



Powered by



# Managed Detection and Response

Cowbell's engineers and analysts within our 24/7/365 Security Operations Center (SOC) respond to active threats by continuously monitoring your environment.





# Managed Detection and Response

Protect your business and clients with a comprehensive, 24/7/365 managed detection and response (MDR) service. Our US-based Security Operations Center (SOC) is staffed with experienced engineers and analysts who provide continuous threat hunting and real-time response to cyber threats.

## SOC-as-a-Service

With 70% of cyber attacks stemming from improperly managed security events, our SOC ensures your organization stays ahead of emerging threats. Through continuous monitoring and embedded threat intelligence we identify potential risks early and deploy response protocols swiftly. Our team utilizes different security tools in tandem with our human element in the Security Operations Center to develop a well-rounded security response.

### **IDENTIFY: Detect Threats Now**

Achieve access to an advanced platform that collects, parses, indexes, and analyzes technical data across an IT environment. By combining user, network, endpoint, and cloud behavior within one data lake, Identify provides actionable insights and advanced analytics.

### **NEUTRALIZE: Eliminate Threats Now**

Neutralize provides exceptional defense against the most advanced attacks against endpoints within an environment. With pre-execution blocking techniques and advanced XDR visibility, Neutralize immediately prevents sophisticated malware, including ransomware.

### **COUNTER: Outmaneuver Your Adversary**

Gain real-time response capabilities against active threats in your environment. From isolating endpoints to securely collecting forensic artifacts or executing response scripts, Counter enables quick remediation of malicious activity.

## Security Operations Center

SpearTip's SOC not only detects and responds to threats in real-time but also provides 24/7 SaaS Identity Monitoring, IdentityAI, for your business applications such as Microsoft Office 365 and Google Workspace to mitigate threats such as business email compromise and wire fraud. Our engineers and analysts work around the clock to mitigate risks, manage the abundance of alerts, and communicate findings to your organization, enabling your business to stay secure while you focus on core operations.

## IdentityAI<sup>SM</sup>

IdentityAI, offered as part of Cowbell MDR, 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, IdentityAI detects anomalies in user actions, file sharing, downloads, and ruleset changes that could indicate potential breaches. All detected activity is continuously monitored by our 24/7/365 Security Operations Center, ensuring rapid response and protection.

To get started, visit [cowbell.ai](https://www.cowbell.ai) or email [crs@cowbell.ai](mailto:crs@cowbell.ai).





This is intended as a general description of certain types of managed security services, including incident response, continuous security monitoring, and advisory services available to qualified customers through SpearTip, LLC, as part of Zurich Resilience Solutions, which is part of the Commercial Insurance Business of Zurich Insurance Group. SpearTip, LLC does not guarantee any particular outcome. The opinions expressed herein are those of SpearTip, LLC as of the date of the release and are subject to change without notice. This document has been produced solely for informational purposes. All information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any of its affiliated companies (collectively, Zurich Insurance Group) as to their accuracy or completeness. This document is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Zurich Insurance Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this document. Nothing express or implied in this document is intended to create legal relations between the reader and any member of Zurich Insurance Group. Certain statements in this document are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by numerous unforeseeable factors. The subject matter of this document is also not tied to any specific service offering or an insurance product nor will it ensure coverage under any insurance policy. No member of Zurich Insurance Group accepts any liability for any loss arising from the use or distribution of this document. This document does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction.