CREST launches comprehensive white paper on Maximising SOAR in the SOC

LONDON, UNITED KINGDOM, September 11, 2024 /EINPresswire.com/ -- CREST, the global leader in cybersecurity accreditation and certification, has unveiled its latest white paper titled Maximising SOAR in the SOC. This new resource provides an in-depth exploration of Security Orchestration, Automation, and Response (SOAR) technologies, detailing how these tools can be effectively deployed within Security Operations Centres (SOCs) to significantly enhance threat detection, incident response and overall security efficiency.

The free-to-read white paper serves as a crucial guide for SOC managers, security analysts and decision-makers, equipping them with the knowledge needed to leverage SOAR to its fullest potential.

The nine-page document covers the implementation challenges, pitfalls, best practices and outcomes of implementing SOAR in the Security Operations Centre, making it an invaluable tool in any organisation's journey to increased automation and stronger SOC effectiveness.

As cyber threats continue to evolve in complexity and frequency, SOCs are under increasing pressure to manage high volumes of alerts, respond to incidents rapidly and ensure the ongoing protection of critical assets. Traditional security operations, often characterised by manual processes and siloed technologies, struggle to keep pace with the dynamic nature of today's cyber environment. This is where SOAR comes into play - integrating various security tools and automating repetitive tasks to free up analysts' time for more strategic, high-value work.

The white paper emphasises the strategic importance of adopting SOAR in SOCs to address these challenges. It outlines how SOAR can help streamline workflows, reduce response times and improve overall threat management by automating routine activities such as alert triage, data enrichment and incident reporting. By centralising these processes, SOAR not only enhances the speed and accuracy of incident response, but also reduces the operational burden on security teams.

Maximising SOAR in the SOC provides detailed guidance on implementing and optimising SOAR solutions in a security operations context.

The paper explores how SOAR platforms can integrate with existing security tools, such as SIEM (Security Information and Event Management), threat intelligence platforms and endpoint

detection systems. By creating a cohesive ecosystem, SOAR helps automate complex workflows, enabling faster, more efficient responses to security incidents.

SOAR's ability to ingest and process threat intelligence from multiple sources allows SOCs to gain a deeper understanding of the threat landscape. This intelligence-driven approach helps in prioritising threats based on their relevance and impact, ensuring security teams focus on the most critical issues.

The white paper highlights the role of playbooks in SOAR solutions - automated, predefined workflows that guide the response to specific types of incidents. Playbooks help standardise response actions, ensuring consistency and reducing the potential for human error during high-stress incidents.

One of the most pressing issues in modern SOCs is analyst burnout caused by alert fatigue and the pressure to keep up with constant threats. By automating repetitive tasks, SOAR reduces manual workload and allows analysts to focus on more strategic tasks, enhancing job satisfaction and retention.

The white paper also mentions the valuable metrics and insights into SOC performance utilising SOAR can provide. By tracking key performance indicators such as Mean Time to Respond (MTTR), organisations can continuously optimise their security operations.

CREST President Rowland Johnson, said: “The increasing sophistication of cyber threats demands a proactive and automated approach to security operations. Our white paper on Maximising SOAR in the SOC provides valuable insights for organisations looking to transform their SOC capabilities. By harnessing the power of SOAR, security teams can significantly enhance their operational efficiency, reduce response times and build a more resilient cybersecurity posture.”

The paper also addresses the challenges that organisations may face when integrating SOAR into their existing security frameworks. It offers practical advice on overcoming common barriers, such as ensuring data quality, managing integration complexities, and customising playbooks to fit the unique needs of the organisation. By providing a clear roadmap for implementation, CREST aims to guide organisations in smoothly navigating the complexities of transitioning to a SOAR-enabled SOC.

CREST’s white paper on Maximising SOAR in the SOC is an essential resource for any organisation looking to modernise its security operations and maximise the impact of its cybersecurity investments. The document serves as both an educational tool and a strategic guide, offering actionable insights that can be applied to enhance SOC performance. To access the full white paper, visit the CREST website.

About CREST

CREST is an international not-for-profit, membership body that represents the global cyber security industry. CREST has over 350 accredited member companies and certifies thousands of professionals across the globe. CREST is working with governments, regulators, academia, training partners, professional bodies and many other stakeholders to build and raise standards in the global cyber security industry. For more information contact: Allie Andrews, PRPR, crestpr@prpr.co.uk +44 (0) 7940 452710

Allie Andrews
PRPR
+44 7940 452710
email us here
