



CYBERBIT
PROTECTING A NEW DIMENSION

CASE STUDY

BANK LEUMI PROVIDES QUICK & EFFECTIVE MITIGATION AND RESPONSE USING CYBERBIT SOC 3D

The bank

Bank Leumi is Israel's largest bank with US\$300 billion in assets, 2.5 million customers, 14,000 employees, more than 300 branches worldwide and tens of thousands of assets to protect.

The bank operates a 24/7 Cyber SOC, facing hundreds of security alerts per day.

The challenge

Providing a Quick, Accurate and Informed Response

Bank Leumi understood that with the growing complexity, frequency, consistency, and variety of cyber threats imposed on financial institutions, the amount of information needed to be handled to mitigate these threats is ever growing.

The mitigation processes involve a myriad of people and teams, all need to be orchestrated and managed together to supply quick response and mitigation.

Using the existing technologies - SIEM, CRM, Ticketing, Email - did not provide the automation, situational awareness, knowledge and process management capabilities required to effectively mitigate the threats and shorten the timeframes required for response.



Industry:
Financial Institutions



The Challenge:
To effectively and quickly mitigate and respond to cyber threats.



The Solution:
Cyberbit SOC 3D



Why CYBERBIT
Field-proven technology with automated decision support mechanisms, advanced reporting and situational awareness and quick response capabilities.



The Results
Better incident response times and informed response measures, updated procedures and best-practices based on post-incident analysis, out-of-the-box reporting and situational awareness capabilities, better SOC resource management.

CYBERBIT Ltd.

22 Zarhin st. P.O.B. 4410, Ra'anana 4310602, Israel
Tel: +972-9-7799843 | Fax: +972-9-7799868
www.cyberbit.com | sales@cyberbitsolutions.com



The bank also needed to integrate and collaborate its intelligence information with network-collected information, and provide reports and updates periodically to its management and internal audit teams.

The Solution

SOC 3D

After examining a few existing solutions, Bank Leumi chose to implement Cyberbit SOC 3D (SOC Management Platform).

SOC 3D seamlessly integrated to the bank's SIEM, automatically receiving alerts and relevant information.

Using Cyberbit SOC 3D, the SOC personnel can now focus on the core mission of protecting the bank's assets and responding to cyber threats, using automated procedures, workflows, and reporting mechanisms that save time and allow the team to concentrate full attention on mitigating the threat.

SOC 3D audit trail and documentation capabilities allow for post-incident investigation and drawing conclusions, leading to constant improvement of SOC procedures and incident management processes.

Using the system, the bank is now able to maintain situational awareness of its cyber domain and of the SOC operations, and easily send general and incident reports to the management and bank audit teams.

The system's automatic capabilities link similar incidents automatically, allowing the bank to leverage the knowledge and experience gained in previous incidents easily.

SOC 3D now serves as a single interface for all related cyber events and is the bank's primary cyber management and control system.

Cyberbit SOC 3D solution was chosen due to its automation capabilities, intuitive and easy-to-use UI, easy implementation, and its advanced and efficient retrieval capabilities, which exceeded the competition.

"Implementing CyberShield MnR allowed our team to be more effective decreasing response times by 30% - with out-of-the-box capabilities to interlink, document and follow up on any relevant data"



The Results

Bank Leumi identifies that the most notable result is the time saved while handling each incident - allowing the team to focus on the threat and response measures rather than be distracted by procedural tasks and documentation.

Using the reports and situational awareness modules, the SOC obtains an updated situational awareness picture, allowing its managers and decision makers to better manage their SOC resources, improve its operations and procedures to meet the ever changing needs and challenges in confronting cyber threats.

Using the reports and situational awareness modules, the SOC obtains an updated situational awareness picture, allowing its managers and decision makers to better manage their SOC resources, improve its operations and procedures to meet the ever changing needs and challenges in confronting cyber threats.

"Implementing SOC 3D allowed our team to be more effective decreasing response times by 30% - with out-of-the-box capabilities to interlink, document and follow up on any relevant data"

"For the first time since our SOC was established, we have a capability to overview, investigate and examine our procedures and processes thoroughly and without effort, and constantly improve our operations and methodologies to meet real-world challenges"

Get in touch with us to see how we can help you close the widening gap between today's sophisticated and continuous cyber threats and the limited mitigation capabilities of current monitoring and security systems

Visit www.cyberbitc.com