

Cyberbit increases security operations efficiency with new SOC 3D release

New version of SOC automation and orchestration platform focuses organizations on the most critical incidents, to address the “alert storm”

Austin, Texas – December 19, 2016 – [Cyberbit](#), whose cybersecurity solutions protect the world’s most sensitive systems, today announced a new version of its SOC 3D automation and orchestration platform that increases productivity and effectiveness of the SOC and substantially reduces incident response times. The new SOC 3D platform integrates with all major SIEM and security solutions, automates SOC runbooks and workflows, and prioritizes incidents according to their business impact. SOC 3D increases a SOC team’s ability to manage and respond to the most critical threats facing the business and eliminate fatigue from the storm of excessive alerts.

According to the Ponemon Institute’s 2016 Cost of Data Breach Study, organizations recognize that the longer it takes to detect and contain a data breach, the more costly it becomes to resolve. SOC 3D reduces the time to identify and respond to these advanced threats saving companies time and money. SOC 3D boosts the effectiveness of the enterprise SOC by maximizing existing investments and staff. The platform simplifies, automates and continuously optimizes response workflows, accelerates decision making, and prioritizes critical incidents via a single management console.

Cyberbit’s experience in protecting high-risk organizations, as well as its background in creating large scale command and control systems, allows it to understand the challenges involved in managing a complex security operation and to assist organizations in responding more effectively to incidents.

Adi Dar, CEO of Cyberbit, said, “The cost of a breach will soar the longer a company is exposed, so companies need a single, automated system like SOC 3D to mitigate these costs, reduce response times, and address the ‘alert storm.’ In a world of increasingly complicated and frequent threats, Cyberbit’s SOC 3D empowers analysts with a platform that enables them to focus on what they should do, rather than on how to do it. The platform also provides less-experienced analysts with the ability to respond based on proven IR tactics and techniques.”

Cyberbit's SOC 3D platform includes the following:

- **Business impact prioritization** – Prioritizes incidents which pose the highest business risk, so SOC teams can respond to them first.
- **Dynamic workflow** – Enforces the organizational best practices for incident response while updating the workflows dynamically as the incident evolves.
- **Response automation** – Automates and executes incident response measures as defined by the security operations team.
- **Automatic data enrichment** – Adds historical context and threat intelligence to incidents, enabling analysts to respond more effectively.
- **Corporate-wide breach management** – Extends breach management and control beyond the SOC to keep finance, operations, HR and the executive stakeholders informed.
- **Ad-hoc reports** – Converges and visualizes raw data from multiple security tools, such as SIEMs, IDSs, IPSs, threat intelligence feeds and firewalls.
- **Unique insights** – SOC 3D provides insights within a clear and easy to operate UI in order to minimize the time-to-insight and accelerate the investigation process.

The new SOC 3D features will be available for enterprises and MSSPs in Q1 2017. For pricing and more details, please contact sales@cyberbit.net.

Additional resources:

- Can incident response live without SOC automation? [Read our blog](#).
- Follow Cyberbit on [LinkedIn](#), [Facebook](#) or Twitter via [@CYBERBITHQ](#).
- Visit our product page to learn more about [SOC 3D](#).
- Contact us to [schedule a demo](#).

About Cyberbit

Created to protect the most high-risk organizations in the world, Cyberbit secures enterprises and critical infrastructure against advanced cyberthreats. The company's battle-hardened cybersecurity solutions detect, analyze and respond to the most advanced, complex and targeted threats. Cyberbit employs a formidable and diverse team from both the public and private sector, including Ph.D.s, hackers, former CISOs and SOC managers, as well as seasoned veterans of the intelligence and military communities. With offices in Texas and Israel, Cyberbit is a subsidiary of Elbit Systems Ltd. (NASDAQ and TASE: ESLT) and has more than 500 employees in the United States, Europe and Asia. To learn more about how Cyberbit maximizes protection against today's signature-less threats, visit <https://www.cyberbit.net>.

Contacts:

Justine Boucher, Metis Communications

Tel: +1 617-236-0500

E-Mail: cyberbit@metiscomm.com

Dalia Rosen, VP, Head of Corporate Communications

Tel: 972-4-831-6784

Fax: 972-4-831-5420

E-mail: dalia.rosen@elbitsystems.com