Insider Threat Detection

Don't let insider threats sabotage your business.

Futurism

Did you know?

More than 70% of enterprise breaches reported involved privileged accounts abuse.

Your own employees/users can put your organizational security at risk! Beyond unintentional damages resulting from lack of cybersecurity hygiene and awareness, insider attacks from former or disgruntled employees or rogue employees, who still have access to your network/ system can cause irreparable damage.

Futurism's **insider threat security services** will help you identify those weak spots or endpoints in your organization. Our **insider threat management** offerings are aimed to prevent your organization from malicious attacks originating from within the organization. warehouse or port terminal. Long story short, it simplifies the work of personnel and reduces time costs.

Insider Threat Security Services

Get the best-of-breed insider threat security services to safeguard your business from a wide range of internal threats.

Privileged User Monitoring

Futurism offers best-in-class threat management and detection services to prevent your organization from an array of hidden internal threats lurking under the network.

- Preset notifications and alerts for hijacked accounts and DoS attacks
- Behavioral insights
- Monitor privileged access to confidential business data
- Implement enterprise-wide data loss prevention strategy
- Detect unauthorized privilege access
- Enforce stronger privilege management and access control

• Trusted Host and Entity Compromise

Identify and stop attacks originating outside of your organization. Futurism's insider threat solutions equip your organization with the right set of resources and tools to protect against insider attacks.

- Check risk score of entity (e.g. disgruntled/ex-employee) using historical behavior data and ML algorithms
- Track and monitor network activity (Abnormal resource access, lateral movement, malware activity, suspicious file downloads, browser exploits, etc.)
- Monitor remote access activity (identity/credential theft, password sharing, etc.)
- Identity (account takeover, credential violations, privilege, etc.)
- DNS (Exfiltration, Tunneling)
- File integrity monitoring

• Abnormal Authentication Behavior

Our **insider threat solutions** will assist to detect and neutralize serious malicious attacks before they turn lethal.

- Real-time notifications for brute force attacks, misconfigured/ unauthorized apps, password guessing, etc.
- Custom rules to identify unusual network activity
- Alerts for:
  - Multiple password attempts
  - Unauthorized access/apps
  - Credentials/VPN sharing
  - Actions at unusual times
  - Same user name in multiple locations

Since the people/employees inside your organization are most aware of your sensitive business data, **insider threat solutions** undeniably become a need of the hour to keep these insider attacks at bay.

Get in touch with one of our **insider threat management** experts now.

+1 512-422-4868

www.futurismtechnologies.com