

THE SECURITY CHALLENGE FOR BANKS



OCTOPUS
control and command

- ◆ Regional, national and international banks manage and operate branches, offices and other facilities across large geographic areas, requiring coordination of human resources, facilities and technologies, particularly as an outcome of acquiring or merging with other banks
- ◆ Most banks manage their physical security and handle crisis management from an operational risk and security division, and their information security and cyber emergency response from their technology division, which discourages collaboration, cooperation, threat transparency, regulatory compliance and the development of unified response protocols
- ◆ With the rise of digital cyber-crime, external and internal fraud, business disruptions, weather and fire events – banks need to enhance their crisis management response, resiliency, governance and business continuity capabilities.
- ◆ Banks are also facing new national and international regulations, such as GDPR, FACTA, FinCEN, GLBA and others, each of which requires regulatory compliance strategies and tools

CASE STUDY: Leumi Bank - Security Fusion Center

COMPANY PROFILE:



- ✓ Leumi Bank Ltd.
- ✓ 250 corporate offices and branches in Israel, USA, UK, China, Romania, etc.
- ✓ 13,000 employees
- ✓ Assets: \$114 Billion
- ✓ 10 subsidiary companies

The Need: A New Bank Security Fusion Center

- Leumi has established a new 11,000 ft² Security Operations Center (SOC) and wants to manage all security technologies from one software platform
- The bank wants the SOC divided into four desks: physical security, cyber security, technical support, and internal fraud
- The desks will be able to receive both phone calls and digital notifications from all bank sites and employees and respond to incoming alarms and incidents
- The 4 desks will be able to receive both phone calls and digital notifications from all bank sites and employees and respond to incoming alarms and incidents.
- The SOC desks will be able to collaborate and share information, such as incidents, threats, reports, response procedures, and compliance protocols
- The SOC will have emergency crisis rooms, unified communications, video walls, and IP telephony

THE SOLUTION: OCTOPUS SECURITY FUSION CENTER

OCTOPUS SECURITY FUSION CENTER

INTEGRATIONS:

- ◆ A converged and unified security management platform that consolidating all the banks security systems, operations, response procedures and governance.
- ◆ An advanced integrations rule engine for correlating cyber security with physical security to detect possible insider threats.
- ◆ Advanced incident management system for call taking, SLA times, response automation and messaging.
- ◆ The control center software system manages 4 desks:
 - ◆ Physical Security
 - ◆ Cyber Security
 - ◆ Technical support
 - ◆ Internal Fraud
- ◆ Integration to 30 sub-systems such as:
 - ◆ Access control
 - ◆ Surveillance cameras
 - ◆ Video analytics
 - ◆ Fire alarm
 - ◆ Intrusion alarm
 - ◆ ATM systems
 - ◆ Vaults and safes
 - ◆ Parking systems
 - ◆ Visitor systems
 - ◆ PA
 - ◆ Radio communication
 - ◆ IP Telephony and Intercom
 - ◆ NOC SCOM system
 - ◆ Active Directory
 - ◆ MDM
 - ◆ ArcSight
 - ◆ Domain Protection
 - ◆ Cyber big data system
 - ◆ Fraud detection system
 - ◆ Mail servers
 - ◆ Sharepoint
- ◆ Octopus provided a Unified communications system for the 4 desks call taking:
 - ◆ Integration to IP PBX
 - ◆ Interface for call answering
 - ◆ Call metrics – active operators, call wait time, SLA, etc.
 - ◆ Assign work station to security role type
 - ◆ Audio recording

OCTOPUS SECURITY FUSION CENTER MODULES:

- ◆ Open architecture integrations API server.
- ◆ Unified security dashboard
- ◆ Device control module
- ◆ Smart rule engine and automation module
- ◆ Global GIS system with all the sites' floor plans
- ◆ Incident management system
- ◆ Standard operation procedure system (SOP) with work-flows
- ◆ Unified communications system and call taking
- ◆ Video management system
- ◆ Mobile application platform
- ◆ External threat and intelligence module
- ◆ Mass notifications via emails and SMS
- ◆ Human resource management for all security staff
- ◆ Site management
- ◆ Vendor management module
- ◆ Managers dashboard with SLA's for incidents, equipment, calls, etc.
- ◆ Business Intelligence (BI) system for reports, trend analysis and predictions.
- ◆ User authentication system with single sign on and onetime password

OCTOPUS SECURITY FUSION CENTER IMPLEMENTATION ROI AND BENEFITS:

- ◆ One state of the art new SOC consolidating all security response
- ◆ 30 systems were integrated and can now be managed from one system
- ◆ A unified system for response protocols, resiliency and governance
- ◆ Improved response time by 30%
- ◆ Reduced insider threat risk for security and fraud by 25%.
- ◆ Increased collaboration and threat sharing between physical security staff and cyber security staff by 50%
- ◆ Provided better insight and analysis into security patterns, trends and threats.
- ◆ Rendered 10 security systems unnecessary – saving \$200k per year
- ◆ Saved over \$250k a year in operational personnel costs
- ◆ Expected reduction in true incidents by 30% and reduction of incident related costs by \$500k annually

