

ProLog Regelwerk Paket

„Das beste aus Millionen von Events“

Nach diesem Konzept bietet Ihnen die Firma NETZWERK die Möglichkeit von den Erfahrungen und Empfehlungen aus dem Praxis und sogar Bankenumfeld zu profitieren die Bereits ProLog® einsetzen.

Zusammen mit vier rheinlandpfälzischen Sparkassen werden in regelmäßigen Workshops Richtlinien und Empfehlungen erarbeitet.

Berichtswesen

Anhand der vorgefertigten Berichte, erhalten Sie ohne großen Aufwand die benötigten Informationen aus ProLog® auf Abruf oder zeitgesteuert. Zum Beispiel:

- Anzahl zurückgesetzter Kennwörter pro Tag/ Monat/Quartal
- Anzahl geänderte Benutzerkonten
- Anzahl gelöschte/deaktivierte Benutzer
- Übersicht getätigter Depseudonymisierungen
- Aggregierte Zahlen von Microsoft Security Events

ProLog® Filter

Ersparen Sie sich das mühevoll definieren von eigenen Filtern und Regeln in ProLog®.

Monitoring

IT@WORK ProLog® bietet Ihnen die Möglichkeit alle Netzwerkgeräte in Ihrer IT Infrastruktur zu Überwachen. Das Regelwerk Paket liefert Ihnen praxisnahe und allgemeingültige Empfehlungen welche Geräte Sie überwachen sollten, mit welchen Schwellwerten und wann es sich lohnt benachrichtigt zu werden.

praxisnahe Empfehlungen

Die Ergebnisse des Workshops werden Revisoren und Verbandsrevisoren vorgelegt und stetig ergänzt.

Zugang zum ProLog® Portal

Mit dem Regelwerkpaket erhalten Sie Zugang auf neue Berichte, Filter, Empfehlungen und Ergebnissen aus zahlreichen Workshops in unserem Produktportal.



ANSPRECHPARTNER:

Niederlassung Frankfurt:

Folker Gollan

Fon: +49 (69) 78 07 98 82
Mob: +49 (152) 22 99 65 30

Email: folker.gollan@netzwerk.de

Niederlassung Stuttgart:

Marco Fritz

Fon: +49 (711) 220 54 98 48
Mob: +49 (152) 22 99 65 10

Email: marco.fritz@netzwerk.de

Niederlassung München:

Rebekka Herdtle

Fon: +49 (711) 220 54 98 17
Mob: +49 (152) 22 99 65 01

Email: rebekka.herdtle@netzwerk.de

ProLog Regelwerk Paket



Exemplarische Montoring Vorlagen:

Allgemein:

- Arbeitsspeicher Auslastung
- Dienststatus von Windows Diensten
- Freier Speicherplatz
- Prozessorauslastung
- Prozessesstatus des ProLog Clients
- Terminalserver Sitzungen
- Überwachung von Port Verfügbarkeiten (z.B. HTTP, SMTP, ...)
-

Lotus Notes:

- Notes - Anzahl ausstehender Mails
- Notes - Anzahl toter Mails
- Notes - Anzahl wartender Mails
- Notes - Aufgabenzugriffsverletzungen der letzten Stunde
- Notes - Datenbank Cache Treffer
- Notes - Datenbank Cache Ueberfuellung
- Notes - Datenbanken im Cache
- Notes - Dienst nAdminp
- Notes - Dienst nAMgr
- Notes - Dienst nEVENT
- Notes - Dienst nRouter
- Notes - Dienst nSERVER
- Notes - Dienst nUPDATE
- Notes - erfolglose Aufgaben

Exemplarische Filtervorlagen:

Microsoft Security Events:

- Microsoft Security ID 512 — Windows wird gestartet
- Microsoft Security ID 513 — Windows wird heruntergefahren
- Microsoft Security ID 528 — erfolgreiche Anmeldung
- Microsoft Security ID 529 — gescheiterte Anmeldung
- Microsoft Security ID 531 — deaktiviertes Konto
- Microsoft Security ID 553 — abgelaufenes Konto

* zwischenzeitliche Änderungen vorbehalten

Das Regelwerk beinhaltet zahlreiche weitere Filtervorlagen für Microsoft Security Events.

Weiterhin finden Sie Filter und Berichte für die gängigsten Anwendungen im Industrieumfeld. Wie zum Beispiel:

- Symantec BackupExec
- Microsoft
- Linux
- Squid
- McAfee ePO
- Citrix
- VMware
- IBM TSM
- Cisco ACS

Empfehlungen und Regeln zur Pseudonymisierung personenbezogener Daten wie zum Beispiel

- Kreditkartennummern
- Benutzernamen
- IP Adressen
- E-Mail Adressen
- Webseiten
- Dateinamen in Druckaufträgen

Prozessbezogene Berichte

Kontrollieren Sie die tägliche Arbeit anhand Ihrer Events z.B.

- Alle Events beim Löschen eines Benutzers von den verschiedenen Systemen
- Alle Events beim Anlegen eines Benutzers von den verschiedenen Systemen
- Alle Events beim sperren eines Benutzers von den verschiedenen Systemen