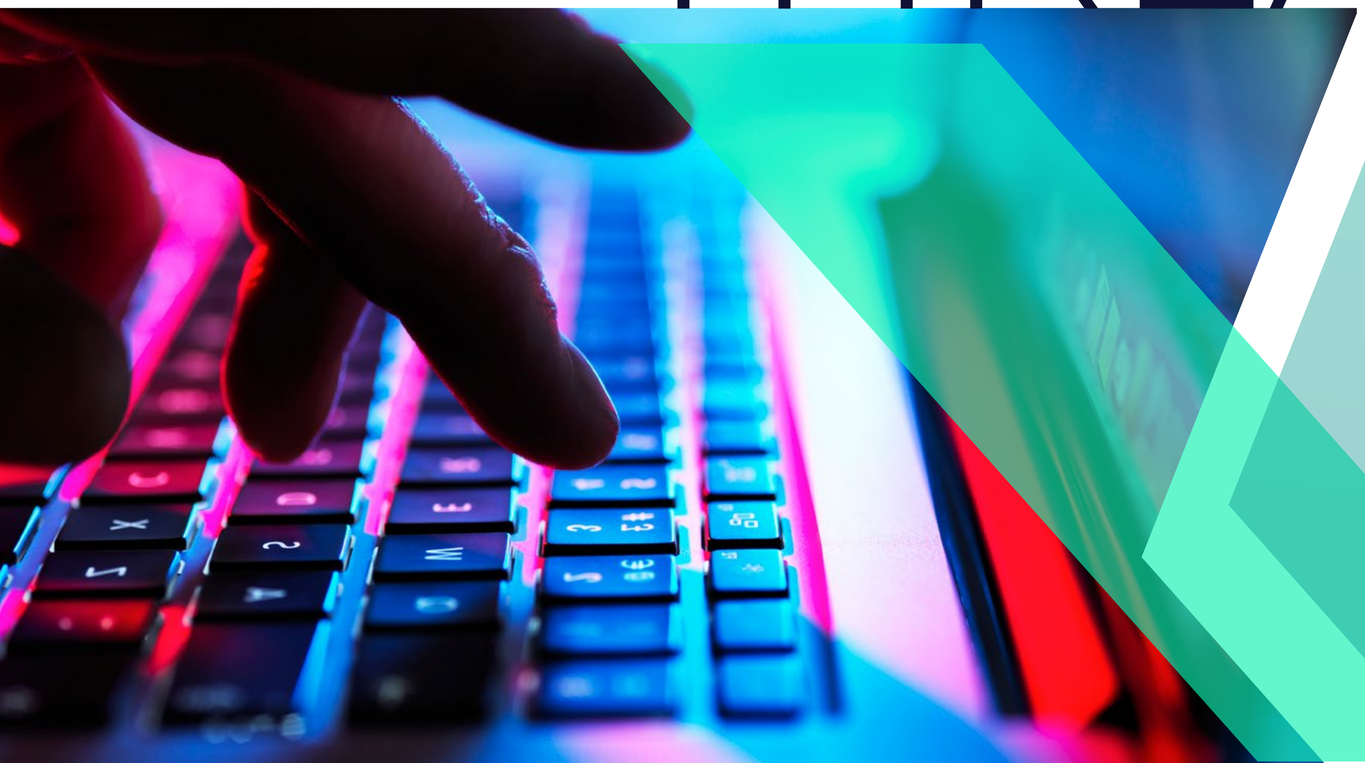
Cyber **security**

MANAGED SOC CROWDSTRIKE NEXT GEN SIEM

THREAT READY



LRQA

Your Risk Management Advantage

INTRODUCTION

A cyber-attack can disrupt your operations, damage your reputation and put sensitive data at risk. Choosing LRQA for Managed SOC services will promise a holistic, industryleading approach that not only enhances your security posture but also establishes a true partnership, acting as an extension of your own team. Our collaborative, hands-on model ensures that we don't just monitor and react – we proactively help you evolve and strengthen your defences.



ABOUT CROWDSTIKE NEXT-GEN SIEM

Speed, scale, and intelligence for the next-era of threats. The AI-native engine of the modern SOC, built to stop breaches — not just log them.

Falcon Next-Gen SIEM is purpose-built for today's threat landscape, where almost 80% of detected intrusions are malware-free and adversaries can move laterally within an environment in under 50 minutes, with the fastest breakout time recorded at 51 seconds.

80% LOWER COSTS

CrowdStrike Next Gen SIEM achieves up to 80% lower total cost of ownership than legacy SIEMs through optimised data ingestion, streamlined management, and scalable, efficient storage.

150X FASTER

CrowdStrike Next Gen SIEMs index-free architecture delivers sub-second query response and up to 150x faster search performance than legacy SIEMs, enabling rapid detection and

A powerful, cloud-native SIEM solution built on CrowdStrike Falcon platform, Falcon Next-Gen SIEM redefines security operations with exceptional visibility, real-time analytics, and seamless workflow automation. Unlike traditional SIEMs that struggle to keep pace with today's data volumes and sophisticated adversaries, Falcon consolidates detection, investigation, and response into an AI-native platform that integrates seamlessly with endpoint, identity, and cloud modules. With a single lightweight agent, it minimises system impact while delivering comprehensive protection across your IT estate.

CROWDSTRIKE



LRQA

CHARLOTTE AI, FUSION SOAR & UEBA

At At the core of the CrowdStrike Falcon platform is Charlotte AI, a generative AI capability that modernises security operations by synthesising data from multiple sources into context-rich incident insights. This enables you to make faster, more informed decisions through real-time correlation of endpoint, network, and cloud telemetry, while proactively identifying stealthy adversary behaviour and prioritising the most critical threats. This AI-driven automation significantly accelerates response and helps organisations stay ahead of attacks that bypass traditional controls such as firewalls, VPNs, and email gateways.

Falcon's native SOAR capabilities further enhance efficiency by automating workflows across the security stack, reducing detection and response times, and enforcing consistent, standardised response procedures while optimising resources through multi-source correlation.

In parallel, Falcon Next-Gen SIEM delivers advanced UEBA by analysing real-time behaviours aligned to attacker techniques rather than simple anomalies, providing immediate and actionable insights with fewer false positives through deep correlation of endpoint and third-party data, and outperforming traditional UEBA tools through its native integration within the Falcon platform.



WHAT TO EXPECT FROM OUR SERVICE

24/7/365 MONITORING, RESPONSE, CONTAINMENT

We will provide continuous monitoring, rapid response, and containment. With adversaries now achieving an average breakout time of 48 minutes and fastest breakout in just 51 seconds, speed of response is crucial to minimising impact.

PROACTIVE THREAT HUNTING

You will benefit from proactive adversary tracking through CrowdStrike's Falcon Adversary OverWatch, complemented by LRQA's own ad-hoc threat hunting. Our 24/7 hands-on-keyboard analysts proactively identify and contain threats, using offensive-informed techniques to

NEXT-GEN SIEM

The CrowdStrike NG-SIEM will ingest and correlate telemetry from Falcon (covering endpoints, identity, and cloud) and third-party systems like firewalls and network devices where agents aren't deployed. This will deliver real-time threat detection, with 150x faster search speeds and up to 80% cost

CREST-ACCREDITED SOC

LRQA stands apart as the first organisation in the world to achieve all CREST accreditations, including being the first globally to be accredited for SOC services. This distinction demonstrates our commitment to delivering trusted, independently validated security services of the highest

SCALABILITY & SIMPLICITY

Expert guidance to help maintain critical operations while recovery measures are implemented. Built in the cloud, the CrowdStrike Falcon platform will scale effortlessly to handle high data volumes – supporting up to 1PB/day ingestion with sub-second response times – while

OFFENSIVE-LED APPROACH

We draw from deep expertise in real-world adversary tactics, techniques, and procedures (TTPs) to design detection strategies that stay ahead of evolving threats. By embedding offensive knowledge and adversary tradecraft into our processes, we ensure that our threat detection

ABOUT LRQA

LRQA is a leading global risk management partner.

Through our connected risk management solutions, we help you navigate an evolving global landscape to keep you one step ahead.

From certification and cybersecurity, to safety, sustainability and supply chain resilience, we work with you to identify risks across your business. We then create smart, scalable solutions, tailored to help you prepare, prevent and protect against risk.

Through relentless client focus, backed by decades of sector-specific expertise, data-driven insight and on-the-ground specialists across assurance, certification, inspection, advisory and training, we support over 61,000 organisations in more than 150 countries.

LRQA – Your risk management advantage.

GET IN TOUCH

Visit **LRQA.com** for more information or email **enquiries.uk@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.

LRQA
Your Risk Management Advantage