Brite

Abnormal + CROWDSTRIKE

Abnormal and CrowdStrike complement one another with high-fidelity detection of sophisticated threats and faster, more effective response playbooks.

Security teams shouldn't have to stitch their solutions together. As the preferred technology integrator of choice, Brite seamlessly combines and optimizes top cybersecurity tools that actually work better together to provide a more comprehensive cybersecurity defense.

One great example is the pairing of **Abnormal** and **CrowdStrike**, who team up to solve the challenge of socially engineered business email compromise attacks. These have accounted for over $43 billion in losses since 2016 and continue to grow. With a 15 percent increase in financial losses over the past year alone, it's clear that organizations need a new, integrated solution to combat this problem.

Rapid detection and response are key, but security analysts are slowed down by the manual effort needed to integrate siloed data from various solutions. Without native connections between email and endpoint security tools, security teams bear the burden of manually correlating signals from multiple security domains..

The bidirectional integrations between Abnormal Security + CrowdStrike provide the solution.

- Protect employees against hard-to-detect, sophisticated email account takeover attacks.
- Consolidate email attacks, account takeovers and identity-based incidents into comprehensive views for faster, more effective investigations.
- Automate response actions that limit lateral movement and downstream risks by requiring multifactor authentication, signing users out of sessions, and more.
- Deploy in seconds via API integration with a few clicks.

The Brite Difference

As a proud partner of both **Abnormal** and **CrowdStrike**, Brite will help you integrate either of these solutions into your current tech stack. We'll then optimize it for you so that you're up and running in no time without any hassle.

The Abnormal + CROWDSTRIKE Advantage

- Protect your largest attack surface areas. Uncovers socially engineered email attacks, compromised endpoints, and account takeovers that traditional security solutions often fail to detect.
- Enrich security context. Breaks down data silos by correlating endpoint, identity, and email events into cross-domain detections alongside other third-party tools.
- Respond faster. Accelerates incident response with automated workflows to contain risks.

Sourcing
Integration
Optimization
Partnership & Beyond

Brite goes beyond sourcing best-in-breed cybersecurity solutions. Our in-house, US-based Security Operations Center is available to co-manage those tools, delivering 24/7 enterprise-grade protection at scale. Choose Brite as your trusted partner, not only to recommend what works better together, but to make it work seamlessly.

Brite.com 1.800.333.0498 SalesInfo@Brite.com