

tacLOM 3.7 verfügbar – Die Highlights kurz erklärt

Kundeninformationen zum neuen Release der Security-Monitoring-Lösung tacLOM von terreActive AG

Aarau, 17.08.2017. Ab sofort ist die neue Version der Security-Monitoring-Lösung tacLOM erhältlich. Der Release 3.7 bietet Ihnen zahlreiche Neuerungen, von denen Sie direkt profitieren können. Im Folgenden eine Auflistung der wichtigsten verbesserten Eigenschaften.

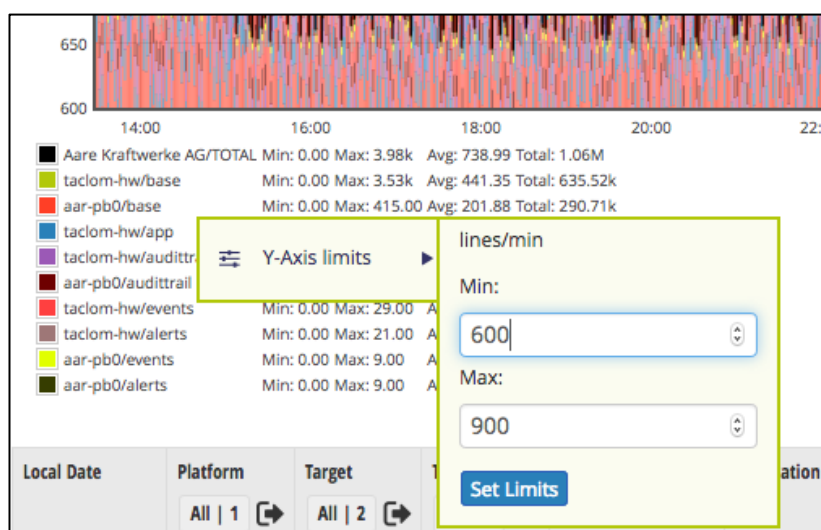
Auch mit der neuen Version bleibt der Hauptnutzen von tacLOM erhalten: Sie können Störungen und Abweichungen vom Normalbetrieb schnell erkennen, sofort lokalisieren und einschätzen. Dies hilft dem Betriebsteam, Fehlkonfigurationen und Ausfälle rasch zu finden, sowie auch den Sicherheitsverantwortlichen, auf Gefahren und Angriffe proaktiv zu reagieren. Mittels konsolidierten Ansichten und Dashboards hat auch das Management den aktuellen Sicherheitsstand der Infrastruktur immer unter Kontrolle.

1. Log Availability Scanner

Mit diesem neuen Scanner können Sie mit wenigen Klicks eine Überwachung einrichten, die alarmiert, wenn die entsprechende Log-Quelle unerwartet versiegt.

2. Skalierbare Y-Achse

In Monitoring- und Log-Management-Grafiken können die Y-Achsen nun individuell angepasst werden. Dadurch können auch kleine relative Änderungen von grossen absoluten Zahlenwerten detailliert analysiert werden.



3. Drill-down von der Eventkonsole auf die Log-Zeile

Die Eventkonsole von tacLOM bietet neu eine drill-down Funktion für alarmierte Log-Ereignisse. Diese intuitive Verknüpfung der Alarmierungen mit den jeweils auslösenden Log-Meldungen ermöglicht dem Anwender das Problem schneller zu verstehen und zu bearbeiten.

Events aar-srvlprx1

Filters Pending events Show 50 entries Show / hide columns

| Select | Detail | First | Last | Failures | Project | System | Description | Operator Name |
|--------------------------|--------|---------------------|---------------------|----------|---------|--------------|-----------------------------|---------------|
| <input type="checkbox"/> | | 27.06.2017 14:56:01 | 27.06.2017 14:56:01 | 1 | Server | aar-srvlprx1 | LOG:Malware link clicked () | nobody |

Event **Work process state** new

| Platform | Target | Type | Local Date | Label | Application | Message |
|----------|--------------|--------|-----------------|--------------------|------------------|-------------------------|
| proxy | aar-srvlprx1 | alerts | Jun 27 14:56:01 | ALERT_0149_Malware | squid_access_log | Malware link clicked () |

| Platform | Target | Type | Local Date | Label | Application | Message |
|----------|--------------|--------|-----------------|--------------------|------------------|-------------------------|
| proxy | aar-srvlprx1 | events | Jun 27 14:56:01 | EVENT_0149_Malware | squid_access_log | Malware link clicked () |

| Platform | Target | Type | Local Date | Label | Application | Message |
|----------|--------------|------|-----------------|-------------|------------------|---|
| proxy | aar-srvlprx1 | base | Jun 27 14:56:01 | user.notice | squid_access_log | 1141034517.621 180194 10.212.0.42 TCP_HIT/304 1320 P... |

4. CSV Export

Die im GUI angezeigten Log- und Monitoring-Daten können nun auch als CSV exportiert und direkt heruntergeladen werden.

Event Console **Monitoring** **Log Management** **Settings** Last reload: 15:16:34 admin (supervisor) Version: 3.6.2-4218

Show 50 entries Show / hide columns

System Description simple Operator Name

All | 5

Export table data to csv

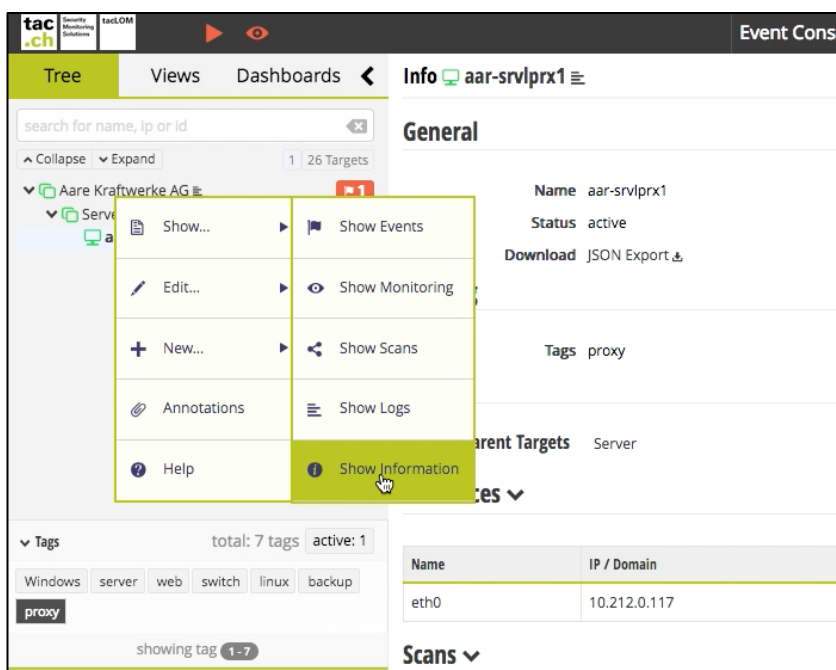
5. Tagging von Dashboards und Views

Neu können auch Public Dashboards und Views getaggt werden. Dadurch erlangen Sie eine bessere Übersicht und es ermöglicht Ihnen, Benutzern mit eingeschränkten Rechten nur die Ansichten freizuschalten, die sie auch sehen sollen.

6. Neue Target-Informationsansicht

Für die im Target-Tree erfassten Projekte und Systeme gibt es nun eine neue Informationsansicht. In dieser Ansicht sind alle Detailinformationen nur zum Lesen einsehbar. Die über- sowie untergeordneten Objekte sind über direkte Links aufrufbar.

Ausserdem bietet die Informationsansicht eine Exportfunktion. Diese liefert eine im JSON-Format strukturierte Exportdatei, die zusätzlich auch die Informationen aller untergeordneten Objekte beinhaltet.



7. Verbesserungen beim Wartungsfenster (Service Window)

Wartungsfenster können nun auch modifiziert werden. Neu erstellte Wartungsfenster sowie Änderungen an periodischen Wartungsfenstern werden nun sofort aktiv.

8. Dynamische URL basierend auf Filterauswahl

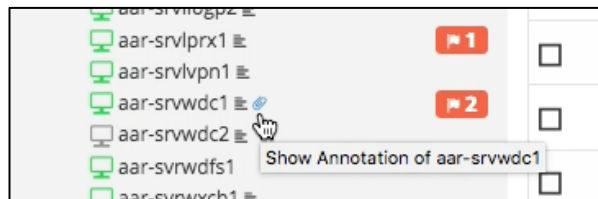
Eingestellte Filter werden nun in die Browser-URL hineincodiert. Dadurch können sie einfach als Lesezeichen abgespeichert oder weitergegeben werden.

9. Direktes Editieren der Log-Berechtigungen im GUI auch für lokale Benutzer

Mit der Version 3.5 wurde im Zusammenhang mit der erweiterten Active-Directory-Anbindung ein neues Permission-Objekt eingeführt, mit dem sich die Log-Berechtigungen fein granuliert direkt im GUI einstellen lassen. Seit der Version 3.6 können die so definierten Berechtigungen auch für lokale Benutzer angewandt werden.

10. Onlinehilfe- und Kommentarfunktion (Annotation Window)

Die Onlinehilfe- und die Kommentarfunktion wurden überarbeitet. Neu weist ein Indikator im Target-Tree, der Scan-Liste oder in der Event-Konsole darauf hin, wenn zu einem Objekt ein Kommentar vorhanden ist. Auf diese Weise lassen sich Handlungsanweisungen im Falle eines Events direkt in tacLOM erfassen.



11. Bessere Monitoring-Unterstützung von Cisco Nexus, SEPPmail und PulseSecure

Durch neue Discovery-Module im SNMP-Scanner können Cisco Nexus-, SEPPmail- und PulseSecure-Geräte detailliert überwacht werden.

12. Automatisches Erfassen von Log-Targets im Tree¹

Empfängt tacLOM Log-Daten, die keinem bereits erfassten System im Target-Tree zugeordnet werden können, so kann das System die unbekannten Targets nun automatisch erfassen und gegebenenfalls auch gleich die im Standard definierten Scans einrichten. Diese Systeme erscheinen in einem gesonderten Projekt und können vom Benutzer in die richtigen Projekte einsortiert und aktiviert werden.

13. Eventpack Integration¹

Eventpacks beinhalten Regeldefinitionen, mit denen Log-Ereignisse für ein entsprechendes Produkt normalisiert und ggf. alarmiert werden können. Die verfügbaren Eventpacks können im GUI angezeigt und selektiv aktiviert oder deaktiviert werden. Folgende Eventpacks stehen bereits zur Verfügung und werden mit tacLOM 3.7 ausgeliefert:

- McAfee ePolicy Orchestrator 4
- Microsoft SQL Server
- BalaBit SCB
- Windows
- Fortinet Fortigate
- Alto Networks Firewalls
- Juniper ScreenOS

Ihr nächster Schritt:

Wenn Sie von den oben genannten neuen Eigenschaften profitieren möchten, nehmen Sie bitte mit Ihrem terreActive Account Manager oder Site Manager Kontakt auf. Wir koordinieren dann gerne mit Ihnen gemeinsam das weitere Vorgehen für eine reibungslose Umstellung auf den neuen tacLOM Release.

¹ Diese Funktionen befinden sich in der Pilotphase. Sie werden von ausgewählten Kunden bereits produktiv eingesetzt und getestet, sind aber standardmässig noch deaktiviert. Die Aktivierung durch terreActive ist auf Kundenwunsch hin möglich.