AlertEnterprise

DATA SHEET

Identity Intelligence Technology

Closing The Security Gaps Through Automation

While most security teams are focused on preventing malicious outsider attacks, recent data suggest that close to 30 percent of confirmed breaches today involve insiders. Today's increasingly complex networks across physical, IT and OT systems make it difficult for security teams to detect and prevent insider threats.

"Automation marks the difference between engaging in a recipe for failure and loosening your dependency on luck."

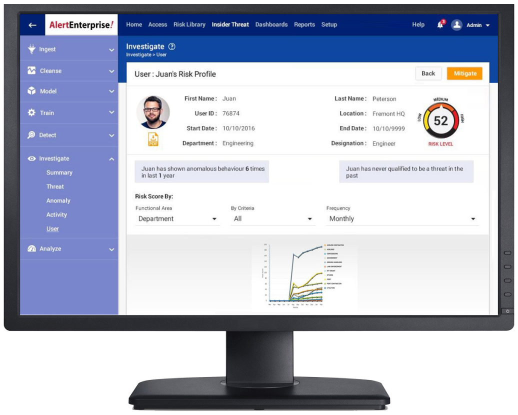
Relying on manual detection of insider or external threats, is no longer a viable solution. An automated system, powered by artificial intelligence, is now the most practical and human error-proof solution today.

Features and Benefits

- Comprehensive and thorough prevention of Insider Threat
- Maintain an identity profile for every employee and contractor and automate the background check, criminal history and all other vetting procedures
- Each individual identity profile is assigned a risk score based on job role, access to critical assets, areas and information
- Introduces risk management into the business and security process
- Ability to conduct risk analysis prior to provisioning access
- Maintain anonymized access and behavior profiles for staff
- Generate security alerts for access attempts outside normal shift hours, or systems not normally accessed
- Automatically enforce policies with access to classified information
- Only allow access when physically present in a SCIF or other secured facilities
- Active Policy Enforcement delivers true security
- Reduction in time and cost for detecting and resolving risk

AI-Powered Identity Intelligence Technology

AlertEnterprise Identity Intelligence technology dramatically reduces the time and cost for detecting and resolving risk by automating threat protection, across IT, physical, and operational systems, from one place. Its enhanced machine learning capabilities automatically baseline identity profiles, allowing it to quickly sort through millions of events to detect behavior anomalies and trends for an effective response to potential malicious behavior and policy violations.



User : Juan's Risk Profile

First Name : Juan
User ID : 76874
Start Date : 10/10/2016
Department : Engineering
Last Name : Peterson
Location : Fremont HQ
End Date : 10/10/9999
Designation : Engineer

Juan has shown anomalous behaviour **6** times in last **1** year

Juan has never qualified to be a threat in the past

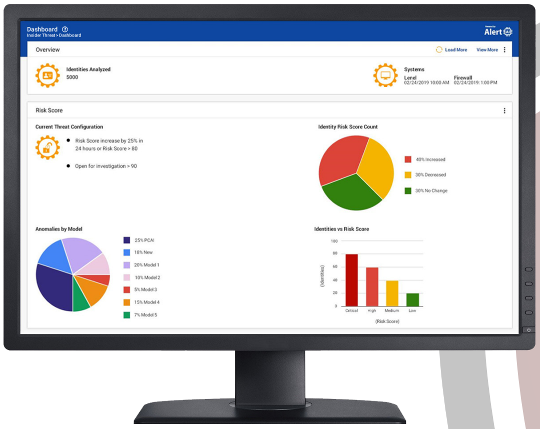
Risk Score By:
Functional Area: Department
By Criteria: All
Frequency: Monthly

Situational Intelligence

The system delivers a clear view of what's happening across an enterprise, providing context and awareness of correlated events, and empowering Security Operation Center personnel to make informed decisions and respond appropriately.

Turns Data Into Insight And Action

Powerful dashboards provide operators with a risk score assigned to individual identity profiles based on access to critical assets, areas, and information, enabling them to conduct a proactive risk analysis before provisioning or removing access.



Identities Analyzed
5000

Systems
Lenel 02/24/2019 10:00 AM
Firewall 02/24/2019: 1:00 PM

Current Threat Configuration
- Risk Score increase by 25% in 24 hours or Risk Score > 80
- Open for investigation > 90

Active Policy Enforcement

The patented active policy enforcement rules-based engine automatically identifies policy violations and unauthorized access, allowing security managers to proactively monitor, and respond to suspicious behavior, criminal activity, security violations, as well as operational and procedural issues.