

tacLOG

Management von Sicherheitsvorfällen. Zentralisierte Logfileanalyse und Sicherheitsüberwachung



Einführung in tacLOG

Seit die terreActive AG 1996 IT-Security-Dienstleistungen anzubieten begann, stellte sie wirksame und leistungsfähige Tools für das IT-Security-Management bereit. Angesichts ständig komplexer und vielfältiger werdenden Sicherheitsstrukturen wurde das Management stets schwieriger. Unser eigenes Security Control Center (SCC) und unsere Kunden benötigten bessere Tools zur Verwaltung der IT-Security und zur Abwehr neuer Bedrohungen.

tacLOG wurde von Sicherheitsexperten für Sicherheitsanalysten entwickelt, um die richtigen Antworten auf die tatsächlichen Probleme zu liefern.

Heute ermöglicht die tacLOG-Lösung den SCCs von Unternehmen eine effizientere Vorgehensweise sowie eine verbesserte Sicherheit. Führende Finanzanbieter, Regierungsbehörden und Hosting-Provider haben tacLOG implementiert, um schneller auf Bedrohungen reagieren zu können und die Sicherheit ihrer Netzwerke zu erhöhen.

Worin die Lösung besteht:

- Echtzeit-Management von Sicherheitsvorfällen mit RIT*-Technologie
- Sekundenschnelles Durchsuchen von Millionen von Vorfällen



- Appliance: Schnelle und einfache Implementierung bei garantierter Leistung



- Software: Für Linux- und Sun® Solaris-Plattformen

Erhältlich bei: www.terreActive.ch contact@terreActive.ch

Wer ist terreActive?

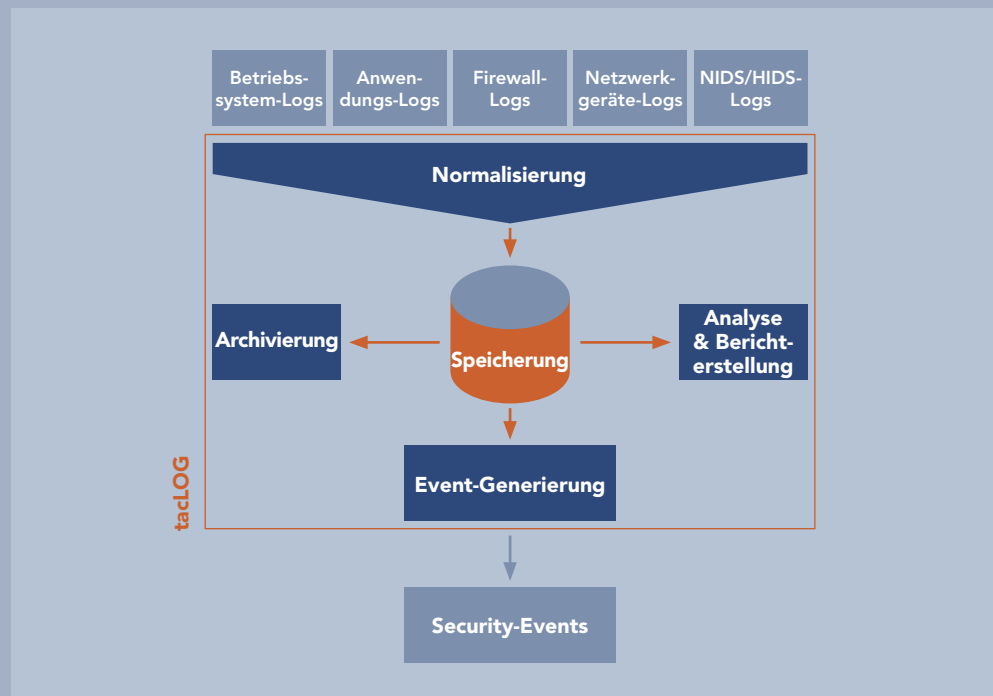
Führende Schweizer IT-Sicherheits-Firma.

Referenzen in Finanzinstituten und öffentlichen Verwaltungen.

Breites Know-how im Bereich IT-Security seit 1996.

* RIT: Realtime Inspection Technology – terreActive bietet eine extrem schnelle Inspektionstechnologie, die gängige Open Source-Komponenten mit der sicheren Linux-Distribution von terreActive kombiniert.





Was die Lösung kann

Normalisierung

- Datenkonvertierung – vom Syslog-Format in Text
- Gemeinsames Log-Format für verschiedene Datenquellen wie: SNMP-Trap, Mail, File, Eventreporter, Opsec usw.

Speicherung

- Zentralisiertes Logging – ermöglicht schnellen Zugriff und Berichterstellung
- Offene Schnittstellen – für externes Speichern und Archivieren
- Verteilte Architektur – unterstützt hochgradig skalierbare Lösungen

Archivierung

- Datenkomprimierung – optimiert die Festplattennutzung
- Zentrales Backup – bietet eine zentrale Archivierung aller sicherheitsbezogenen Mitteilungen
- Integritätssicherung – zur Verwendung im Audit-Trail

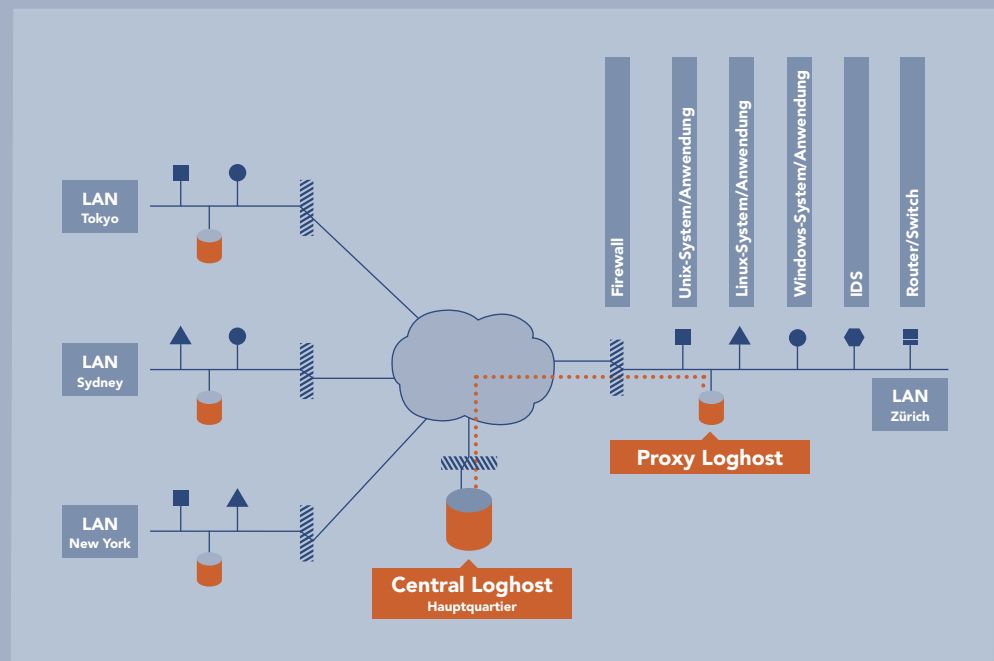
Analyse und Berichterstellung

- Intuitives webbasiertes GUI – mit sicherem Zugriff jederzeit und überall
- Benutzerprofile – ermöglichen personalisierten Datenzugriff
- Leistungsfähige Berichterstellung – für Analyse und Management von Trends



Event-Generierung

- Realtime Event Generierung (RIT) und Alarmierung – für eine rasche Reaktion
- Leistungsfähige Korrelationsfunktionen – für hohe Alarmqualität über alle integrierten Objekte hinweg
- Vordefinierte Muster – für eine schnelle und erfolgreiche SEM-Implementierung
- Informationsverdichtung – beispielsweise werden 10 Million Log-Einträge zu nur 20 Alarmen komprimiert
- Event-Schnittstellen – für die einfache Integration mit externen Helpdesk-Tools und Ticketing-Systemen



Wie die Lösung eingesetzt wird

tacLOG ist zweistufig aufgebaut. Auf der ersten Ebene erhält der tacLOG-Proxy die Logdaten der Systeme. Die Daten werden direkt nach dem Eingang mit Realtime Inspection Technology (RIT) überprüft.

Relevante Datensätze werden durch die Muster erkannt und erzeugen Events, die an tacLOG-Central weitergeleitet werden. Ein tacLOG-Proxy kann die Logdaten von mehreren hundert Systemen annehmen, prüfen und archivieren. Die Lösung ist auf mehrere tausend Systeme skalierbar.

tacLOG Central führt eine weitere Verdichtung und Korrelation der Daten durch, wobei ein oder mehrere Events zur Erzeugung eines Alarms zusammengefasst werden können. Diese Alarme stellen die verdichtete Form der ursprünglichen Logdaten dar und können von externen Helpdesk- oder Ticketing-Systemen verwendet werden.

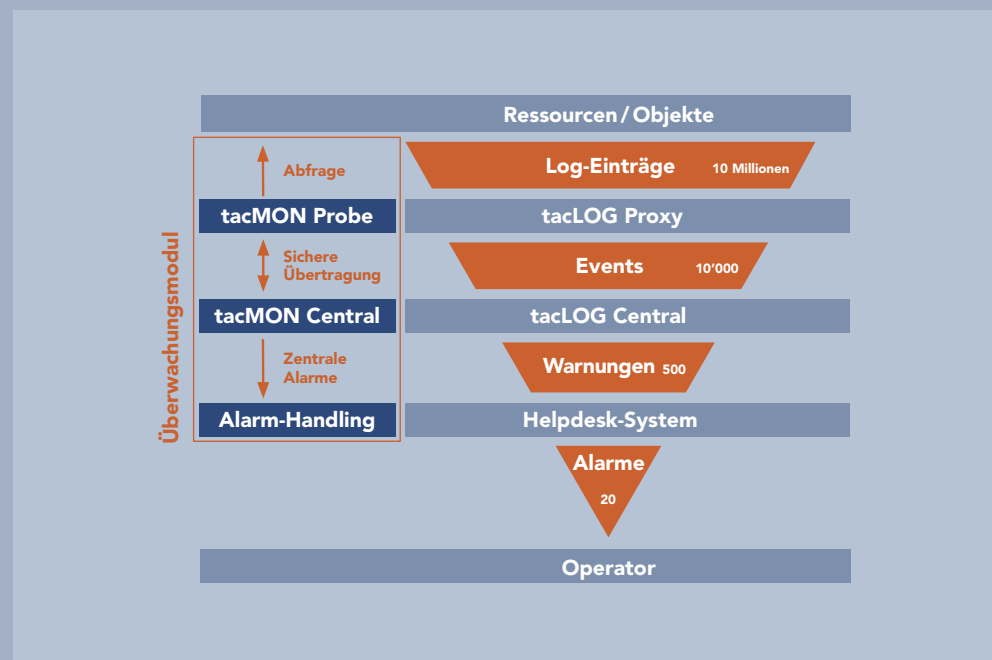


Dieser ganzheitliche Ansatz, der eine breite Auswahl an Geräten und Marken unterstützt, liefert dem zentralen Security-Team einen einzigartigen Überblick über den Sicherheitsstatus der von ihm betreuten IT-Umgebung.

Dank eines flexiblen Rollenmodells können bestimmte Informationen für verschiedene Mitarbeiter, Abteilungen oder sogar Unternehmen bereitgestellt werden. Dies ermöglicht eine bessere Zusammenarbeit sowie eine schnellere Reaktion auf Bedrohungen.

Übliche Rollen:

- Security Operator
- Netzwerk- / System- / Anwendungs-Operator
- Helpdesk und Support
- Management



Überwachungsmodul

tacMON ist eine Lösung zur System- und Netzwerküberwachung. Dieses Überwachungsmodul ist perfekt in die tacLOG-Architektur integriert und kann innerhalb der gleichen Appliance eingesetzt werden, wodurch eine ganzheitliche Übersicht über alle Objekte in der IT-Umgebung entsteht. tacMON und tacLOG werden über die Event-Ebene integriert. Dies ermöglicht eine zweistufige Korrelation aller eingehenden Informationen und somit eine erheblich verbesserte Alarmqualität. Der äusserst geringe Anteil an «False Positives» spart dank kürzerer Reaktionszeiten und schnellerer Problembehebung innerhalb des SCC Zeit und Geld.



Ihre Vorteile

Weniger Zeitaufwand und Kosten im Security-Management

Mit unserer RIT-Technologie wird eine Echtzeit-Generierung von Ereignissen aus tausenden von Objekten in Ihrem Netzwerk möglich. So erhält das SCC einen besseren Überblick über den aktuellen Status aller installierten Sicherheitsstrukturen, was den Wert dieser Investitionen steigert. Dank dieser neuen Transparenz kann das SCC schnell und präzise auf alle gemeldeten Vorfälle reagieren. Dies verbessert auch die interne Zusammenarbeit zwischen den verschiedenen am Prozess der Handhabung und Vorbeugung von Sicherheitsvorfällen beteiligten Abteilungen. So sparen Sie jeden Tag Zeit und Geld.

Verbessertes Management des Geschäftsrisikos durch mehr Transparenz

Zu wissen, was in der verwendeten IT-Umgebung geschieht, ist für das heutige Management entscheidend. Nur mit wirksamen Security Policies und strengen Kontrollprozessen kann sich ein modernes Unternehmen vor externen und internen Sicherheitsvorfällen schützen. Mit einem SEM-Tool wie tacLOG ist es möglich, einen Kontrollprozess zu gewährleisten, der das Management über Vorfälle informiert, bevor es zu spät ist.

Einhaltung gesetzlicher Vorgaben

Immer mehr Branchen sind zur Einhaltung bestehender gesetzlicher Vorgaben in Hinblick auf die IT-Security verpflichtet. Bedingungen wie Audit-Trails und die Archivierung relevanter Informationen wie z.B. Logdateien sind in den meisten Ländern bereits vorgeschrieben. Neue und zukünftige Vorschriften wie SOX oder Basel II werden die Art und Weise, wie Unternehmen ihre Sicherheit handhaben und überwachen, weiter verändern. tacLOG und die mit diesem Tool erreichte Transparenz stellen einen bedeutenden Fortschritt hinsichtlich der Einhaltung bestehender und neuer Standards für die IT-Security dar.

Die wichtigsten Produktvorteile

Geschwindigkeit und Skalierbarkeit

tacLOG ist ein schlankes und schnelles Software-Produkt, das für verschiedene Hardware-Plattformen optimiert werden kann. Die Linux-Appliance von terreActive basiert auf Intel®-Plattformen und erfüllt höchste Kundenanforderungen. Mit ihrer verteilten Architektur unterstützt die Lösung eine lokale oder weltweite Implementierung und skaliert mit jedem installierten tacLOG Proxy.

Optimales Preis-/Leistungsverhältnis

Die ohne Agenten konzipierte modulare Architektur ermöglicht die Integration aller Objekte in einer IT-Umgebung ohne zusätzliche Lizenzkosten. Somit werden die Kosten pro Objekt minimiert und der Investitionsaufwand gegenüber den Lösungen unserer Wettbewerber verringert sich.

In der Software ist ein Grundbestand an bekannten Mustern zum Filtern und Auffinden von Vorfällen enthalten. Dadurch werden Implementierungsprojekte beschleunigt und dem SCC-Team von Beginn an wertvolle Informationen geliefert. Angesichts der rasch zunehmenden Anzahl installierter Lösungen wird terreActive seinen Kunden kostenlos laufend neue Muster bereitstellen.

Schnelle Installation und geringe Wartungskosten

Durch die Verwendung vorinstallierter Appliances werden die Integration beschleunigt und gleichzeitig die Wartungskosten niedrig gehalten. Je nach den Anforderungen der Kunden bietet terreActive unterschiedliche Support-Level an:

- Basic: Software- und Hardware-Support
- Standard: Basic plus Überwachung und Systempflege
- Premium: Standard plus Konfiguration, Berichterstellung und Analyse

Leistungsfähige Open Source-Komponenten und einfache Integration

tacLOG wurde gemäss den «Recommended Practices for Security Improvement» des CERT entwickelt. Die integrierten Open Source-Komponenten sind allgemein bekannt und werden in Millionen von Installationen in der ganzen Welt eingesetzt. Diese breite Benutzerbasis macht in Kombination mit unserer Support- und Entwicklungsabteilung aus tacLOG ein äusserst stabiles und leistungsfähiges Produkt.

tacLOG ist für eine Integration mit bestehenden Helpdesk-Tools ausgelegt. Es unterstützt eine Vielzahl von Produkten und Anbietern.

Garantierter Software-Support

Uneingeschränkter Zugang zur Engineering Hotline von terreActive.

Wir garantieren für die Dauer von 3 Jahren einen Software-Support für jeden Release von tacLOG oder tacMON.

Software Upgrade Service – für uneingeschränkte Software-Releases von tacLOG und tacMON

Kontakt

Gerne erarbeiten wir Ihnen ein detailliertes Angebot. Kontaktieren Sie uns:

Kasinostrasse 30, CH-5001 Aarau
www.terreActive.ch, info@terreActive.ch

© terreActive AG

Die – auch auszugsweise – Reproduktion, Übersetzung sowie sonstige Verwendung der Inhalte dieser Publikation ist nur nach ausdrücklicher Genehmigung durch terreActive AG gestattet. Änderungen vorbehalten.



Wir sichern Ihren Erfolg.

terre**Active**
terre**Active**
terre**Active**
terre**Active**