetics matter: attractive things work better.*“ (Norman 2002). Hierzu gehören z.B. Dinge wie die sorgfältige Abstimmung von im Interface verwendeten Farben oder die Auswahl geeigneter Schriften, die im Zusammenspiel mit der restlichen Gestaltung harmonisch und ansprechend wirken. Wichtig zu betonen hierbei ist, dass mit Ästhetik hier vor allem die ästhetische Gestaltung der Daten gemeint ist. Die Gestaltung sollte die Usability idealerweise unterstützen keinesfalls behindern, wie bereits weiter oben unter Fokussierung auf die Daten beschrieben.

Konsistenz

Gleiche Bedeutungen sowohl in Visualisierungen als auch im Interface sollten auch auf die gleiche Art und Weise dargestellt werden. Hierzu (Few 2006: 168): „*Differences in appearance always prompt us to search, whether consciously or unconsciously, for the significance of those differences.*“ Auch sollten möglichst gleiche Visualisierungen verwendet werden, um gleicharti-

ge Datenzusammenhänge darzustellen.

Usability und Interface Design Guidelines

Einfache Bedienbarkeit

Das Interface eines Dashboards sollte soweit wie möglich reduziert sein. Jedes zusätzliche Element, jede zusätzliche Information muss vom Nutzer erlernt werden und birgt die Gefahr, missverstanden zu werden (Vgl. Nielsen 1994: 115). Dies bedeutet nicht, dass die Funktionalität eingeschränkt sein sollte, vielmehr sollte es verschiedene Ebenen der Komplexität geben, so dass mehr Funktionalitäten bei Bedarf aufgerufen werden können, der Nutzer aber nicht permanent damit konfrontiert ist. (Vgl. Nielsen 1994: 120ff.) Weiterhin sollten die teilweise bereits unter *Information Design Guidelines* zur Sprache gekommenen Gestaltungsprinzipien eingesetzt werden, um das Interface des Dashboards zu strukturieren, zu ordnen und somit für den Nutzer leichter nachvollziehbar zu machen. Diese basieren auf den aus der Wahrnehmungspsychologie bekannten Gestaltprinzipien. Hier sind vor allen Dingen das Gesetz der Nähe und das Gesetz der Ähnlichkeit nach Wertheimer, sowie das Gesetz der gemeinsamen Region, das Gesetz der Gleichzeitigkeit und das Gesetz der verbundenen Elemente zu nennen (Rock and Palmer 1990). Durch das Gruppieren von zusammengehörigen Elementen des Interfaces durch räumliche Nähe, ähnliche Erscheinung oder durch das Umschließen mit Linien, Hinterlegen mit Hintergründen oder durch das Verbinden kann so eine Zusammengehörigkeit für den Nutzer offenbar gemacht werden. Das gleichzeitige Verändern von Elementen deutet ebenfalls eine Zusammengehörigkeit an. Umgekehrt können mit Hilfe der Gestaltgesetze aber auch Elemente von den anderen separiert werden und so explizit in den Vordergrund gerückt werden.

Sprache der Zielgruppe verwenden

Das Dashboard-Interface sollte in der Darstellung und in der Wahl der verwendeten Worte sich an den Vorstellungen (*Mentalen Modellen*) und den gewohnten Termini der Nutzer orientieren. Vor der Konzeption eines solchen Softwareproduktes muss deshalb mit Methoden wie Interviews, Workshops oder Beobachtungen ein möglichst genaues Bild von den Nutzern und deren Bedürfnissen und Vorstellungen erzeugt werden. Dazu gehört beispielsweise auch, dass für den Nutzer unsichtbare Prozesse, die im Hintergrund ablaufen, im Interface anders dargestellt werden, als sie in Wirklichkeit sind, weil diese Darstellung für den Nutzer vertrauter ist und es ihm leichter fällt, damit umzugehen. Hier kommen häufig Metaphern, aus der analogen Welt entlehnt, zum Einsatz.

Feedback

Der Nutzer sollte nicht im Unklaren darüber gelassen werden, was das System gerade tut. Hierzu gehört sowohl positives, als auch negatives Feedback. So sollte der Nutzer nicht nur auf Fehler aufmerksam gemacht werden, sondern auch auf zusätzliche Informationen, die verfügbar werden, wenn der Nutzer bestimmte Interaktionen durchführt (Vgl. Nielsen 1994: 134). Hierzu gehört beispielsweise das Verändern des Mauscursors, wenn der Nutzer mit dem Mauszeiger über bestimmte Bereiche des Interfaces fährt (Handcursor, um zu zeigen, dass hier etwas verschoben werden kann). Meldungen des Systems wie etwa Fehlermeldungen oder Warnungen bei bestimmten Interaktionen sollten in einer für den Nutzer verständlichen Weise ausgedrückt werden (Vgl. Nielsen 1994: 134).
Ein kritischer Faktor in Interfaces generell ist insbesondere die Reaktionszeit eines Systems. Eine Zehntelsekunde wird vom Nutzer als sofortige Reaktion wahrgenommen, bei mehr als einer Sekunde wird der Nutzer in seinem Fluss unterbrochen. Wird der Nutzer länger als zehn Sekunden unterbrochen, wird er in der Regel sich anderen Aufgaben zuwenden wollen. In diesen Fällen sollte das System anzeigen, wann der Prozess voraussichtlich abgeschlossen sein wird, soweit voraussagbar (Vgl. Nielsen 1994: 135). Lässt sich dies nicht voraussagen, sollte auf andere Weise kommuniziert werden, dass das System etwas tut. Dies kann zum Beispiel durch einen sich drehenden Ball geschehen (wie von manchen Betriebssystemen bekannt) oder in einer Reihe nacheinander gezeichnete Punkte (Vgl. Nielsen 1994: 137).

Exit und Undo

„A basic principle for user interface design should be to acknowledge that users will make errors no matter what else is done to improve the interface, and one should therefore make it as easy as possible to recover from these errors.“ (Nielsen 1994: 139)
Gemäß diesem Prinzip sollte darauf geachtet werden, dass der Nutzer stets die Möglichkeit hat, durchgeführte Aktionen rückgängig zu machen oder beispielsweise aufgerufene Ansichten wieder zu schließen. Die Interface-Elemente sollten im Interface gut erkennbar sein. Der Nutzer sollte nicht auf eine Tastenkombination o.Ä. angewiesen sein, um eine bestimmte Ansicht wieder zu schließen oder einen Schritt zurückzugehen.

QRadar

Hersteller: IBM
Analysegrundlage: Demo 1 – Demos on Demand (27.03.2013), http://goo.gl/HlqJv;
Demo 2 – Youtube (27.03.2013), http://www.youtube.com/watch?v=B7mMFFVj7lc

IBMs QRadar gehört laut *Gartner* zu den fünf Marktführern im Bereich der *SIEM*-Tools. In *QRadar* sind die einzelnen Elemente des Dashboards in dichter Form nebeneinander als kleine Fenster mit der typischen, durch Betriebssysteme bekannten Titelleiste mit Bedienelementen am rechten Rand (z.B. Schließen, Einstellungen, ...) angeordnet. Die Darstellung der Widgets beruht auf vorgefertigten Suchstrings mit Filtern. Diese können entweder aus einer Liste ausgewählt werden oder durch den Nutzer erstellt werden. Es können verschiedene Dashboards für unterschiedliche Zwecke/ Sichtweisen angelegt werden. Die verschiedenen Funktionalitäten des Systems sind auf mehrere Tabs aufgeteilt. Die Diagramme der Dashboards sind in der Regel mit einem Link zu den Inhalten in den einzelnen Tabs verbunden. *QRadars* User Interface wirkt insgesamt etwas konservativ und kleinteilig.

Abb. 1: QRadar Dashboard – Ansicht A (Screenshot Demo 2)

Information und Interface Design

1 QRadar setzt Verläufe und 3D-Darstellungen (z.B. für Säulendiagramme) ein. Diese Visualisierungen lenken vom eigentlich zu kommunizierenden Inhalt ab.

2 Die Zuordnung der Farben zu den grafischen Elementen des Dashboards scheint willkürlich vorgenommen zu werden. Gleiche Farben werden zur Darstellung unterschiedlicher Daten verwendet. Es ist nicht klar, ob Farben durch den Nutzer angepasst werden können.

3 Eines der primären Ziele eines Dashboards, einen Überblick über alle wichtigen Vorgänge zu liefern, wird durch die Möglichkeit, mehr Widgets hinzuzufügen, als auf eine Seite passen, sabotiert.

4 Alle Elemente wie Schrift, Grafiken und Skalen haben ein ähnliches visuelles Gewicht, die Daten sollten stärker betont werden und heraustreten.

5 Generell ist die Zusammenstellung der Farben als nicht harmonisch anzusehen. Farbkontraste sind häufig zu hoch und es bleibt in den Widgets kaum Weißraum übrig, der das gesamte Dashboard etwas auflockern würde und dem Nutzer die Betrachtung erleichtern würde. Auch wird kaum von den Gestaltungsmöglichkeiten durch Schrift Gebrauch gemacht, durch Kontraste in der Größe, dem Schriftschnitt oder der Schriftart.

Abb. 2: QRadar Dashboard – Ansicht A (Screenshot Demo 2)

6 Einzelne Diagramme, z.B. Flächendiagramme, wirken sehr fein aufgelöst, so dass sie nur noch schwer zu lesen sind. Eine derartig feine Auflösung wär eher angebracht in einer vom Dashboard aus aufgerufenen Detailansicht.

7 Die Zahlenangaben in den einzelnen Diagrammen sind sehr exakt. Es ist zu überlegen, ob durch abgekürzte Werte, die einen ausreichend genauen Eindruck vermitteln können, möglicherweise Platz eingespart werden könnte.

8 Die Fensterleisten der einzelnen Widgets beanspruchen sehr viel Platz und lenken von den Inhalten des Dashboards ab. Auch die umrahmenden Linien sorgen für weitere Unruhe.

9 Zusammenhängende Widgets lassen sich in räumlicher Nähe zueinander positionieren, so dass semantisch zusammenhängende Gruppen gebildet werden können.

10 Wenn der Nutzer den Link „View in ...“ aufruft, der im unteren Bereich jedes Widgets zu finden ist, gelangt er zu einer Detailansicht der Daten. Er verliert jedoch hierbei den Kontext des Dashboards und gelangt zu einer ganz neuen Ansicht in einem anderen Tab. (Z.B. im oberen Fall zu dem Tab *Network Activity*, siehe Abb. 3)

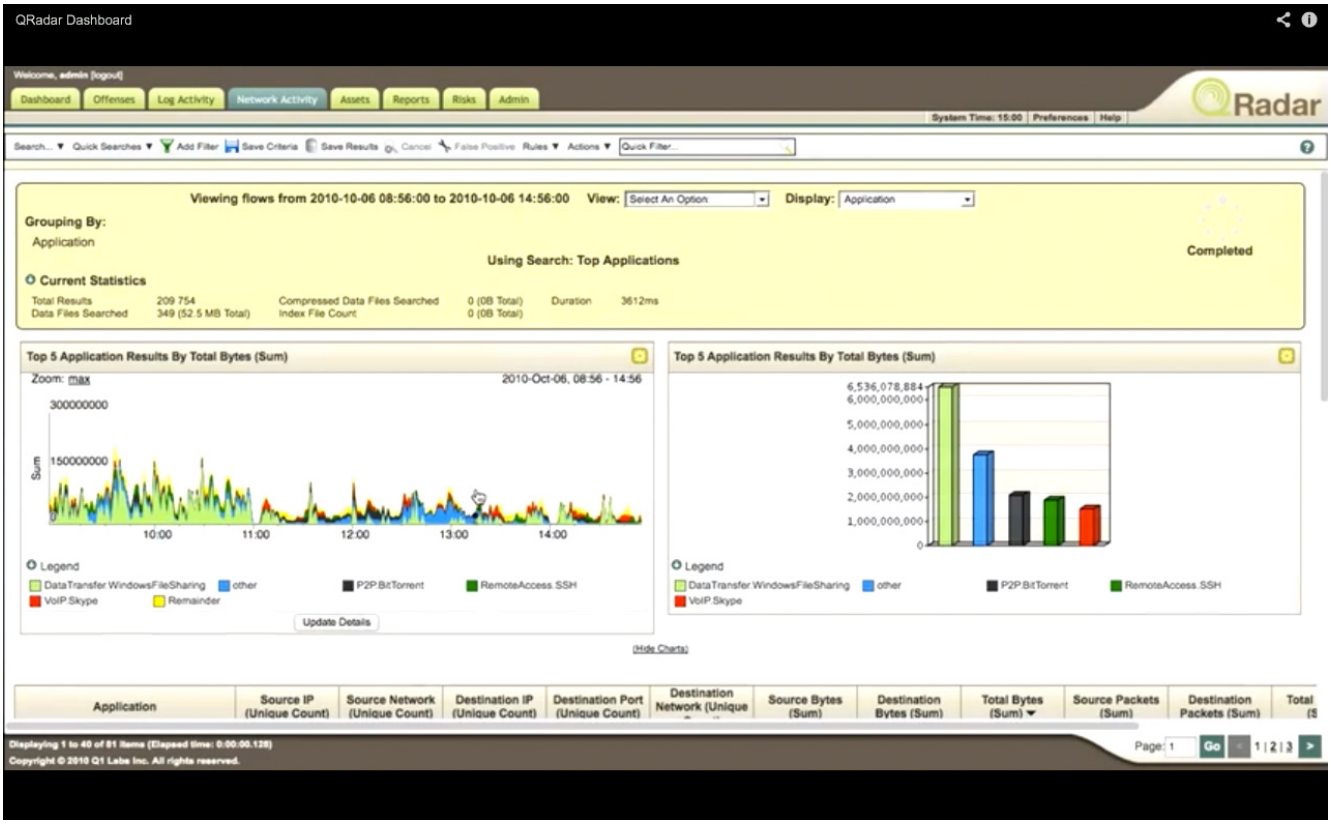

Abb. 3: QRadar Detailansicht in Tab Network Activity – Ansicht B (Screenshot Demo 2)

Abb. 4: QRadar Dashboard – Ansicht C (Screenshot Demo 1)

11 Die Legende für die einzelnen Widgets scheint standardmäßig eingeklappt zu sein. Hier ist fraglich, ob diese Funktionalität wirklich benötigt wird, um ein bisschen mehr Platz zu bekommen. Der Platz könnte an anderer Stelle sinnvoller eingespart werden – z.B. bei den Titelleisten der Widgets.

12 Noch ist nicht klar, inwiefern der Nutzer selber bestimmen kann, welche Art der Visualisierung verwendet wird für die zugrundeliegenden Daten.

Splunk

Hersteller: Splunk, Inc.
Analysegrundlage: Demo 3 – Splunk 4.3 Overview (27.03.2013), http://www.youtube.com/user/splunkvideos?feature=watch;
Demo 4 – Splunk 4.3 Demo (27.03.2013), http://www.youtube.com/watch?v=Zds8qw-CnTI

Gartner ordnet die Software *Splunk* der gleichnamigen Firma in ihrer Studie in den Bereich *Challengers* ein. *Splunk* bietet neben der *SIEM*-Funktionalität und der Datenkorrelation sicherheitskritischer Daten außerdem vor allem Möglichkeiten zur Verwaltung von Anwendungsdaten, Infrastruktur-, sowie Prozessdaten. Die einzelnen Widgets des Dashboards basieren auf vom Nutzer zusammengestellten Suchstrings. Wie in anderen Lösungen auch können unterschiedliche Dashboards für unterschiedliche Zwecke zusammengestellt werden. Insgesamt fällt *Splunk* durch ein moderneres, reduzierteres User Interface in dieser Analyse auf.

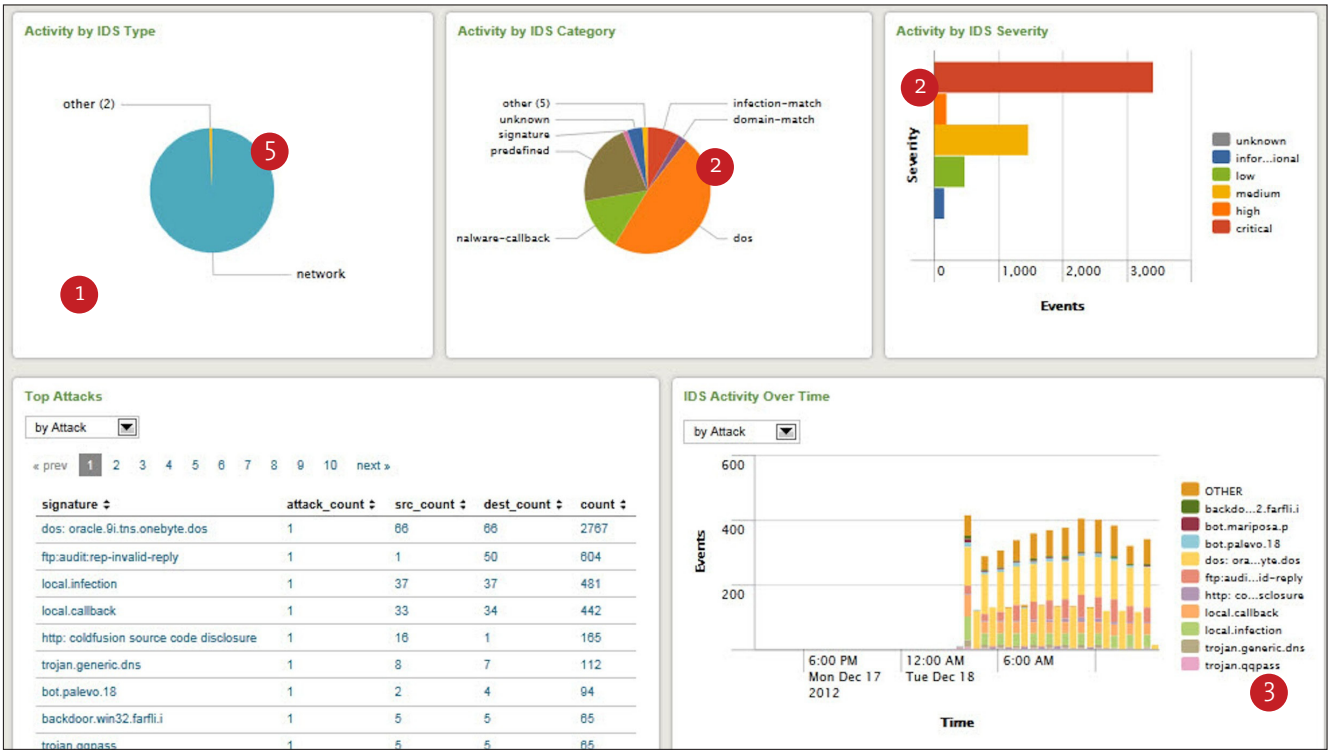

Abb. 5: Splunk Dashboard – Ansicht A (http://www.computerwoche.de/a/denken-wie-ein-angreifer,2529952)

Information und Interface Design

1 Die Gestaltung des Dashboards wirkt insgesamt zurückgenommen und aufgeräumt. Eine großzügige Verwendung von Weißraum trennt die einzelnen Widgets eindeutig voneinander.

2 Nebeneinanderstehende Widgets nutzen die gleichen Farben für unterschiedliche Zusammenhänge. Die Farben scheinen willkürlich zugeordnet zu sein.

Der Nutzer hat die Möglichkeit, mehr Widgets hinzuzufügen, als Platz auf einer Seite vorhanden ist. Er muss dann scrollen, um alles sehen zu können.

3 Die Farbzuweisungen in den Diagrammen werden willkürlich vorgenommen. Zwar sind die verwendeten Farben ästhetisch aufeinander abgestimmt, aber bisweilen wird die

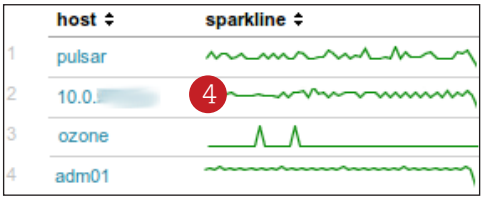

Abb. 6: Sparklines

Anzahl der Farben in einem Diagramm so groß, dass es schwierig wird, diese auseinanderzuhalten. Wie es scheint, hat der Nutzer im Nachhinein keine Möglichkeit, diese zu verändern.

4 Der Nutzer hat die Auswahl zwischen einer großen Menge verschiedener Diagramme, um seine Daten darzustellen. Allerdings ist nicht jede Visualisierung gleich gut geeignet. Einige Visualisierungen sind grundsätzlich nie zu empfehlen, wie z.B. das Pie Chart. Einige Visualisierungen sind ungewöhnlich

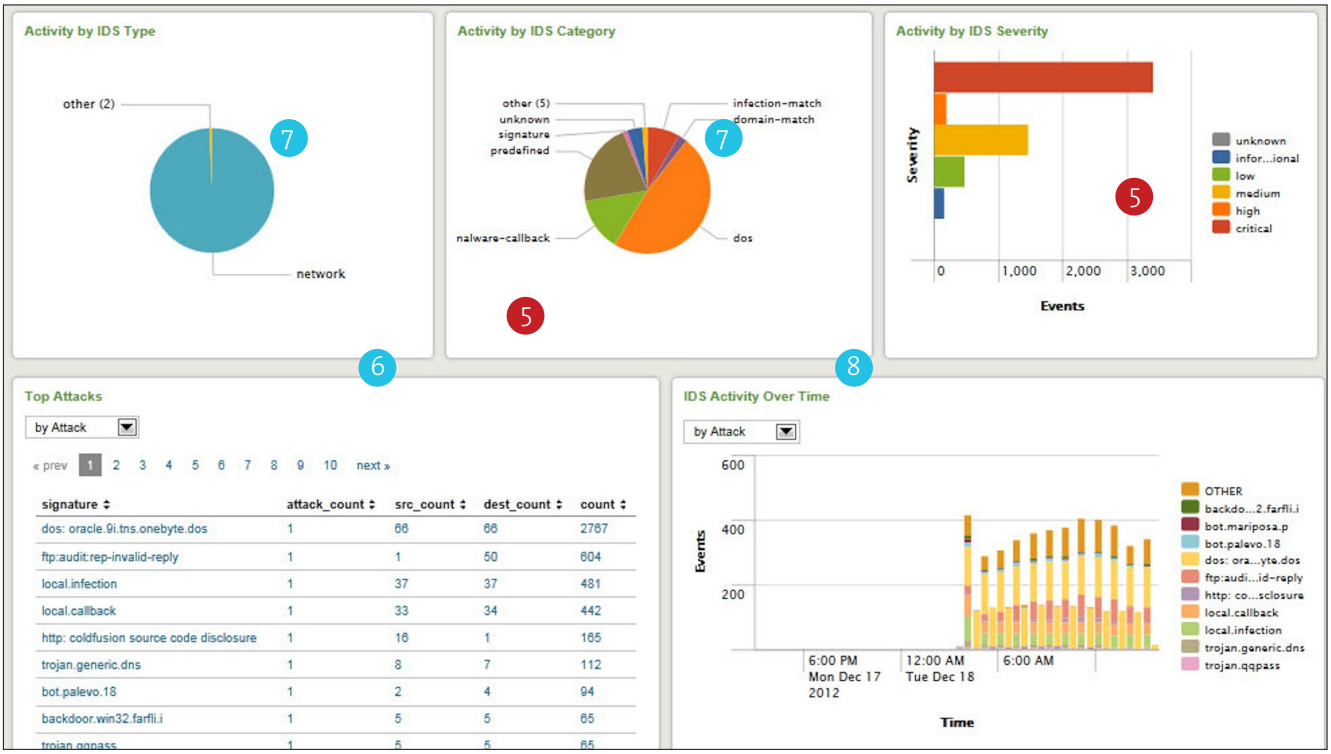

Abb. 7: Splunk Dashboard – Ansicht A

und nicht typisch für Dashboards, wie z.B. sogenannte Sparklines, siehe Abb. 6.

Ästhetisch weist das Dashboard eine höhere Qualität als viele Konkurrenzprodukte auf. Farben werden bewusst zusammengestellt, Schriften sind aufeinander abgestimmt und Weißraum wird bewusst zur Gliederung eingesetzt.

5 Strukturierende, gliedernde Elemente treten durch dezente Grautöne in den Hintergrund.

6 Zusammenhängende Widgets lassen sich verschieben, skalieren und ohne Schwierigkeiten in räumlicher Nähe zueinander positionieren.

7 Problematisch: Freie Wahl von Visualisierung führt dazu, dass unter Umständen gleiche Visualisierungen für vollkommen unterschiedliche Daten verwendet werden.

8 Widgets sind durch Farbe (grau und weiß) und Schatten voneinander getrennt. Diese subtile Art der Trennung drängt sich nicht in den Vordergrund und lenkt nicht von den Inhalten der Widgets ab.

Abb. 8: Splunk Dashboard – Ansicht B

9 Unter den Diagrammen befindet sich ein Link „View Results“, mit dem man die dargestellten Daten im Detail betrachten kann (In Abb. 5 bzw. Abb.7 ist dieser nicht zu sehen, weil der Edit-Modus eingeschaltet ist).

AlienVault Unified SIEM

Hersteller: AlienVault
Analysegrundlage: Demo 5 – AlienVault Unified SIEM v3 (27.03.2013): http://www.youtube.com/watch?v=xtBjA1UCB5I

AlienVault rangiert in der Gartner-Studie unter *Visionaries*. Die Software basiert auf der Open Source-Lösung *Open Source SIM (OSSIM)*. Mit der Software lässt sich eine Vielzahl von Dashboards für unterschiedliche Nutzungszwecke erstellen und verwalten. Ähnlich wie bei *QRadar* sind die einzelnen Funktionsbereiche der Software auf unterschiedliche Tabs verteilt. Im Gegensatz dazu gibt es aber nicht einen zentralen Dashboardbereich, sondern jeder Tab kann wieder eigene Dashboards aufweisen. Das User Interface wirkt insgesamt reduziert, allerdings grafisch etwas uneinheitlich.

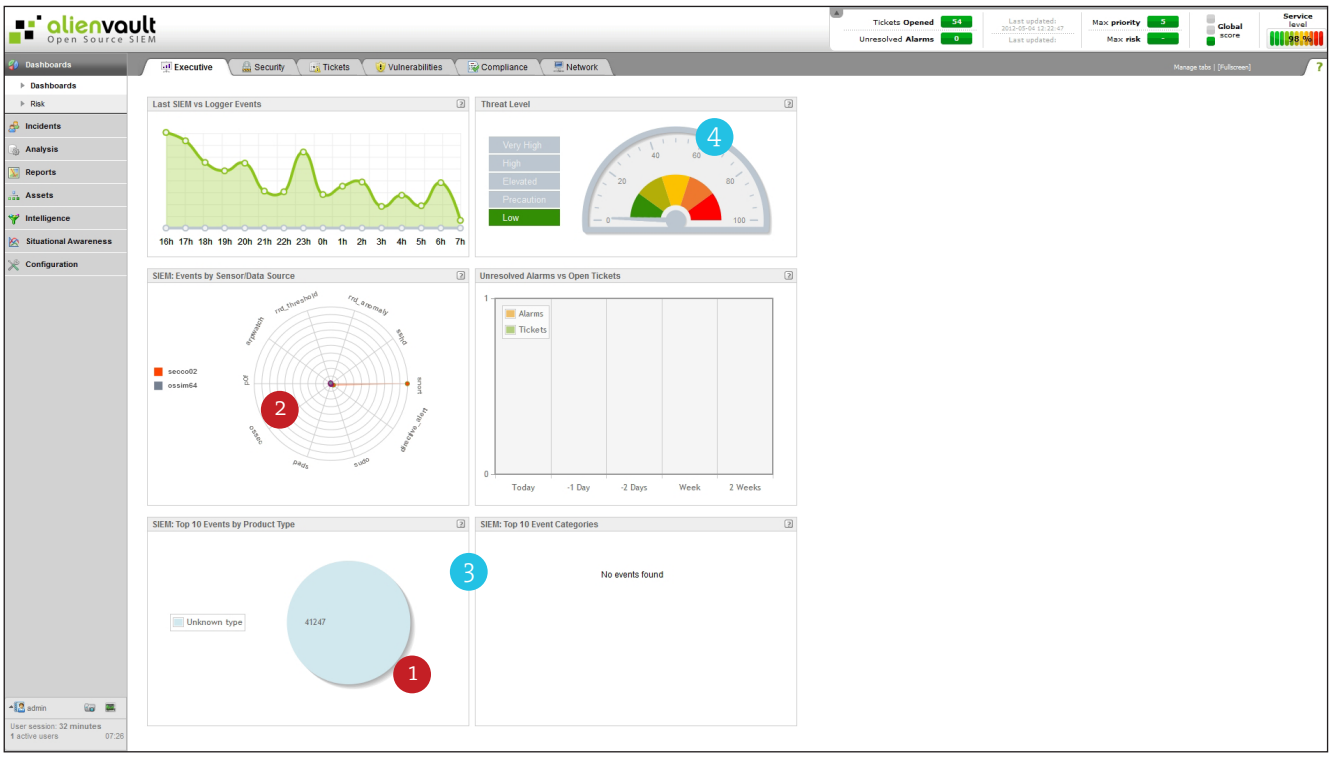

Abb. 9: AlienVault Unified SIEM Dashboard – Ansicht A (Screenshot Leibniz-Rechenzentrum)

Information und Interface Design

1 Schattenwurf von grafischen Elementen, z.B. einzelnen Säulen in einem Säulendiagramm oder von Pie Charts ist Dekoration, die vom eigentlichen Inhalt ablenkt. Auch tritt der Schattenwurf nicht bei allen Elementen auf, ist also nicht konsistent.

2 Strukturelemente wie Gitterlinien oder Skalen treten manchmal in den Hintergrund, manchmal bekommen sie zu viel Gewicht, so dass sie von den darzustellenden Daten ablenken.

Dashboards können größer als eine Seite sein. Damit geht das Alleinstellungsmerkmal von Dashboards, eine Gesamtübersicht auf einen Blick zu bieten, verloren. Hier ist zu überlegen, ob es sinnvoll sein könnte, den zur Verfügung stehenden Platz tatsächlich auf eine Seite zu begrenzen.

Gestalterisch vermag das Dashboard insgesamt nicht zu überzeugen. Zwar wird in der Regel darauf geachtet, durch ausreichend Weißraum ein aufgeräumtes Erscheinungsbild zu erzeugen, jedoch harmonieren die verwendeten Farben kaum miteinander und Typografie spielt nur eine untergeordnete Rolle. Insgesamt wirkt das Erscheinungsbild sehr nüchtern.

3 Die Umrandung der einzelnen Widgets mit dezenten grauen Linien lenkt nicht von den Inhalten ab.

4 Teilweise werden metaphorische Visualisierungen verwendet, bei denen fraglich ist, ob sie dem Zweck angemessen sind.

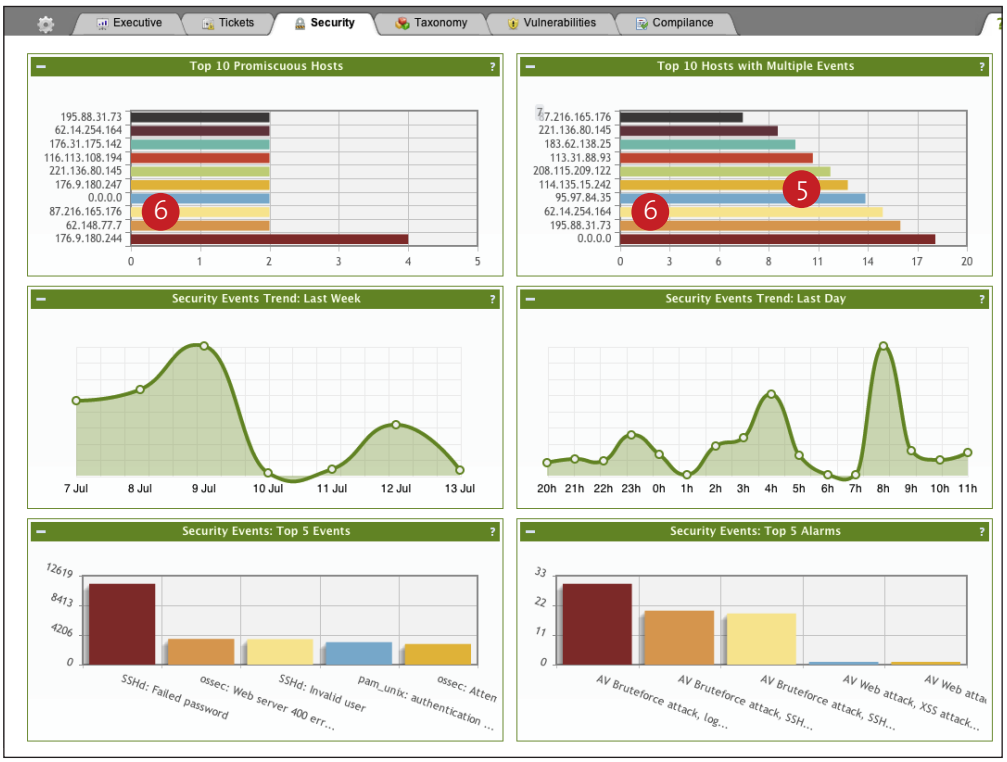

Abb. 10: AlienVault Unified SIEM Dashboard – Ansicht B

5 Farben werden offenbar willkürlich zugewiesen, teilweise wirken die Diagramme durch eine bestimmte Farbzusammenstellung sehr blass und wenig ansprechend.

6 Wenn in verschiedenen Diagrammen gleiche Daten dargestellt werden, sollten diese auch mit der gleichen Farbe gekennzeichnet werden. Dies ist bei AlienVaults Lösung nicht gegeben. (In Abb. 10 ist ersichtlich, dass die Farben nach Reihenfolge zugewiesen werden, nicht inhaltlich.)

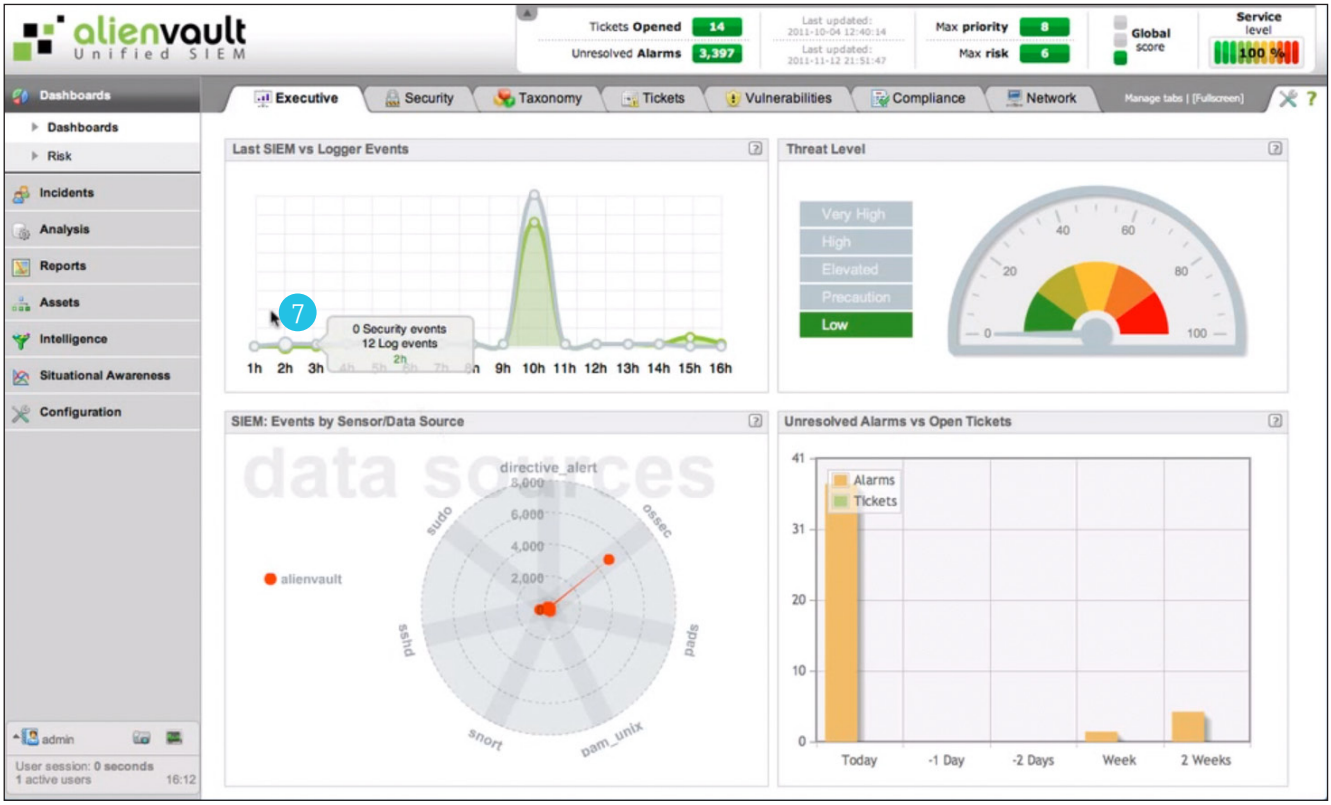

Abb. 11: AlienVault Unified SIEM Dashboard – Ansicht C (Screenshot Demo 5)

7 Wenn der Nutzer über Diagramme mit der Maus fährt, werden Elemente gehighlightet und in manchen Fällen mit einem kleinen Text-Label versehen, das zusätzliche Informationen liefert.

NitroView/
Enterprise Security Manager

Hersteller: AlienVault
Analysegrundlage: Demo 6 – Tracking an ICS cyber attack with NitroView (27.03.2013) : http://www.youtube.com/watch?v=_c8D4oeFxj8&list=UUvUQ-18gECNiAnk4jFPIohQ&index=1
Demo 7 – McAfee GTI and McAfee SIEM Demo (27.03.2013) , http://www.mcafee.com/us/products/enterprise-security-manager.aspx#vt=vtab-Demo

Nitroview (bzw. seit kurzem als *Enterprise Security Manager* vertrieben) ist eine *SIEM*-Lösung von *McAfee*, die laut Gartner zu einem der fünf Marktführer im Bereich *SIEMs* gehört. Ähnlich wie *IBMs QRadar* bedient sich auch *McAfee* typischer GUI-Elemente, die man aus Betriebssystemen kennt, wie etwa Titelleisten mit Buttons zum Maximieren u.Ä. Es lassen sich mehrere Dashboards für unterschiedliche Kontexte erstellen. Insgesamt wirkt das User Interface des Dashboards eher konservativ und bietet dem Auge wenig Raum zum ruhen.

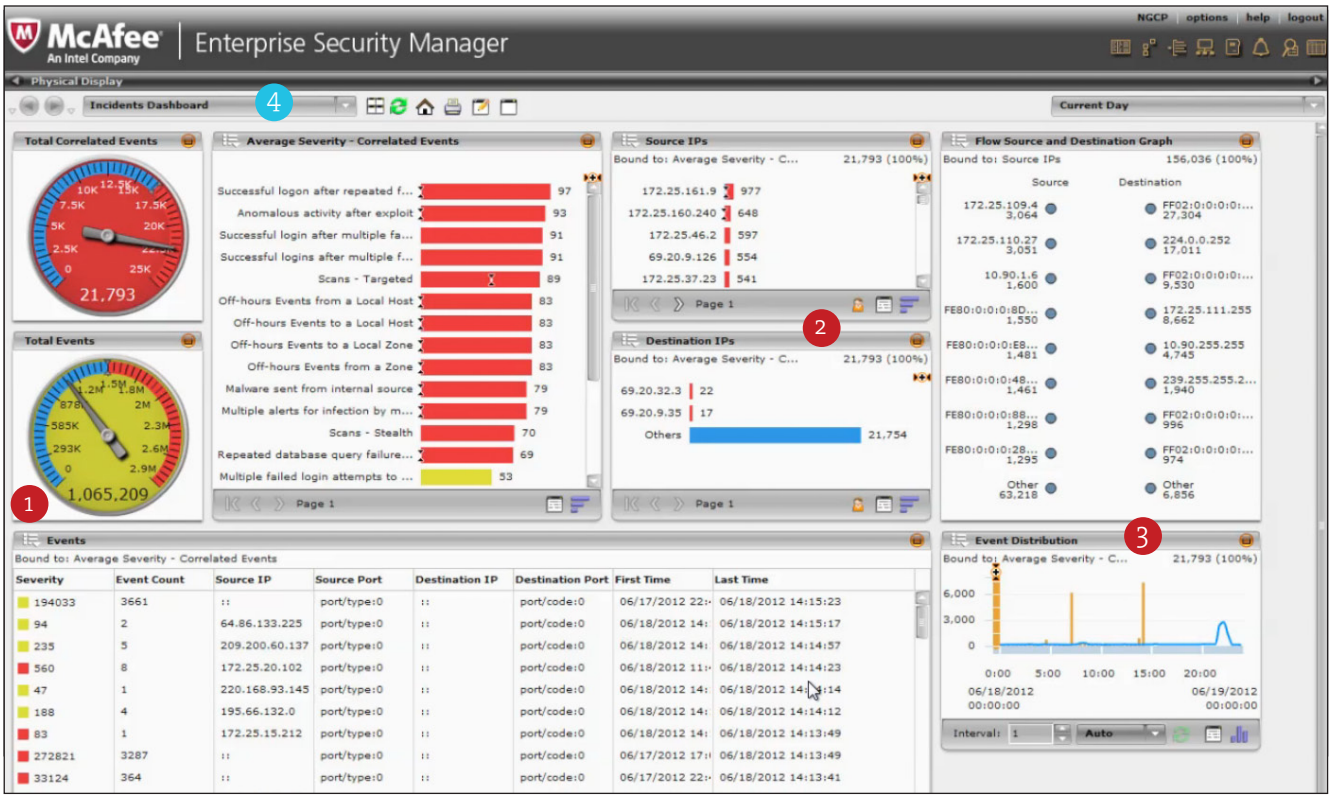

Abb. 12: McAfee Enterprise Security Manager – Ansicht A (Screenshot Demo 7)

Information und Interface Design

1 Darstellung teilweise reduziert mit Fokus auf den darzustellenden Daten, teilweise aber auch Einsatz von schmückenden visuellen Mitteln, die die Lesbarkeit eher erschweren wie etwa das Speedometer, das sich durch die Verwendung von Verläufen und dreidimensionalen Darstellungen von den einfachen flachen Balkendiagrammen abhebt.

2 Widgets sind auf dem Dashboard frei positionierbar, so dass zusammengehörige Widgets auch nebeneinander angeordnet werden können.

3 Die Darstellung ist insgesamt konservativ: Einzelne Widgets sehen aus wie kleine Fenster mit Titelleiste und Maximize-Button. Die Überschriften in den einzelnen Titelleisten sind so klein, dass sie auf den ersten Blick nur schwer zu erfassen sind. Weißraum als ästhetisches und strukturierendes Element kommt nur in geringem Maße zum Einsatz. Die verwendeten Farben kontrastieren häufig zu sehr miteinander.

– Widgets vermitteln Übersicht, Elemente sind einzeln auswählbar. Doppelklick öffnet diese in neuem Fenster als Detail.

4 Verschiedene Dashboards existieren für verschiedene Zusammenhänge, das Verhältnis dieser zueinander wird aber im Interface nicht in ausreichendem Maße deutlich gemacht.

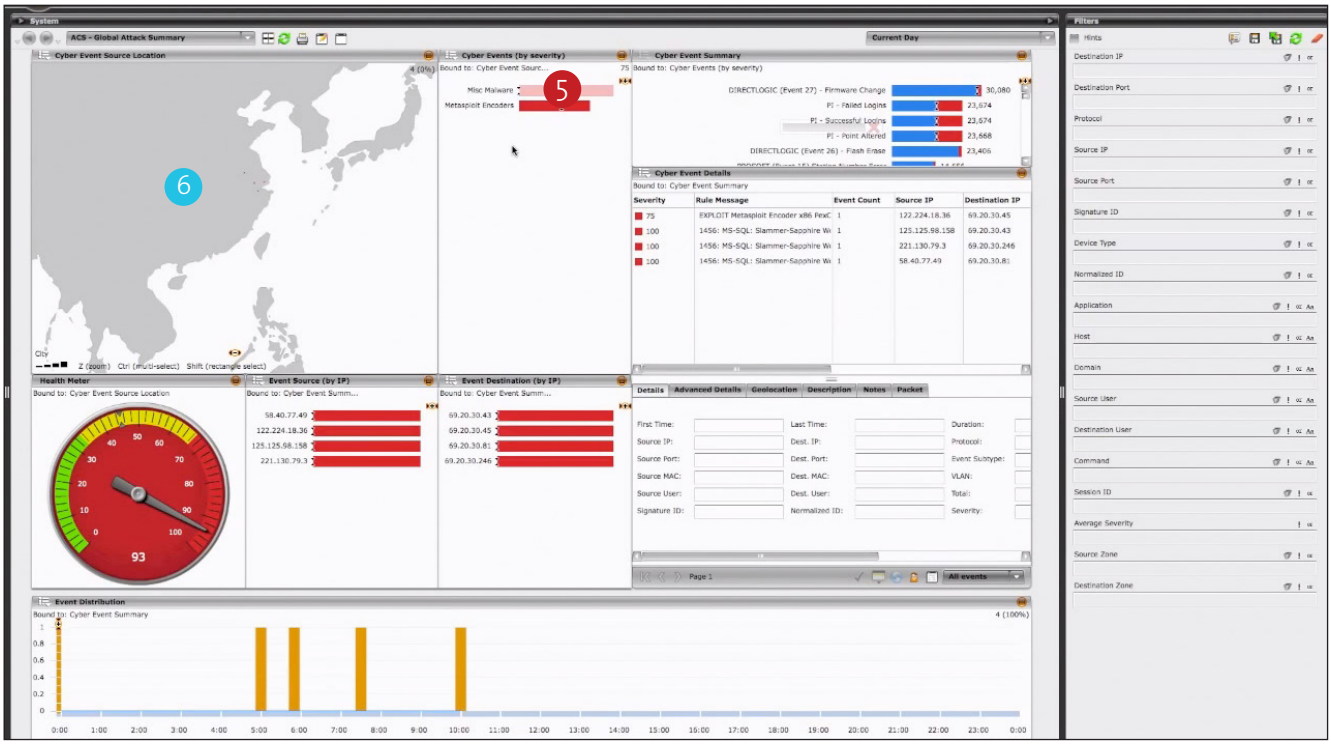

Abb. 13: McAfee Enterprise Security Manager – Ansicht B (Screenshot Demo 6)

5 Das Dashboard unterstützt sogenanntes Brushing, d.h. die Auswahl einzelner Elemente in einem Widget führt dazu, dass diese Elemente als Filter gesetzt werden und die Darstellung anderer mit diesen Daten verknüpfter Widgets ebenfalls entsprechend dieser Auswahl gefiltert werden. Wenn also bspw. nur Source-IPs einer bestimmten Region auf der Karte ausgewählt werden, dann wird in den anderen Widgets, die mit der Karte verknüpft sind, die Darstellung ebenfalls nur auf die mit dieser Source-IP zusammenhängenden Daten beschränkt.

6 Bereiche können auf Karte ausgewählt werden (Brushing), Auswahl wird jedoch nicht angezeigt, der Nutzer erhält also keinerlei Feedback darüber, auf welchen Bereich sich die Filterung bezieht .

Abb. 14: McAfee Enterprise Security Manager – Ansicht C (Screenshot: Leibniz-Rechenzentrum, März 2013)

7 Soweit sich aus den Demonstrationen schließen lässt, sind Farbzuweisungen nicht immer konsistent über mehrere Widgets hinweg.

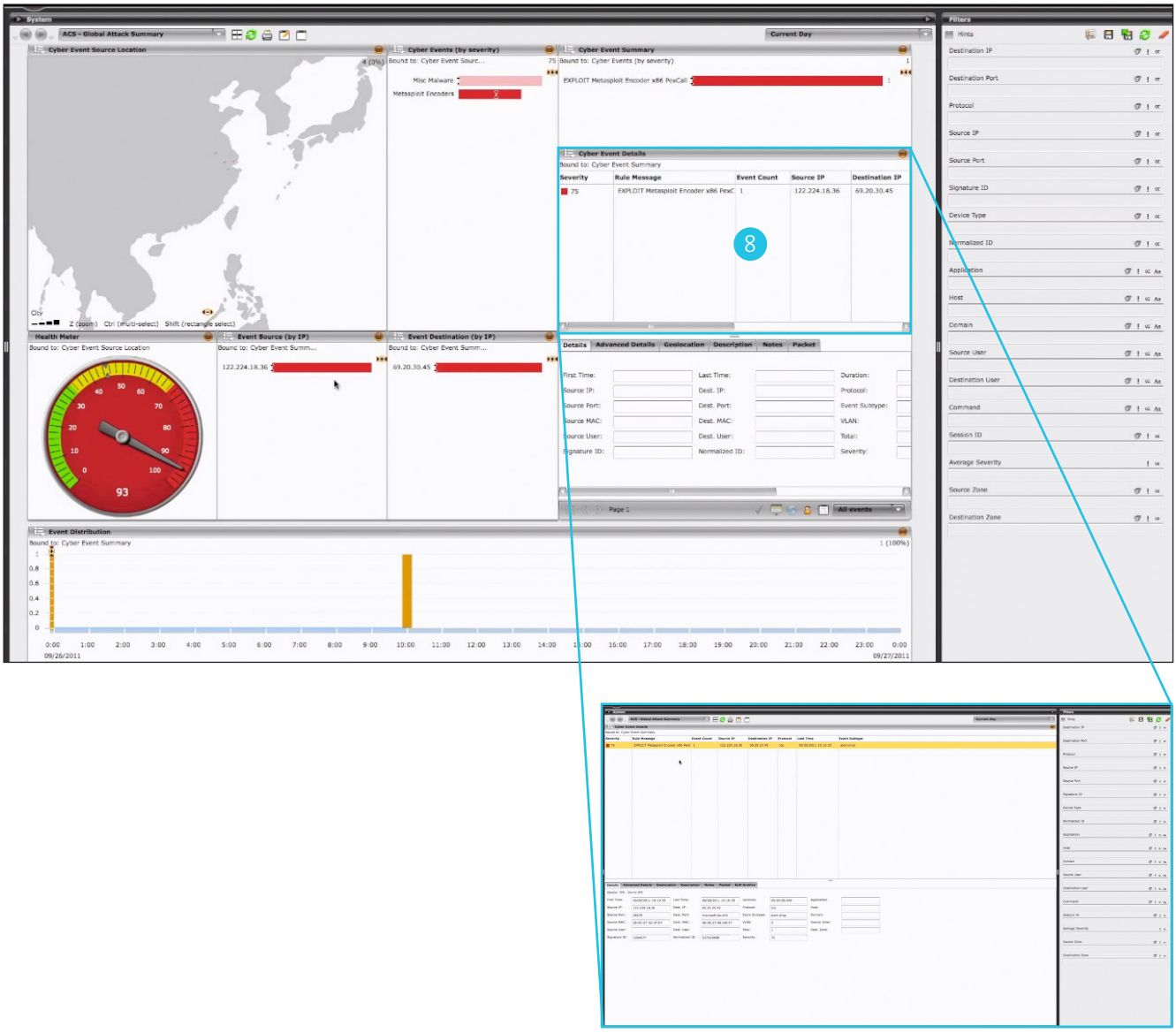

Abb. 15: McAfee Enterprise Security Manager – Ansicht D (Screenshot Demo 6)

8 Detailinformationen werden sichtbar, sobald man einzelne Widgets maximiert.

Zusammenfassung

Allen betrachteten *SIEM*-Lösungen ist gemein, dass sie es dem Nutzer erlauben eine Vielzahl verschiedener Dashboards für unterschiedliche Zwecke anzulegen. Bisweilen ist aber die Organisation und Verwaltung der Dashboards für den Nutzer nicht leicht nachvollziehbar. Hier können am ehesten *Splunk* und *AlienVault* überzeugen. *QRadar* besitzt zwar auch einen zentralen Dashboardbereich, allerdings tauchen Diagramme auch an vielen anderen Stellen auf, an denen man sie nicht erwarten würde. Die Informationsarchitektur ist hier uneindeutig. *NitroViews* Dashboard-Verwaltung erscheint wenig strukturiert.

Die Tatsache, dass bei einer derart großen Menge an komplexen Daten, die in einem *SIEM*-System zusammenkommt, mehrere Dashboards erforderlich werden, um Übersicht alle Daten zu schaffen, ist leicht nachvollziehbar. Besonders, wenn man bedenkt, dass das *SIEM* ganz unterschiedliche Funktionalitäten miteinander vereint, die jeweils spezielle Sichtweisen auf die Daten erforderlich machen. Allerdings ist bei allen untersuchten *SIEM*-Lösungen festzustellen, dass die Dashboards ansich auch wieder die Größe eines Bildschirms sprengen können, so dass gescrollt werden muss, um alles zu sehen. Eine Tatsache, die der eigentlichen Kernaufgabe von Dashboards, einen Überblick zu verschaffen, zuwiderhandelt.

Bei dreien der vier betrachteten Tools fällt auf, dass visuelle Mittel verwendet werden, die teilweise vom Inhalt der Daten ablenken. Hierzu gehören etwa Verläufe, oder Schattenwürfe oder auch dreidimensionale Darstellungen. Darstellungen rein ästhetischer Natur, die in Interfaces, in denen weniger große und komplexe Datenmengen visualisiert werden sollen, vielleicht noch hinnehmbar sind, tragen im Falle von *SIEMs* erheblich zu einer Verschlechterung der Usability bei. Einzig *Splunk* bildet hier die Ausnahme mit seinen klaren, reduzierten Darstellungen.

Bei allen vier Lösungen lässt sich die Frage nach der Angemessenheit der verschiedenen zur Verfügung stehenden Diagramme stellen. Darstellungen wie das Kuchendiagramm sind häufig zu sehen, grundsätzlich ist aber generell von diesem abzuraten, da es wesentlich schwerer ist, hiermit Mengen miteinander zu vergleichen. Auch die Metapher des Messinstrumentes wird von allen Produkten angeboten. Die damit dargestellten Daten ließen sich aber auf kleinerem Raum, z.B. durch einen einfachen Balken, wesentlich prägnanter darstellen.

Ein weiterer Schwachpunkt aller vier *SIEMs* ist die Art und Weise, wie Farben eingesetzt werden. Diese werden offenbar willkürlich zugewiesen, so dass man Daten in verschiedenen Widgets mit der gleichen Farbe fälschlicherweise für identisch hält oder umgekehrt nicht wahrnimmt, dass in unterschiedlichen Widgets gleiche Daten auftauchen, weil die Farben nicht identisch sind. Der willkürliche Einsatz von Farben hat auch zur Folge, dass diese teilweise stark miteinander kontrastieren, das Auge ablenken bzw. auch ästhetisch

nicht zusammenpassen. Wichtige Daten können so zumindest mit dem Mittel der Farbe nicht hervorgehoben werden.
Ästhetisch betrachtet ist nur bei *Splunk* festzustellen, dass bei der Abstimmung der Farben aufeinander etwas mehr Sorgfalt geherrscht hat. Auch typografisch und in Bezug auf die Verwendung von Weißraum differenziert sich *Splunk* hier klar von den drei Konkurrenten.
Bei *NitroView* fiel besonders auf, dass in einzelnen Widgets Elemente direkt ausgewählt werden, die dann als Filter gesetzt werden. Andere Widgets, die mit dem manipulierten durch die Daten verknüpft sind, werden dann automatisch im augenblicklich upgedatet. Diese Funktionalität konnte in den Demonstrationen der anderen Produkte nicht beobachtet werden. Man bezeichnet sie als *Brushing*.
Bei allen Lösungen stört der Kontextverlust, wenn man Details zu einem Widget angezeigt bekommen möchte. Häufig landet man an einer ganz anderen Stelle, wie bei *QRadar* z.B. oder ein neues Fenster öffnet sich, das die aktuelle Ansicht vollständig verdeckt, wie etwa bei *NitroView*. Wünschenswert wäre hier ein kleiner Bereich, der das Dashboard in verkleinerter Form zeigt. oder zumindest eine einfache Rückkehr mit einer Interaktion ermöglicht.

Literaturverzeichnis

Few, Stephen (2006): *Information Dashboard Design*. Sebastopol: O'Reilly Media Inc.

Francis, Dean (2012): *IT Pro Ranking: SIEM*. URL: http://reports.informationweek.com/abstract/21/8901/security/it-pro-ranking-siem.html.
Stand: 28.03.2013

Marty, Raffael (2008): *Applied Security Visualization*. Amsterdam: Addison-Wesley Longman.

Nicolett, Mark; Kavanagh, Kelly M. (2012): *Magic Quadrant for Security Information and Event Management: SIEM*. URL: http://www.gartner.com/technology/reprints.do?id=1-1ANUJF3&ct=120525&st=sb.
Stand: 28.03.2013

Nielsen, Jakob (1994): *Usability Engineering*. San Francisco: Morgan Kaufmann.

Norman, D. A. (2002): *Emotion and design: Attractive things work better*. In: Interactions Magazine, ix (4), 36-42.

Rock, Irvin; Palmer, Stephen (1990): *The Legacy of Gestalt Psychology*. Scientific American 263, 6 (December), 84–90

Rothmann, Mike (2010): *Network Security Fundamentals: Monitor Everything*. URL: https://securosis.com/blog/network-security-fundamentals-monitor-everything. Stand: 28.03.2013

Tufte, Edward (2001): *The Visual Display of Quantitative Information*. Cheshire: Graphics Press

Tufte, Edward (1990): *Envisioning Information*. Cheshire: Graphics Press.