securonix

SOLUTION BRIEF

Insider Threat Detection & Response

Monitor and mitigate threats from malicious and compromised insiders

Stop Risky Insiders

More than two-thirds of attacks or data loss incidents originate from insiders. Mitigating this risk is difficult because, unlike external attackers, insiders already have login credentials and permission to access critical data and intellectual property. Left unchecked, both compromised and malicious insiders can cause massive data breaches and damage to your organization.

Securonix for Insider Threat Detection & Response

Securonix helps detect insider threats with real-time monitoring, while advanced behavioral analytics brings context and clarity to alerts. Securonix lets you detect and respond to both external and internal threats with our Next-Gen SIEM solution, that is powered by industry-leading behavior analytics. Machine learning algorithms allow you to stitch together a series of events to surface the highest risk alerts and identify low and slow attacks with threat models that map to both the MITRE ATT&CK and US-CERT frameworks.

; padding
nt-size: 20px;
in: 0; text-align
or: #428BCA; positio
loat: left; margin: 1px 0 0 5px;}
eft; }
height: 73px !important;}
ant; height: 225px; padding: 5px 0px !important; border:
tant;}
x !important;}
ne; -khtml-user-select: none; -moz-user-select: none;
ransform: rotate(180deg);transition: all 0.5s ease-out 0s;}
mportant;}
om: 5px !important;}
10px; margin-left: 35px;}
border-radius: 5px !importan
portant;}
top-color: #
0 1px 4px

Solution Benefits

Mitigate the risk of insider attacks with advanced behavioral analytics from Securonix.

Quickly Detect and Respond to Threats From Within

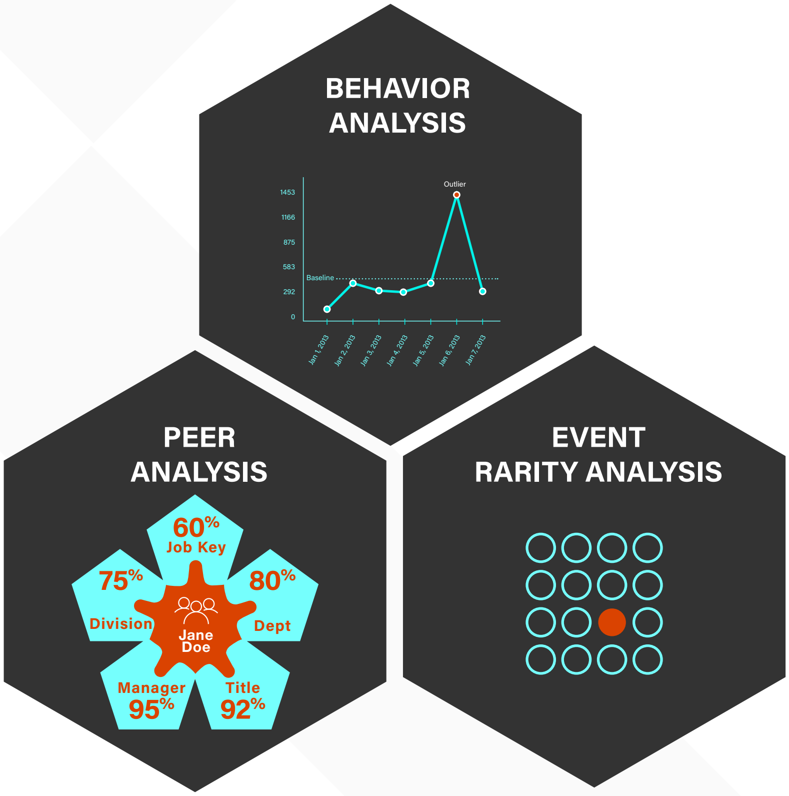
Insiders regularly access valuable data as a part of their job. This access can pose a huge risk when left unmonitored. Using behavioral analytics, you can identify and investigate when user access patterns deviate from normal behaviors.

Monitor the Highest-Risk Users

Even with behavioral analytics, it is difficult to find abnormal user behavior. Many users and entities have multiple accounts and may work on different networks. Securonix gives you the ability to track users across multiple accounts and trace lateral movement and nefarious activity.

Hunt for Threats in Real-Time

Insider threats often use low and slow attacks to avoid detection. To address this, Securonix Next-Gen SIEM streamlines threat hunting using both historical and real-time data.



How it Works

Securonix Next-Gen SIEM gives your security team fast detection, and response at cloud scale and integrates seamlessly with data sources, threat intelligence tools, and other technologies in your SOC. Powered by industry-leading analytics, our solution enables analysts to stay ahead of insider threats with the ability to:

- Generate comprehensive identity and risk profiles for every user and entity in your environment.
- Monitor user's access and activities around critical assets with out-of-the-box analytics content and patented machine learning algorithms.
- Identify insider attacks that span across multiple alerts with threat models that map to both the MITRE ATT&CK and US-CERT frameworks.

Detect Compromised Credentials

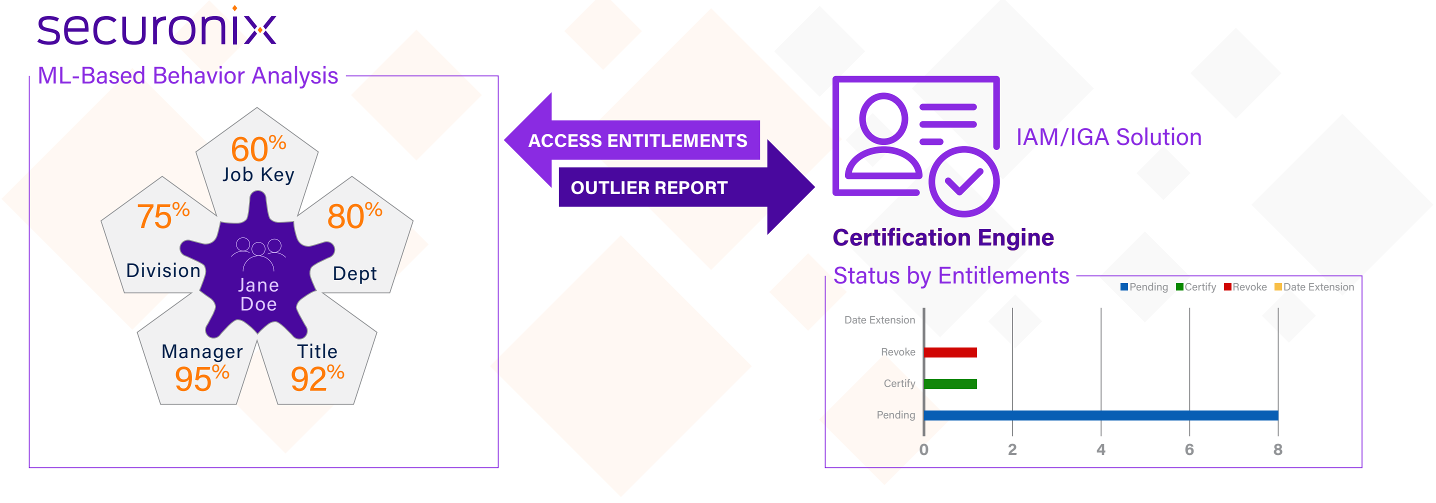
With 61% of breaches involving credentials, the need for identity analytics is crucial to staying ahead of cyber threats. Securonix helps you make dynamic, informed access decisions by collecting data from your IAM solution and correlating it with user risk intelligence. Securonix can rapidly recognize high-risk users by comparing the actions of one user against their peers, allowing you to automate manual outlier anomaly detection. Once you identify high-risk users, you can add them to a watch list to keep a close eye on their activities.

Cover Top Insider Threat Monitoring Use Cases

Catch common insider threats with Securonix, including:

- Stop data exfiltration
- Detect compromised credentials
- Identify lateral movement
- Monitor privileged accounts
- Identify attackers evading detection

For more information about Securonix, schedule a demo at:
www. securonix.com/request-a-demo



About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.
For more information visit securonix.com