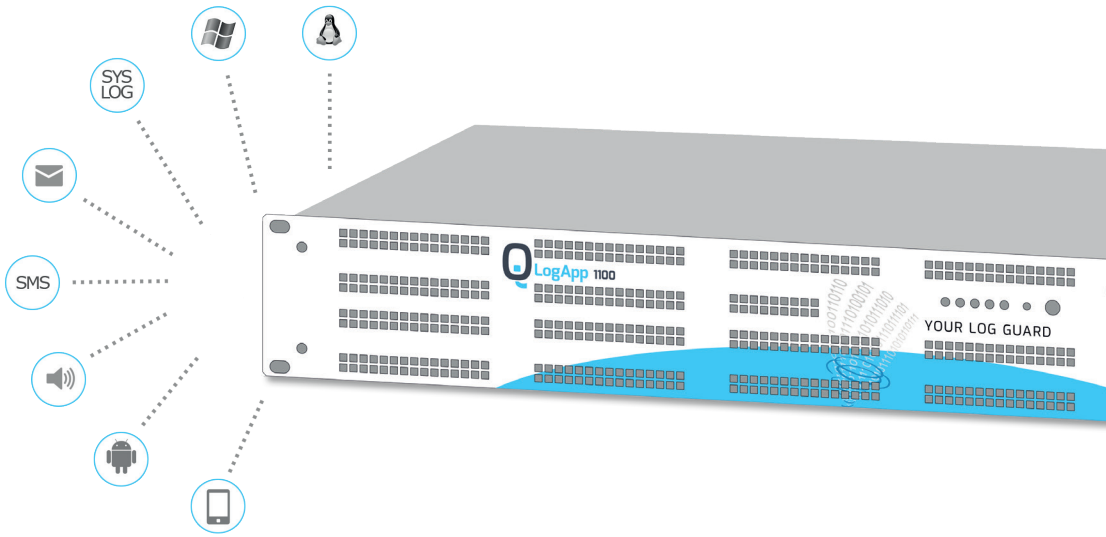
LogApp - Verordnungskonforme Protokollierung
Das Werkzeug für IT-Sicherheit und Compliance

iQSol
Security made in Austria.



LogApp

Endlich vernünftig: iQSol Log-Management ermöglicht umfassenden Datenschutz und bringt Security-Management auf den nächsten Level. Als Managed Security Service ist es rasch im Einsatz und absolut kalkulierbar!

Wer hat wann und wo (un-)erlaubterweise zugegriffen?

Erst mit unserer zentralen Protokollierung der Logs aus Betriebssystemen, Datenbanken, Applikationen und Netzwerkgeräten ist eine forensische Analyse möglich. Internationale Standards und die EU-DSGVO verlangen den Nachweis von Zugriffen. Log-Management sammelt als zentrale Datendrehscheibe Informationen aus vielen Quellen und ermöglicht die Analyse von Zusammenhängen und Angriffsmustern. Durch Testverfahren ist es möglich, Datenintegrität zu überprüfen und Veränderungen festzustellen („File-Integrity-Monitoring“).

Das smarte OT SIEM „Made in Austria“

Die LogApp schützt auch OT-Umgebungen zuverlässig: Diese sind oft das Herzstück von kritischen Infrastrukturen und müssen unbedingt gegen unerlaubte Zugriffe und Manipulation abgesichert werden. Genau das verlangt die EU mit den Sicherheits-Standards der NIS2-Richtlinie. Die LogApp ist die smarte Lösung für ein Next Generation OT SIEM und macht es möglich, zahlreiche NIS2-Anforderungen und andere gesetzliche Vorgaben mühelos zu erfüllen.

TIPP PROJEKTABLAUF!

In einem ersten Schritt empfehlen wir die Integration von zentralen Diensten und den Betriebssystemen. Im Zuge dessen erfolgt zum Beispiel ein Windows-Hardening mit Bordmitteln und somit bereits eine Verbesserung der IT-Security für die nächsten Monate. Über mehrere Wochen werden Reports generiert und angepasst sowie das Feintuning kontinuierlich ausgebaut. In Zusammenarbeit mit Consultants vor Ort oder remote bzw. mit den Spezialisten des iQSol MSSPs werden bekannte Einfallstore geschlossen.

LogApp

Kernfunktionen

- verfügbar On-Premise als Hardware oder als virtuelle Appliance
- zentrales Management mit manipulationssicherer Archivierung
- LogAgents für Windows- und Linux-Server sowie Windows-Clients
- Syslog-Anbindung von Netzwerkgeräten und anderen Syslog Quellen
- SNMP-Anbindung von Netzwerkkomponenten
- Kaskadierung LogApps
- wahlweise verschlüsselte Kommunikation zwischen LogAgent und LogApp
- Alarmierung per E-Mail oder iQSol Alert Messaging Server (SMS, Voice)
- umfassendes Reporting (Enterprise-Reporting-Services)
- Vier-Augen-Prinzip für Events und Alarme (online und Archiv)
- umfangreiches Rollenkonzept

LogAgent

LogAgents sammeln Events von Windows- oder Linux-Servern und leiten diese an eine LogApp weiter. Archivierung, Korrelation und Alarmierung werden vollständig von der LogApp übernommen.

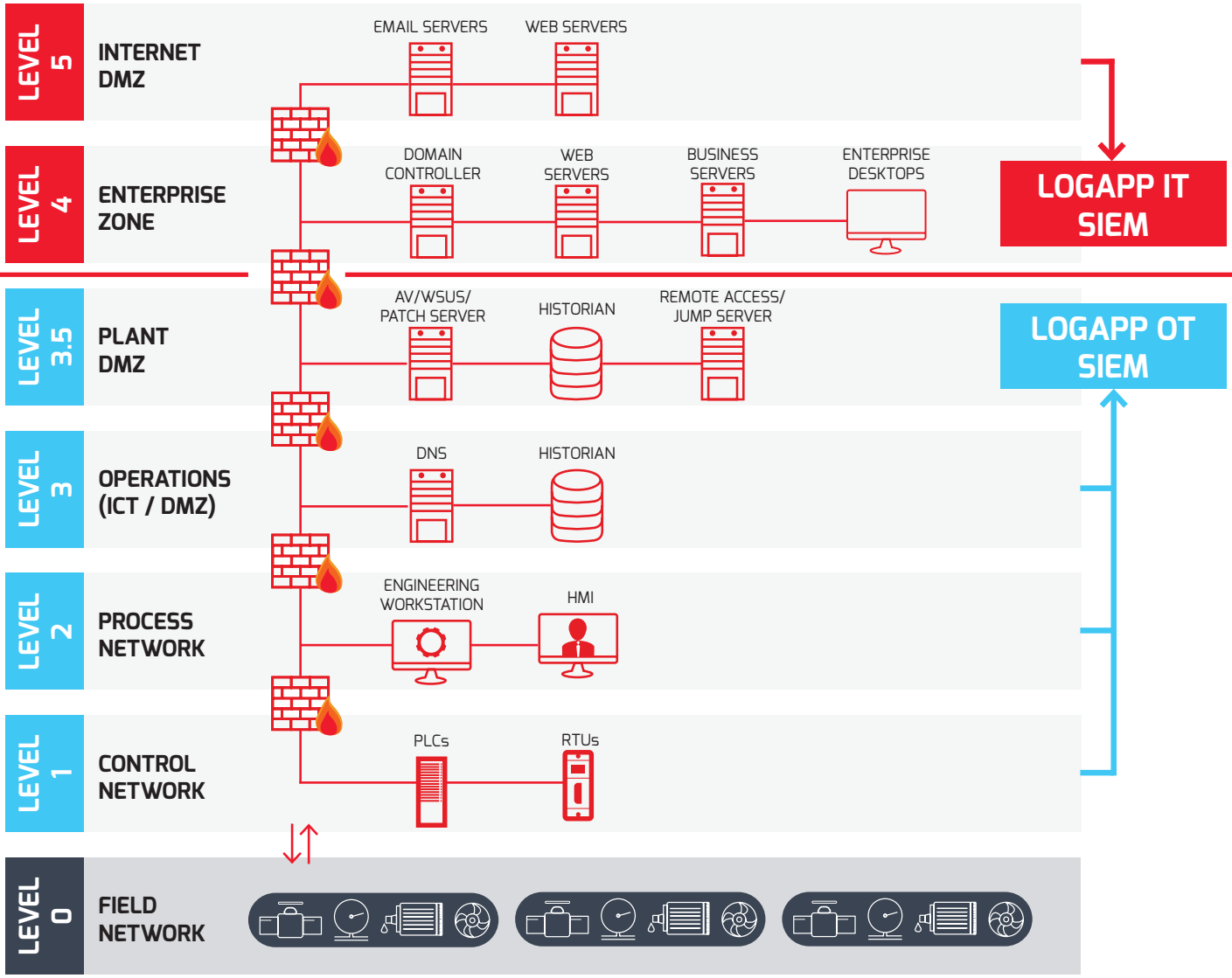
Alle **Events** werden über einen **verschlüsselten Kanal an die LogApp weitergeleitet.** Geografisch verteilte Szenarien können effizient und sicher abgebildet werden. LogAgents stehen für Windows und Linux zur Verfügung und stellen keine besonderen Anforderungen an die Systemressourcen.

Agent Features

- Log Formate
  - Windows-Event-Logs (Application, Security, Setup, System, ...)
  - Linux-System-Logs (User Authentication, ...)
  - Log-Files (Flatfiles, XML, CSV, ...)
- File-Integrity-Monitoring
- Windows-Change-Auditing
- Syslog- und SNMP-Proxy-Funktionalität
- Buffer-Funktion
- verschlüsselte Übertragung (optional)
- Remote oder lokale Installation

Syslog

Ereignisse von Netzwerkgeräten und anderen Syslog Quellen können direkt an eine LogApp gesendet werden. Die Syslog-Schnittstelle übernimmt und verarbeitet Ereignisse analog zu Ereignissen von einem LogAgent. Wahlweise können auch LogAgents als Syslog- und SNMP-Proxy konfiguriert werden, um in komplexeren Netzwerk-Architekturen Ereignisse dezentral zu sammeln.



Durch die Möglichkeit, LogApps zu kaskadieren, können zahlreiche Szenarien hinsichtlich Event-Sammlung, Alarmierung und Archivierung abgebildet werden. Sowohl die Zusammenführung aller Events der untergeordneten LogApps als auch eine selektive Weiterleitung sicherheitskritischer Events ist konfigurierbar. Alarmierungen können auf den untergeordneten oder auch nur auf der hierarchisch obersten LogApp-Ebene ausgelöst werden.

Webinterface für LogApp

- einfache Administration von LogAgents, Syslog- und SNMP-Quellen
- Benutzer- und Gruppenverwaltung mit Active-Directory-Anbindung
- umfangreiche Filter- und Suchfunktion in Alarmen und Events
- Import und Export von Regeln
- Dashboard mit Systeminformationen und Reports
- ausführliches System Protokoll
- Mandantenfähigkeit
- Mehrsprachensupport

Technische Spezifikationen

	LogApp 2700	LogApp 1200	LogApp 700	LogApp VM
Hardware				
Cores	12C / 2.4 GHz	12C / 2.0 GHz	8C / 1.8 GHz	mind. 4
RAM	64 GB	32 GB	16 GB	mind. 4 GB
HDD-Kapazität	8x 1.8 TB 10K SAS 12G	4x 2 TB 7.2k SATA 6G	4x 1 TB 7.2k SATA 6G	mind. 250 GB
RAID	RAID 10	RAID 10	RAID 10	-
LAN	4x Gigabit Ethernet	4x Gigabit Ethernet	4x Gigabit Ethernet	1-2x Gigabit Ethernet
Abmessungen	19“ 1 HE	19“ 1 HE	19“ 1 HE	-
Netzteil	Dual	Dual	Dual	-
Defective Media Retention	inkl.	ink.	inkl.	-

LogApp 2700 ist die performanteste LogApp-Anwendung. Mit hoher Ressourcenausstattung werden Events gesammelt und korreliert. Ein Raid-Controller und ein redundantes Netzteil sorgen dabei für maximale Zuverlässigkeit. Durch die hohe Performance eignet sich die LogApp 2700 speziell für große Unternehmen mit einem geografisch verteilten Netzwerk und einer großen Anzahl von LogAgents und Syslog Quellen.

Unterstützte Betriebssysteme

LogAgent für Windows Windows 10 / 11, Windows Server 2022 / 2019 / 2016 (ältere Versionen auf Anfrage)

LogAgent für Linux Red Hat Enterprise Linux und CentOS ab Version 7 (ältere Versionen auf Anfrage)
Ubuntu ab Version 14.04 (ältere Versionen auf Anfrage)
SUSE Linux Enterprise und OpenSUSE ab Version 12 (ältere Versionen auf Anfrage)

Weitere Vorteile

- kalkulierbare Lizenzierung nach Anzahl der Server und Applikationen
- kostengünstiger Einstieg in das Log-Management und smarte OT SIEM-Lösung
- Rechtssicherheit mit europäischer Software
- revisionssichere Archivierung
- Vier-Augen-Prinzip für Echtzeitdaten und Archiv

TIPP ORGANISATION!

Die Erfahrung zeigt, dass Log-Management durch Spezialisten und eingespielte Teams abgehandelt wird, also einem MSSP Ihrer Wahl. Ein bisher gemiedenes, teures Projekt wird dadurch zu einem laufenden Betrieb mit monatlichen, kalkulierbaren Kosten. Regelmäßiges Reporting und der Zugriff auf Security-Know-How spricht für die Partner von iQSol – oder im Idealfall für Ihren bestehenden Dienstleister.

iQSol GmbH, Petrusstraße 20, A - 3312 Oed T: +43 7472 207 67 E: office@iqsol.biz W: www.iqsol.biz