senhasegura®

Bedrohungsanalyse

Automatische Analyse der wichtigsten Aktivitäten

Was ist das?

Umgebungsüberwachung zum Erkennen und Melden verdächtiger Aktivitäten mithilfe privilegierter Anmeldeinformationen.

Wie funktioniert das?

Es wir fortlaufend eine Liste der im System beobachteten Befehle und verdächtigen Verhaltensweisen erstellt. Sie werden nach dem Grad des Risikos klassifiziert und, falls sie erkannt werden, konsolidiert und im Administrationsbereich grafisch angezeigt.

Funktionen

- Kontrollpanel, das alle Risiken und Bedrohungen in grafischer Form anzeigt;
- Detaillierte Warnungen zu verdächtigen Aktivitäten;
- Analyse von Benutzersitzungen;
- Audit-, Alarm- und Blockierungsbefehle;
- Speicherung von Befehlsprotokollen;
- Markieren Syntax von Befehlen;
- Identifizierung von Querverkehr und Eskalation von Berechtigungen;
- Warnungen vor verdächtigen Aktivitäten für SIEM/SYSLOG.

Technische Funktionen

- Automatisches Lernen des Benutzerverhaltens und Betrieb von Geräten;
- Blockierung von Befehlen auf der Basis von weißer und schwarzer Liste;
- Automatische Reaktion, wenn eine Bedrohung erkannt wird.

Vorteile

- Erkennen potenzieller Schwachstellen
- Beschleunigte Reaktion im Falle eines Angriffs
- Automatische Blockierung gestohlener Anmeldeinformationen;
- Bedrohungserkennung;
- Vollständige Informationen zum Vorfall.