Visualisierung von Lagebildinformationen innerhalb eines Security Operation Centers
Ausarbeitung zum Masterseminar GSM, WS 14 /15

Robert Johns

Hochschule für Angewandte Wissenschaften
Berliner Tor 7
20099 Hamburg, Germany
Email: robert.johns@haw-hamburg.de

I. Einführung

Ein großes Thema bei informationsverarbeitenden Systemen (IS), ist immer auch die Informationssicherheit [1]. Unternehmen, Behörden, Forschungseinrichtungen und auch Privatpersonen haben das Bedürfnis, sich und ihre Daten vor Angriffen und Spionage zu schützen. Berichte, wie etwa der Hacker-Angriff auf Sony in der jüngsten Vergangenheit, sind ein gutes Beispiel dafür, welchen Schaden ein unerkannter Angriff verursachen kann. Während es sich bei Privatpersonen in der Regel auf das Heimnetzwerk beschränkt, sind moderne IS in Unternehmen, Behörden und Forschungseinrichtungen häufig verteilte Systeme. Nicht selten sind deren Komponenten auf mehrere Standorte verteilt und über das Internet miteinander verbunden. Um diese vor Angriffen zu schützen und um dies zu erkennen, setzen Security Teams verschiedene Tools ein. Firewall's(FW), Intrusion Detections Systeme(IDS), Intrusion Prevention Systeme(IPS) und andere Datenquellen generieren Logs und Events, mit denen der Systemzustand der Komponenten rund um die Uhr überwacht wird und woraus ein Rückschluss auf den Gesamtzustand geschlossen werden kann. Speicherung, Überwachung und Kontrolle dieser Daten laufen in sogenannten *Security Operation Center (SOC)* zusammen. Dort werden die Daten normalisiert, korreliert, aggregiert und gespeichert (Abbildung 1) [2] [3]. Security Analysten werten diese Daten live aus, um bei einem Angriff entsprechende Gegenmaßnahmen zu ergreifen oder nutzen die gespeicherten Einträge für forensische Untersuchungen, um unentdeckte oder in Vorbereitung stehende Angriffe zu analysieren.

SOC's als solches sind keine standardisierte Einrichtung mit fest vorgegebenen Werkzeugen. Vielmehr sind die dort eingesetzten Produkte ein Ergebnis der vorliegenden Infrastruktur und des Bedarfs des jeweiligen Betreibers. Ein Anbieter von Cloud-Lösungen beispielsweise unterscheidet sich mit seinem Gesamtsystem von dem eines Industrieunternehmens. So unterschiedlich wie das Gesamtsystem, sind auch die SOC's, da jeder die Werkzeuge einsetzt, die zum jeweiligen Einsatzzweck passen. Lediglich der Kern eines SOC bildet heute ein *Security Information and Event Management System (SIEM)*, hierauf wird im Kapitel II noch einmal näher eingegangen.

A. Problemstellung

Es existiert keine wissenschaftliche Arbeit darüber, wie Lagedaten in einem SOC visualisiert werden können. Zwar gibt es Arbeiten über die Security Visualisierung im Allgemeinen [5] und es existieren Arbeiten über die Visualisierungen

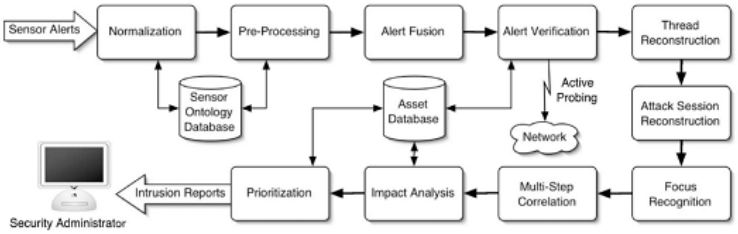

Abbildung 1. *Korrelationsprozess nach [4].*

in SIEM's [6] [7]. Wie dies aber in einem SOC derzeit umgesetzt wird, ist abhängig vom jeweiligen Betreiber. Durch die Auswahl bestimmter Werkzeuge, resultieren entsprechende Angebote an visuellen Darstellungsmöglichkeiten.

B. Motivation

Ich möchte in meiner Masterarbeit die visuelle Darstellung von Lagebildinformationen in einem Security Operation Center aufarbeiten und eine Grundlagenarbeit dafür schaffen. Dazu muss die aktuelle Situation erforscht werden, um Anforderungen herauszuarbeiten und Lösungsansätze zu entwickeln.

C. Ideenskizze

Um dieses Thema zu bearbeiten, muss zuerst untersucht werden was ein SIEM ist, wie es arbeitet und welche Daten es zur Verfügung stellen kann. Danach muss herausgestellt werden, welche Rollen von Benutzern in einem SOC tätig sind. Dazu ist wichtig festzustellen, welche Informationen für welche Rolle von Interesse sind. Zum Schluss kann mit den Erkenntnissen, welche Daten es überhaupt gibt und für wen sie eine Rolle spielen, die Arbeit beginnen zu untersuchen wie diese dargestellt werden können.

D. Inhalt dieser Arbeit

Die Anwendung von Visualisierung in der Computersicherheit erfordert die Kenntnis von zwei unterschiedlichen Disziplinen, *Sicherheit* und *Visualisierung* [5]. Zu dem Thema Sicherheit, wird in Kapitel II das SOC mit seiner Kernkomponente dem SIEM vorgestellt und es werden die unterschiedlichen Benutzerrollen angesprochen, für die unterschiedlichen Sichten erarbeitet werden müssen. In Kapitel III wird zu dem Thema Visualisierung über die Grundlagen gesprochen, die für

dieses Thema erarbeitet werden müssen. In beiden Kapiteln werden jeweils die Arbeitspakete gezeigt. Am Ende wird eine aktuelle Arbeit aus dem Bereich *Security Visualisierung* vorgestellt.

II. Security Operation Center

Ein SOC dient der Gefahrenabwehr von Cyberangriffen auf den ihm unterstellten Bereich. Dazu muss es Informationen sammeln, diese analysieren und visualisieren. Mitarbeiter sind dort rund um die Uhr damit beschäftigt, die Informationen die ihnen dargestellt werden auszuwerten. Das können zum Einem konkrete Alarme sein, auf die entsprechend reagiert werden muss, zum Anderen können das auch einfache Meldungen sein.

A. Der Kern im SOC das SIEM

Die Herausforderung an das bereits angesprochene SIEM-System ist es, Analyseergebnisse zusammenzufassen und darzustellen, damit deren Bediener effektivere und effizientere Entscheidungen treffen können. Dazu müssen Visualisierungstechniken eingesetzt werden, die es dem Menschen erleichtern relevante Informationen aus großen Datenmengen zu sammeln [3]. Um Informationen zu sammeln und um diese zu verarbeiten, besteht ein SIEM aus zwei relevanten Kernkomponenten, dem *Security Information Management*(SIM) für die Informationsgewinnung und dem *Security Event Management*(SEM) für die Informationsverarbeitung. Diese beiden Komponenten lassen sich wie folgt charakterisieren:

SIM sind Systeme, die Events und Logs von verschiedensten Sensoren im Netzwerk sammeln und diese in Echtzeit verknüpfen, verarbeiten, analysieren und speichern. Daraus lassen sich dann, auf die jeweilige Rolle angepasst, Berichte erstellen. Die Herausforderung an ein SIM ist dabei, die unterschiedlichen Formate der unterschiedlichen Datenquellen zu interpretieren [8].

SEM sind Systeme die, anhand von vorgegebenen Richtlinien, Logs korrelieren und mit definierten Regeln eine Echtzeitüberwachung vornehmen. Das SEM wird zum Beispiel dazu verwendet, die mit einem SIM gesammelten Daten zu verwerten [8].

Diese beiden Komponenten zusammen als ein System zu betreiben, hat mehrere Vorteile. Die folgende Aufzählung aus dem Paper *Security information and event management in the cloud computing infrastructure* [8] fasst die grundlegenden zusammen:

1) *Log Management:* Alle von den Geräten im Netzwerk erzeugten Logs, können mit dem Log Management für spätere Analysen in eine Datenbank abgespeichert werden, beziehungsweise können direkt zur Echtzeitüberwachung verwendet werden.
2) *IT Standards:* Im SIEM können Standards und Vorschriften für das Unternehmen festgelegt werden. Durch die Verwendung von Zertifikaten kann der Schutz zusätzlich erhöht werden.
3) *Event Korrelation:* Ist eine der Kernfunktionen eines SIEM. Mittels einprogrammierter künstlicher Intelligenz werden Events, die von den unterschiedlichen Geräte im Netzwerk stammen, auf Beziehungen zueinander untersucht. Viele Hersteller statten ihre Produkte mit einer Vielzahl an vordefinierten Korrelationsregeln aus.
4) *Automatische Reaktion:* Die automatische Reaktion ist eine mögliche Folge der Event Korrelation. Werden Events erkannt, deren Verhalten dem eines Sicherheitsrisikos gleicht, wird eine darauf abgestimmte Reaktion ausgelöst, um eventuelle Gefahren für das Netzwerk abzuwehren. Diese Abläufe müssen allerdings getestet und überprüft werden, da es im Falle von *false positives* zu unnötigen Eingriffen im System kommt. Aus diesem Grund sollten *false positives*, so selten wie möglich auftreten.
5) *Überwachung von Endgeräten:* Ein wichtiger Faktor, ist die Überwachung von Anwender und Endgeräten. Thor [9] beschreibt in seinem Artikel, dass viele Bedrohungen auf menschliches Fehlverhalten zurückzuführen sind. Es ist also ebenso wichtig, das Verhalten eines Anwenders und den Systemzustand des Endgerätes mit zu überwachen.
6) *Zentrales Security Management:* Eine enorme Auswahl an Security Lösungen und Produkten, die eine eigene Logik und Bedienung beinhalten, erschweren die Interoperabilität. Das ist unvorteilhaft, wodurch eine zentrale Lösung hier von Vorteil ist.
7) *Reporting:* Mit Hilfe einer zentralen Infrastruktur, liefert das Reporting präzise und wertvolle Informationen. Mit diesen sind die Security Teams in der Lage auf kritische, sowie normale Situationen zu reagieren und Entscheidungen zu treffen.

Die Architektur eines SIEM, unabhängig von einer herstellerspezifischen Umsetzung, ist im folgenden zusammengefasst.

Datenquellen sind einer der wichtigsten Komponenten für ein SIEM. Ohne Daten kann ein SIEM nicht arbeiten und es kann nur so gut sein, wie die Daten die es bekommt [2]. Die Datenquellen gehören nicht direkt zum jeweiligen SIEM-Produkt, sondern sind ein Ergebnis der vorliegenden Infrastruktur und Auswahl an Sicherheitskomponenten für das Gesamtsystem. Als Quellen kann alles genutzt werden, was Logs generiert und nützliche Informationen liefert, um im SIEM verarbeitet zu werden [8]. Dies können zum Beispiel Server, Netzwerkkomponenten, Firewalls, IDS, IPS, Host Intrusion Prevention Systeme(HIPS) und Betriebssysteme sein [10]. Diese Aufzählung ist bei weitem nicht vollständig und kann durch beliebige Quellen erweitert werden. Hierbei ist das Angebot an Datenquellen auf dem Markt enorm. Nimmt man HIPS als Beispiel heran, gibt es allein in diesem Segment eine Vielzahl an Herstellern.

Logsammlung ist die Eigenschaft die Logs, die von den im vorigen Abschnitt genannten Quellen, auch tatsächlich zu sammeln. Dabei gibt es zwei unterschiedliche Arten, Daten zwischen SIEM und Datenquelle zu übertragen. Die eine ist, dass die Geräte die Daten mittels *Push* selbst an das SIEM senden. Der Vorteil ist hier, dass dieser Ansatz aus Sicht des SIEM einfach zu konfigurieren ist und die Daten in Echtzeit übertragen werden. Der Nachteil allerdings ist seine Verwundbarkeit auf dem Übertragungsweg. Durch die Verwendung von UDP, gibt es keine Garantie für Datenübertragung und Integrität. Die andere Möglichkeit ist es mittels *Pull*, die Daten selbst von den Geräten abzurufen. Hierfür muss allerdings eine Verbindung aufgebaut werden. Mittels Benutzerauthentifizierung kann das SIEM sich bei einem Gerät anmelden und Daten abrufen. Diese Variante ist sicherer, weil das SIEM Kenntnis über die Verfügbarkeit der Daten hat und genau weiß welche

Daten gesammelt wurden. Allerdings ist nicht garantiert, dass die Daten in Echtzeit übermittelt werden, da es vom Intervall abhängt, wie oft das SIEM die Daten abfragt. Zudem entsteht ein höherer *Overhead* in der Kommunikation [8].

Normalisierung bringt die gesammelten Daten in ein standardisiertes Uniform Format, dargestellt in Abbildung 2, da die Datenquellen Logs nach herstellerspezifischer Syntax generieren. Damit diese durch das SIEM weiterverwendet werden können, werden sie normalisiert. Dabei ist es auch hier so, dass jeder SIEM- Hersteller seine Normalisierung nach eigener Implementierung vornimmt [11].

Regeln und Datenkorrelation sind ein wichtiges Werkzeug eines SIEM [3]. Hiermit lassen sich Logs bewerten und miteinander korrelieren, woraus dann wiederum Events resultieren. Eine Regel kann es zum Beispiel sein, fehlgeschlagene Loginversuche in der Active Directory Gruppe der Administratoren zu einem Event zu machen, außerdem könnte eine weitere Regel lauten, dort stattfindende Passwortänderung zu überwachen. Jedes für sich genommen ist ein eigener Log, 'Loginversuch fehlgeschlagen' und 'Passwort geändert'. Die künstliche Intelligenz der Datenkorrelation allerdings, kann daraus einen Zusammenhang erkennen und einen Alarm geben, wenn diese Events in einem definierten Zeitabstand zueinander stattfinden und daraus eine Gefahr identifiziert wird. Informationen können so in einem breiteren Kontext betrachtet werden, um potentielle Gefahren für das Gesamtsystem zu identifizieren.

Datenspeicherung dient der Langzeitanalyse aller Logs und Daten. Mit diesen Daten können erfolgte, fehlgeschlagene oder auch unentdeckte Angriffe analysiert werden, um das System stetig zu verbessern und zu aktualisieren. Es sollte allerdings auch darauf geachtet werden, diesen Speicher vor unautorisierten Zugriff zu schützen, da er auch private und sensible Daten von Mitarbeitern enthalten könnte [3].

Monitoring ist die Schnittstelle zwischen dem SIEM und seinem Bediener. Hier werden die Informationen wie Events und Alarme grafisch dargestellt, um den aktuellen Zustand des Gesamtsystems abzubilden. Außerdem können Dashboards angezeigt und als Berichte in die oberen Unternehmensebenen gereicht werden.

B. Externe Informationsquellen

Neben den Informationen die im SOC aus dem eigenen Netzwerk gesammelt werden, gibt es noch weitere Quellen. Durch die Auswertung von Cybernews, dem Informationsaustausch zwischen SOC's und anderen Quellen können Erfahrungen ausgetauscht weden, um Gefahren zu identifizieren und entsprechende Vorbereitungen und Anpassungen am System vorzunehmen. Allgemein wird das unter dem Begriff *Cyber Intelligence* zusammengefasst [2]. In Deutschland gibt es beispielsweise das *DFN-CERT* [12] oder das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* [13], die in aktuellen Meldungen Informationen über Gefahren und Schwachstellen verteilen. Diese Quellen sind ein wichtiger Bestandteil und müssen bei der Darstellung genauso berücksichtigt werden, wie interne Daten.

C. Benutzerrollen

In einem SOC arbeiten, je nach Ausprägung und Größe der Einrichtung, unterschiedlichen Mitarbeiter in unterschiedlichen Aufgabenbereichen. Während in kleineren SOC's

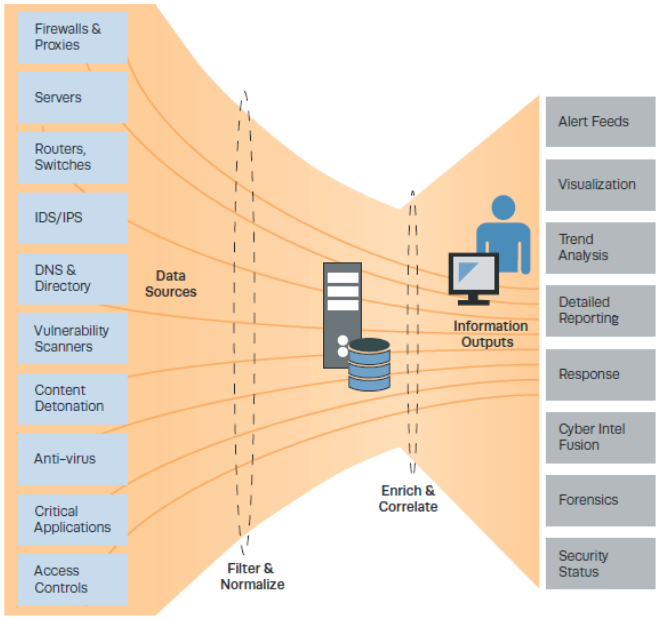

Abbildung 2. *Datenverarbeitung in einem SIEM [2].*

einzelne Mitarbeiter mehrere Aufgabenbereiche gleichzeitig übernehmen , bilden größere Einrichtungen Teams und der Mitarbeiter arbeitet dort in einem einzelnen Bereich. [2]. Die Mitarbeiter- Profile die es gibt sind:

- SOC Chief - ist der Leiter des SOC. Bei großen SOC's hat dieser noch einen Stellvertreter.
- Security Manager - sind in SOC's für die Führung von Teilbereichen bzw. Verantwortungsbereichen verantwortlich.
- Security Analyst - überwachen Logs, Events, Meldungen und Alarme aus den Echtzeit-Daten und führen Untersuchungen an den forensischen Daten durch.
- Security Engineer - sind mit der technischen und administrativen Weiterentwicklung des SOC beauftragt.

Die Teilbereiche mit ihren Unterfunktionen, die gegebenenfalls noch weiter untergliedert werden können, sind dabei [2]:

- *Analysis and Response* - Call-Center, Analyse von Echtzeit-Daten, Sammeln und analysieren von Cybernews, Auswertung und Analyse von Zwischenfällen, Koordinierung und Gegenmaßnahmen bei Zwischenfällen, Untersuchung von Malware, Bedrohungsanalyse, Trendauswertung, Bearbeitung von Alarmierungen und Warnungen.
- *Scanning and Assesstment* - scannen des Netzwerkverkehrs, scannen von Schwachstellen, Schwachstellenanalyse, Umgebungsanalyse (situational awareness), Pentrationstests, Produktanalyse, Security-Beratung.
- *System Life Cycle* - Q&A der SOC-Infrastruktur, Verbesserung und Wartung der Sensoren, Erstellung von Skripts und Automatisierung, Tool-Entwicklung und Einführung.

Außerhalb vom SOC angeordnet, ist der Chief Information Security Officer (CISO). Dieser ist der Leiter für Informa-

tionssicherheit und als Vorgesetzter des SOC Chief, mitverantwortlich für das SOC. Aktuell können durch die SIEM-Funktionalität des Reportings Dashboards erzeugt werden, um außerhalb als Bericht vorgelegt zu werden. In dieser Arbeit soll auch untersucht werden, wie eine entsprechen Sicht für einen CISO aussehen könnte, wenn dieser sich ein Lagebild vom SOC ansehen möchte, welches nicht ausschließlich aus historischen Daten besteht.

D. Analysearbeit

Aus den aufgearbeiteten Bereichen in diesem Kapitel, können folgende Punkte festgehalten werden, die für diese Arbeit näher untersucht werden müssen:

1) Welche Daten, die das SIEM bereit hält, sind für einen Analysten von Interesse? Zu unterscheiden sind hier Rohdaten, korrelierte Daten, Events und Alarme.
2) Wie viel der Ansicht, soll dabei durch welche Daten eingenommen werden? Der mengenmäßige Anteil an hochbrisanten Informationen ist eher gering und der Anteil an normalen Informationen ist umso höher [2]. Daher stellt sich die Frage, wie dies in einem adäquaten Verhältnis angezeigt werden kann.
3) Wie müssen die historischen Daten dargestellt werden?
4) Was muss neben den reinen Informationen in die Darstellung mit einfließen um ein verständliches Lagebild zu erhalten?
5) Welche Daten kommen von Extern hinzu, wie lassen sich diese mit den anderen Daten aggregieren und wie sollen diese dargestellt werden?
6) Welche Daten sind für welche Benutzerrolle relevant?
7) Wie können diese Ansichten vermengt werden, wenn ein Benutzer mehrere Benutzerrollen hat?

III. Visualisierung

Eine gute Visualisierung von Inhalten ist wichtig. Es trägt dazu bei die Übersicht zu behalten und aus dem Kontext der Darstellung das zu erkennen, was viele tausend Zeilen Protokolldaten niemals schaffen können. Der Autor des Buches *Applied Security Visualization* [5], dass derzeit als eines der umfassendsten Werke über Securtiy Visualisierung [7] gilt, sagt dazu: *„A picture is worth a thousand log records“*.

A. Grundlagen

Die visuelle Wahrnehmung des Menschen hat eigene Regeln. Diese gilt es aufzuarbeiten, wenn man gute, verständliche Visualisierungen darstellen möchte. Es gibt Muster, die der Mensch schnell und leicht erkennt, andere wiederum können so in der Darstellung untergehen, dass sie nicht wahrgenommen werden. Das Wissen über diese Regeln, kann also dazu genutzt werden, Informationen verständlich zu visualisieren. Andernfalls können diese irreführend und missverständlich sein [5].

Farben: - Eine Verwendung von Farbe in grafischen Oberflächen ist der ästhetische Aspekt. Bei der Verwendung in diesem Kontext, wird allerdings davon abgeraten, Farben zu ästhetischen Zwecken einzusetzen. Eine weitere Verwendung, die in diesen Kontext von großer Bedeutung ist, ist es Inhalten Bedeutungen und Informationen hinzuzufügen. Zum Beispiel lassen sich damit Dimensionen in Graphen darstellen oder Werte können mittels Farbe kodiert werden, die dann von einer Legende wieder dekodiert werden. Hierbei ist allerdings darauf zu achten, dass die Anzahl an Werten, die von Farben repräsentiert werden, nicht zu hoch ist. Der Betrachter verbringt sonst die meiste Zeit damit, die unterschiedlichen Farben wieder zu dekodieren, was den Einsatz der Farben hinfällig macht. Verwendet man Farben zur Kodierung ohne eine Legende, dann ist unbedingt darauf zu achten, dass der Kontext der Farbe offensichtlich ist. Das einfachste Beispiel dafür, ist die Farbe Rot für etwas negatives und die Farbe Grün für etwas positives. Ein weiterer guter Anwendungsfall für den Einsatz von Farbe,sind stetigen Wertebereiche. Dieser kann durch einen Farbverlauf (zum Beispiel Graustufen) dargestellt und verdeutlicht werden. Helle Farben eigenen sich außerdem, Inhalte in einer Oberfläche hervorzuheben, um die Aufmerksamkeit des Betrachters darauf zu lenken. Das Web-Tool *ColorBrewer*[1] kann bei der Farbwahl für Graphen helfen. Es bietet zudem die Möglichkeit, eine Auswahl daraufhin abzusichern, dass auch farbenblinde Bediener Farbunterschiede sicher erkennen können [5].

Form und Größe - Die Darstellung von Daten in unterschiedlichen Dimensionen mittels Formen und Größen, ist eine weitere Möglichkeit der Darstellung. Formen können genauso wie Farben dazu verwendet werden, Werte zu kodieren. Anstelle unterschiedlicher Farben, können beispielsweise Kreuze, Kreise, Ovale, Rechtecke und andere Formen verwendet werden. Mit der Größe von Objekten, können Werte ebenso widergespiegelt werden. Es sollte aber nicht zur Darstellung absoluter Werte verwendet werden, sondern um die Relationen zwischen Werten abzubilden. Ersteres kann nur schwer anhand der Größe abgeleitet werden [5].

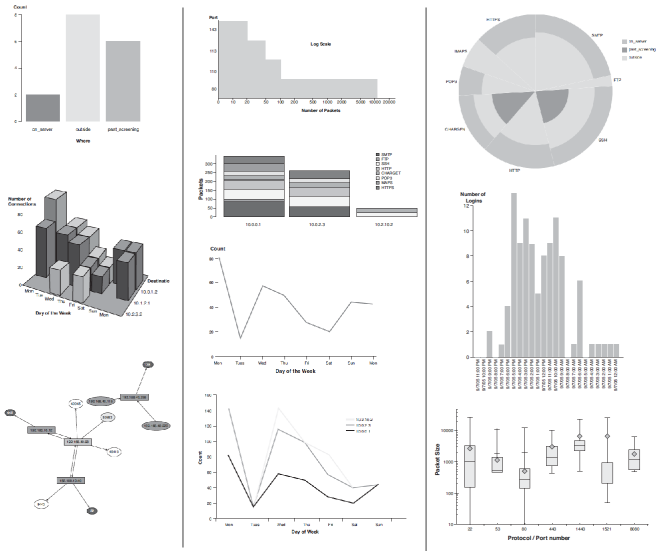

Abbildung 3. *Beispiele für grafische Darstellungen von Werten [5].*

Graphen: - Bei der Darstellung von Daten und Werten gibt es verschiedene Graphen die verwendet werden können, Abbildung 3 zeigt einige Beispiele:

1) Einfache und mehrschichtige Diagramme
   - Kreisdiagramm
   - Balkendiagramm
   - Liniendiagramm

[1]ColorBrewer 2.0 online: http://colorbrewer2.org/ - Abruf: 19.02.15

- Säulendiagramm

2) Histogramme
3) Box Plots und Scatter Plots
4) Parallele Koordinaten
5) Verlinkte Graphen
6) Maps und Treemaps

Einigen können nicht nur zweidimensional sondern auch dreidimensional verwendet werden und manche Darstellungen lassen sich auch animieren. In dem Buch gibt es auch Vorschläge, welche Graphen zu welchen Datentypen und Use-Cases geeignet sind und bis zu welcher maximalen Anzahl an Werten diese überschaubar bleiben [5].

Hat man den richtigen Graph für einen Anwendungsfall ausgewählt, bleiben bestimmte Herausforderung. Erstens, diesen mit sinnvollen Informationen zu füllen. Bläht man ihn mit zu viel unnötigen Daten auf, wird die Darstellung schnell unübersichtlich und verliert ihren Zweck. Alle irrelevanten Daten müssen also vorher ausgefiltert werden. Zweitens kann die Menge an Daten pro Graph ein Problem darstellen, gegebenenfalls muss geprüft werden, diese Daten zu aggregieren. Es muss also ein methodischen Vorgehen entwickelt werden, wie man von der Auswahl der Daten, über Filterung und Normalisierung hin zur Ausgabe gelangt. In dem Buch [5] wird dazu ebenfalls ein Vorschlag gemacht, der *Information visualization process*, der hier nur als ein Beispiel genannt werden soll. Ob dieses Vorgehen in dieser Arbeit angewendet wird, muss im weiteren Verlauf analysiert werden, er verdeutlicht jedoch wie vorgegangen werden kann. Der Prozess, dargestellt in Abbildung 4, enthält sechs Schritte:

1) Problem definieren - Welche Fragestellung soll durch den Graphen gelöst werden?
2) Daten bewerten - Welche Daten stehen dafür generell zur Verfügung? Welche Daten können nützlich sein?
3) Informationen verarbeiten - Die Logs müssen geparsed und eventuell gefiltert werden um die nötigen Informationen zu erhalten.
4) Visuelle Umsetzung - Welcher Graph, Farbe, Größe, Form? Wie können die Eigenschaften der Informationen gut dargestellt werden?
5) Ansichten verändern - Wechsel der Ansichten ermöglichen (Zoom, skalieren,etc.) um wichtige Bereiche der Informationen zu fokussieren.
6) Interpretieren und Entscheiden - Sichten und Beurteilen des Ergebnisses. Wurde das erreicht was anfangs definiert wurde?

B. Analysearbeit

Aus diesen Abschnitt ergeben sich die folgenden Arbeitspakete, die beim weiteren Vorgehen zu dieser Arbeit näher untersucht werden müssen:

- Welche Graphen sind für die Daten, die das Ergebnis der Untersuchungen in Abschnitt II-D sind, die richtigen?
- Wie kann die Visualisierung der Graphen mittels Farbe, Form und Größe verdeutlicht werden? Welche Daten können zusätzlich durch den Einsatz von Farbe hervorgehoben werden?
- Wie sind diese Daten zu filtern, zu normalisieren und zu aggregieren? Gibt es bei diesem Vorgehen Unterschiede zwischen den Benutzerrollen aus Abschnitt II-D, die zu beachten sind?
- Wie viel Information kann auf einem Bildschirm dargestellt werden, bevor es unübersichtlich wird? Können Ansichten gruppiert werden?

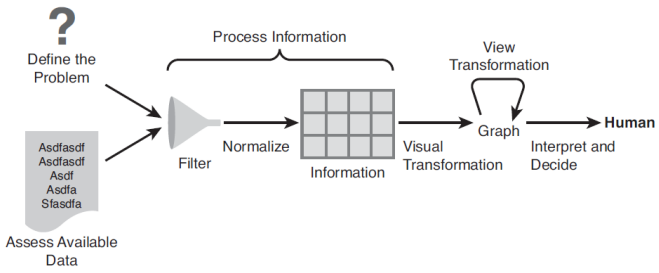

Abbildung 4. *Information visualization process [5].*

IV. Aktuelles

Eine interessante Arbeit aus dem Themenbereich der *Security Visualisierung* ist das Paper *Visualization of Security Metric for Cyber Situation Awareness* [6]. Die Autoren stellen dort ein Verfahren vor, Netzwerkkomponenten anhand einer definierten Metrik zu bewerten und dieses grafisch abzubilden. Dadurch soll ein mögliches Gefährdungspotential für das Gesamtsystem optisch erkennbar sein. Die Komponenten bekommen die Eigenschaften:

- *Host Criticality Level*
- *Host Vulnerability Level*
- *Attack Probability*
- *Attack Impact Level*

Mit der in dem Paper beschriebenen Metrik, erfolgt eine Einstufung nach dem standardisierten Scoring System *Common Vulnerability Scoring System (CVSS)* [14]. Für die Darstellung, gezeigt in Abbildung 5, wird jeder Host als Kreissymbol repräsentiert und jeweils ein Viertel der Innenfläche codiert farblich die vier genannten Eigenschaften. Auf dem Außenkreis ist der vorherige Zustand dargestellt , zum Beispiel bevor ein Update auf einem der Komponenten eingespielt wurde. Dadurch kann nachvollzogen werden, wie sich der Zustand durch eine Aktion verändert hat und ob es dadurch Wechselwirkungen zu anderen Geräten im Netzwerk gegeben hat. Diese Form der Darstellung erleichtert es den Security Administratoren, verwundbare Geräte im Netzwerk zu identifizieren und zu reagieren bevor kritische Situationen eintreten. Anhand der erkennbaren schwere der Gefährdung kann zudem priorisiert vorgegangen werden.

A. Abgrenzung

Diese Vorgestellte Arbeit beleuchtet nur einen Teilaspekt innerhalb eines SOC, gibt aber interessante Anreize und Beispiele. Es zeigt, wie durch gute visuelle Darstellung die *Situational Awareness* im *Scanning und Assessment- Team* gesteigert werden kann und dadurch ein Mehrwert für das Gesamtsystem entsteht.

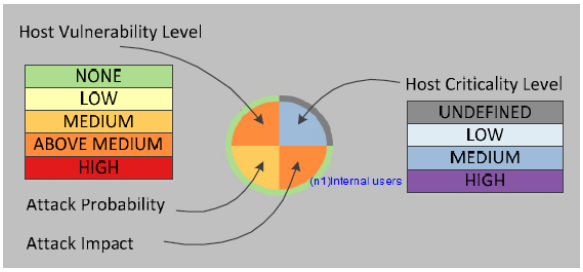

Abbildung 5. *Darstellung eines Hosts als Symbol [6].*

V. Schluss

Dieser Abschnitt fasst den Inhalt dieser Arbeit zusammen, zeigt die Arbeitsgruppen und andere Quellen und gibt einen Ausblick auf das Grundpraktikum.

A. Zusammenfassung

In dieser Ausarbeitung wurden die grundlegenden Bereiche aufgearbeitet, die für die Umsetzung meiner Arbeit notwendig sind. Zuerst wurde das Thema *SOC* behandelt und erarbeitet. Welche Komponenten arbeiten in einem SOC, welche Daten generieren sie und welche Unterschiede machen ein SOC aus. Des Weiteren wurde auch behandelt, welche Rollen in einem SOC tätig sind und welche Aufgabebereiche diese haben. Im Anschluss wurde das Thema *Visualisierung* untersucht. Hier wurde angesprochen, welche grafischen Elemente Verwendung finden können und wie mit Hilfe des Einsatz von Farbe, Form und Größe diesen Elementen ein Mehrwert hinzugefügt werden kann. In beiden Kapiteln wurden Arbeitspakete identifiziert. Am Ende dieser Arbeit wurde ein Beispiel aus der aktuellen Forschung im Bereich *Security Visualization* gezeigt.

B. Arbeitsgruppen

Die folgenden Arbeitsgruppen, Konferenzen und Bereiche dienen bei der weiteren Suche als dienliche Quellen und geben interessante Informationen:

- International Symposium on Research in Attacks, Intrusions and Defenses (RAID)[2]
- Deutsches Forschungsnetz CERT [3]
- International Conference on Availability, Reliability and Security [4]
- Bundesamt für Sicherheit in der Informationstechnik [5]

C. Ausblick

Die Erkenntnisse aus dieser Arbeit sollen im Grundpraktikum dazu genutzt werden, die identifizierten Arbeitspakete in II-D und III-B auszuarbeiten. Dazu muss vor allem der Bereich *Visualisierung* noch intensiv untersucht und Grundlagen erarbeitet werden, da dieser Bereich für mich neu ist.

[2]International Symposium on Research in Attacks, Intrusions and Defenses http://www.raid-symposium.org/ - Abruf: 20.02.15

[3]DFN CERT https://www.dfn-cert.de/ - Abruf: 19.02.15

[4]ARES Conference http://www.ares-conference.eu/conference/ - Abruf: 19.02.15

[5]BSI https://www.bsi.bund.de - Abruf: 20.02.15

Literatur

[1] I. Aguirre and S. Alonso, "Improving the automation of security information management: A collaborative approach," Security Privacy, IEEE, vol. 10, no. 1, Jan 2012, pp. 55–59.

[2] C. Zimmermann, Ten Strategies of a World-Class Cybersecurity Operations Center. Mitre, 2014, online verfügbar unter http://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center - Abruf: 15.02.2015.

[3] S. Bhatt, P. Manadhata, and L. Zomlot, "The operational role of security information and event management systems," Security Privacy, IEEE, vol. 12, no. 5, Sept 2014, pp. 35–41.

[4] F. Valeur, G. Vigna, C. Kruegel, and R. Kemmerer, "Comprehensive approach to intrusion detection alert correlation," Dependable and Secure Computing, IEEE Transactions on, vol. 1, no. 3, July 2004, pp. 146–169.

[5] R. Marty, Applied Security Visualization. Addison-Wesley, 2009. [Online]. Available: http://books.google.de/books?id=m2eZNAAACAAJ

[6] I. Kotenko and E. Novikova, "Visualization of security metrics for cyber situation awareness," in Availability, Reliability and Security (ARES), 2014 Ninth International Conference on, Sept 2014, pp. 506–513.

[7] E. Novikova and I. Kotenko, "Analytical visualization techniques for security information and event management," in Parallel, Distributed and Network-Based Processing (PDP), 2013 21st Euromicro International Conference on, Feb 2013, pp. 519–525.

[8] J. Pavlik, A. Komarek, and V. Sobeslav, "Security information and event management in the cloud computing infrastructure," in Computational Intelligence and Informatics (CINTI), 2014 IEEE 15th International Symposium on, Nov 2014, pp. 209–214.

[9] T. Olavsrud, "Most data breaches caused by human error, system glitches," CSO Security and Risk, June 2013, online verfügbar unter http://www.csoonline.com/article/2133631/data-protection/most-data-breaches-caused-by-human-error--system-glitches.html - Abruf: 13.02.2015.

[10] C. Constantin, "A beginner's guide to siem," 2013, online verfügbar unter http://de.slideshare.net/alienvault/siem-for-beginners - Abruf: 14.02.15.

[11] D. Miller, S. Harris, A. Harper, S. VanDyke, and C. Blask, Security Information and Event Management (SIEM) Implementation. McGraw-Hill Education, 2010. [Online]. Available: http://books.google.de/books?id=gaEBvcfeu3IC

[12] "Deutsches forschungsnetz - computer emergency response team (dfn-cert)," online erreichbar unter https://www.dfn-cert.de/informationen/meldungen-vom-dfn-cert.html - Abruf: 19.02.15.

[13] "Bundesamt für sicherheit in der informationstechnik," online erreichbar unter https://www.bsi.bund.de - Abruf: 19.02.15.

[14] P. Mell, K. Scarfone, and S. Romanosky, "A complete guide to the common vulnerability scoring system version 2.0," June 2007, online verfügbar unter https://www.first.org/cvss/cvss-guide.pdf - Abruf: 14.02.15.