

Der NSK Security Logger

SIEM-Projekte auch für NSK

Compliance ist eine Synthese aus technischem Fortschritt und daran angepassten gesetzlichen Anforderungen. Dieses top-aktuelle Thema bringt strukturelle Anforderungen und komplexe Rahmenbedingungen mit sich. Prozesse werden transparenter gestaltet und Kosten und Effizienz optimiert. Dabei spielt die IT eine entscheidende Rolle. Laut führender Publikationen und Analysen ist es den meisten Unternehmen bewusst, dass sie sich früher oder später mit dem Thema Compliance befassen werden müssen. Davon kann das Überleben der Firma abhängen.

Im Zuge sicherheitsrelevanter SIEM-Projekte (Security Information and Event Management) werden IT-Mitarbeiter zunehmend häufiger gebeten, ihre Zugangsdaten zu schützen und per Unterschrift deren Geheimhaltung zu garantieren, um bei Missbrauch durch einen Dritten in die Pflicht genommen werden zu können.

Es mag sein, dass Ihr NSK-Server sein Dasein unauffällig, effizient und problemlos in der mission-critical Ecke verbringt; er ist jedoch gleichermaßen, wie andere Plattformen, von

Compliance und damit verbunden Fragen betroffen: „Wer macht was auf dem System?“ „Wer hat dieses TACL-Makro gestartet?“ „Wer hat gerade Zugriff auf sensible Daten erhalten?“

Hier setzen der NSK Security Logger von TWINSOFT und ihr Partner ArcSight ein:

Der TWINSOFT NSK Security Logger kann Ihnen helfen, die notwendige Sicherheit zu erreichen und Compliance-Anforderungen einzuhalten.

Der Vorläufer des NSK Security Loggers wird bereits seit Jahren von einem führenden Geldinstitut eingesetzt. Seitdem wurde das Thema vertieft und die Erstentwicklung zu einem eigenständigen Produkt entwickelt.

Jede NSK Security Komponente hat eine eigene Struktur und Vorgehensweise, um sicherheitsrelevante Zugriffe zu protokollieren. Hier setzt der NSK Security Logger an. So genannte, von der TWINSOFT entwickelte, Extraktoren greifen die Log-Dateien der verschiedenen Security-Komponenten des NSK-Systems ab.



TWINSOFT GmbH & Co. KG

Europaplatz 2
64293 Darmstadt
Tel.: 06151 39756-0
Fax: 06151 39756-50

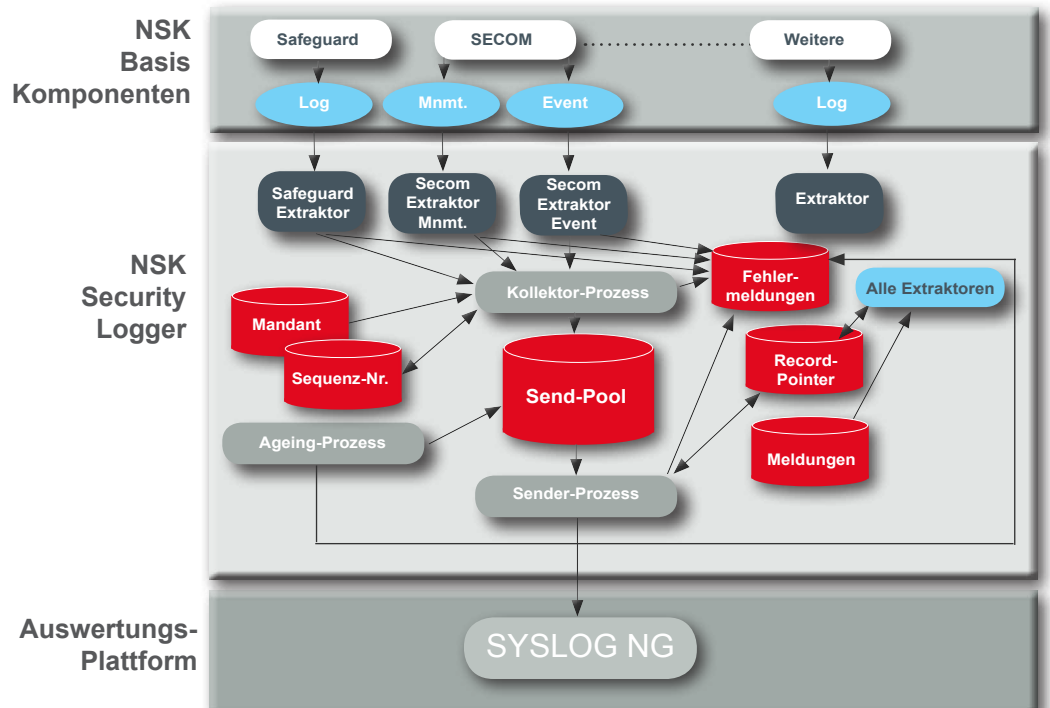
Siemensstr. 8-10
40885 Ratingen
Tel.: 02102 3004-0
Fax: 02102 3004-50

Einsteinstr. 55
89077 Ulm
Tel.: 0731 407697-0
Fax: 0731 407697-50

www.twinsoft.de
info@twinsoft.de

TSM V1/03.11

Komponenten NSK Security Logger





Der NSK Security Logger



Anwenderaktivitäten führen zu neuen Einträgen in der jeweiligen Logdatei der betroffenen Komponente. Die Extraktoren formatieren den Inhalt und schreiben die umformatierten Meldungen zeitnah in die HP-Nonstop SQL Datenbank und melden diese umgehend an die Auswertungsplattform ArcSight. Dabei werden die Begriffe zeitnah und umgehend streng gefasst (immediate fire). Über einstellbare Zeitintervalle führt das System eine Selbstüberwachung (heartbeats) und Aufräumaktionen (ageing/ housekeeping) durch.

Anstatt durch Tausende von Log-Datei-Sätzen, die aus unterschiedlichen Security-Subkomponenten (wie Safeguard, Secom, FTPS oder SSH) kommen, zu suchen, um Vorgänge im Nachhinein zu rekonstruieren, können Sie in Echtzeit über unzulässige Aktivitäten auf Ihrer NSK informiert werden.

Von Usern eingegebene sicherheitsrelevante Kommandos in der NSK Security Komponente werden vom TWINSOFT NSK Security Logger protokolliert, formatiert und an die außerhalb des NSK-Systems liegende ArcSight-Software übertragen. Alarmierungen können ausgelöst werden, wenn vordefinierte Schwellenwerte

überschritten werden, z.B. drei fehlgeschlagene Subkomponenten-Logins innerhalb von fünf Minuten, um Sie ständig auf dem Laufenden zu halten, wer auf Ihrem System was macht. Der TWINSOFT NSK Security Logger übernimmt diese Aufgabe.

Der ArcSight ESM untersucht die Extraktormeldungen aufgrund hinterlegter Regeln. Eine Regel könnte sein, wie oft innerhalb von 10 Minuten jemand ohne Erfolg versucht hat, sich einzuloggen. Beim Überschreiten eines vordefinierten Security-Schwellenwertes wird dann eine entsprechende Alarmierung verschickt. Die Firma ArcSight ist darauf spezialisiert, komplizierte Vorgänge nachzubilden, um entsprechende Schwellenwerte zu definieren.

Mittlerweile hat sich die Zusammenarbeit von TWINSOFT und ArcSight in weiteren Projekten bestens bewährt.

Die Funktionalität des NSK Security Loggers wird erweitert, um zusätzliche Ausgabeformate zu unterstützen.

Wir erzählen Ihnen gerne mehr über den NSK Security Logger - sprechen Sie uns einfach an.

TWINSOFT GmbH & Co. KG

Europaplatz 2
64293 Darmstadt
Tel.: 06151 39756-0
Fax: 06151 39756-50

Siemensstr. 8-10
40885 Ratingen
Tel.: 02102 3004-0
Fax: 02102 3004-50

Einsteinstr. 55
89077 Ulm
Tel.: 0731 407697-0
Fax: 0731 407697-50

www.twinsoft.de
info@twinsoft.de

TSM V1/03.11