cowbell

Resiliency Services

Identity Threat Detection

(CRS) Identity Threat Detection continuously monitors and secures user identities across critical cloud platforms.

(CRS) Identity Threat Detection provides continuous monitoring and immediate detection of suspicious user behavior across your essential SaaS applications, including Microsoft 365, Google Workspace, Salesforce, and email tenants. Utilizing cutting-edge machine learning algorithms, (CRS) Identity Threat Detection identifies anomalies in user actions, file sharing, downloads, and ruleset changes that could indicate potential breaches all while being monitored by our 24/7/365 Security Operations Center.

(CRS) Identity Threat Detection Responds To:

- Business Email Compromise
- User Account Takeover
- MFA Bypass
- Wire Transfer Fraud

User behaviors are captured in application logs which are then monitored in real-time by SOC engineers and analysts and delivered as monthly reports.

To get started, visit **cowbell.ai** or email **crs@cowbell.ai**.

Features & Benefits

With our 24/7/365 Security Operations Center (SOC) vigilantly monitoring your environment, any detected irregularities trigger instant alerts. This allows our expert team to respond promptly and manage the situation to safeguard your environment.

(CRS) Identity Threat Detection ensures minimal disruption to your business operations while delivering the highest level of security and peace of mind. Trust (CRS) Identity Threat Detection, to provide unparalleled visibility into user behavior and robust protection for your organization.

With our state-of-the-art technology and dedicated SOC team, you can focus on running your business, knowing that your environment is continuously monitored and secure.

cowbell®

Resiliency Services

The sound approach to resilience

Learn more at cowbell.ai

CRS0002 0326