CYBERBIT
PROTECTING A NEW DIMENSION

Case Study:
Cybersecurity for Smart Buildings

About the Project

Overview

Cyberbit provides cyber security solutions for smart buildings, including the Ram Compound, which is the first smart-building government facility in Israel, and considered to be one of the most innovative IT projects in the country. Smart buildings use automated processes to control the building's operational systems and increase reliability and efficiency. The Ram Compound will serve as headquarters for sensitive government ministries and as such integrates physical and cybersecurity to achieve resilience.

Most of a smart building's systems are digitally controlled and connected:

- **Operational Technology (OT) systems** including heating, ventilation and air conditioning (HVAC), lighting, power systems, elevators and fire alarms.
- **Internet of Things/connected devices (IoT)** including IP cameras, motion detectors and other surveillance systems, internal communication systems, and more.
- **Information Technology systems (IT)** including servers, laptops and workstations.

The building's OT systems reside within the IT infrastructure.

Cybersecurity Challenges

Automation and digital control provide functional and operational advantages, but also introduce new cybersecurity risks:

- **Tampering with surveillance systems –** attackers can now put surveillance systems out of service or take control of them.
- **Putting critical physical systems out of service –** attackers can access and damage elevator control systems, gates, or the entire power system.
- **Taking control of IP connected devices –** attackers may take control of connected devices such as cameras to retrieve sensitive data or to use as an internal attack vector, as in the case of the DYN attack.

These challenges join the array of existing IT security risks, such as compromising sensitive data and disruptions to business continuity.

About the Project

Project Goals

The Israeli government defined cyber resilience as a primary goal of the Smart Building project. The typical goals of a smart building project such as the Ram Compound are:

1. **Integrated security across the entire infrastructure -** the solution must secure the entire IT, OT and IoT infrastructure and devices, and should analyze data from all 3 segments to understand context rapidly in the event of a multi-vector attack, or when an attacker moves between segments.
2. **Centralized visibility –** the building's security operations are managed centrally, at a Security Operations Center (SOC). SOC managers and analysts must have 24/7 situational awareness across IT, OT and IoT segments and have access to data, dashboards and reports, which visualize security systems in a central location, and provide cross-segment information and context in the event of an IT/OT attack.
3. **Centralized incident response –** in the event of a security incident, the SOC team will manage it centrally, at the SOC. This requires access to all security tools from a single location, as well as access to data from all systems and segments in real-time, to investigate it during the incident.

Vendor Selection

Consulting firm Deloitte led the process of choosing the product vendor and system integrator for the Ram project and eventually chose Cyberbit as both system integrator and product vendor, to provide integrated security across the converged network.

Cyberbit is typically chosen for smart building project being the only vendor providing a proprietary portfolio of IT/OT/IoT products, and SOC management. The Company provides a broad set of sensors, which monitor and aggregate data from various IT/OT/IoT systems, and feed the data into a central repository. The data is then processed and analyzed to reveal attacks and continuity risks, and is available to SOC analysts for investigation.

Cyberbit's key advantages in smart building projects:

Proprietary Products – Cyberbit provides the core security portfolio based primarily on proprietary products rather than 3rd party products.

Ease of integration – smart building projects involve complex integrations with a wide range of devices and infrastructures. Cyberbit is experienced in integrating with a variety of IT/OT infrastructures from electric grids and railway control to baggage and IT systems: and was also experienced in SOC implementation, so could be trusted to perform multi-faceted smart building projects.

Unified technology for superior cyber resilience – Cyberbit's products are designed to interconnect so can provide better context about incidents that occur across multiple environments. This is particularly important in converged environments, where attacks often traverse between IT, OT and IoT.

Reduce operational complexity – reducing the number of vendors would substantially reduce the operational complexity of the project and integration overhead.

Broad portfolio – Cyberbit offers IT security, OT security, incident response tools and training products.

Experience with public sector and government projects – through its parent company Elbit Systems (NASDAQ: ESLT) Cyberbit set up large scale projects for government and public sector organizations.

Implementation

Sensors

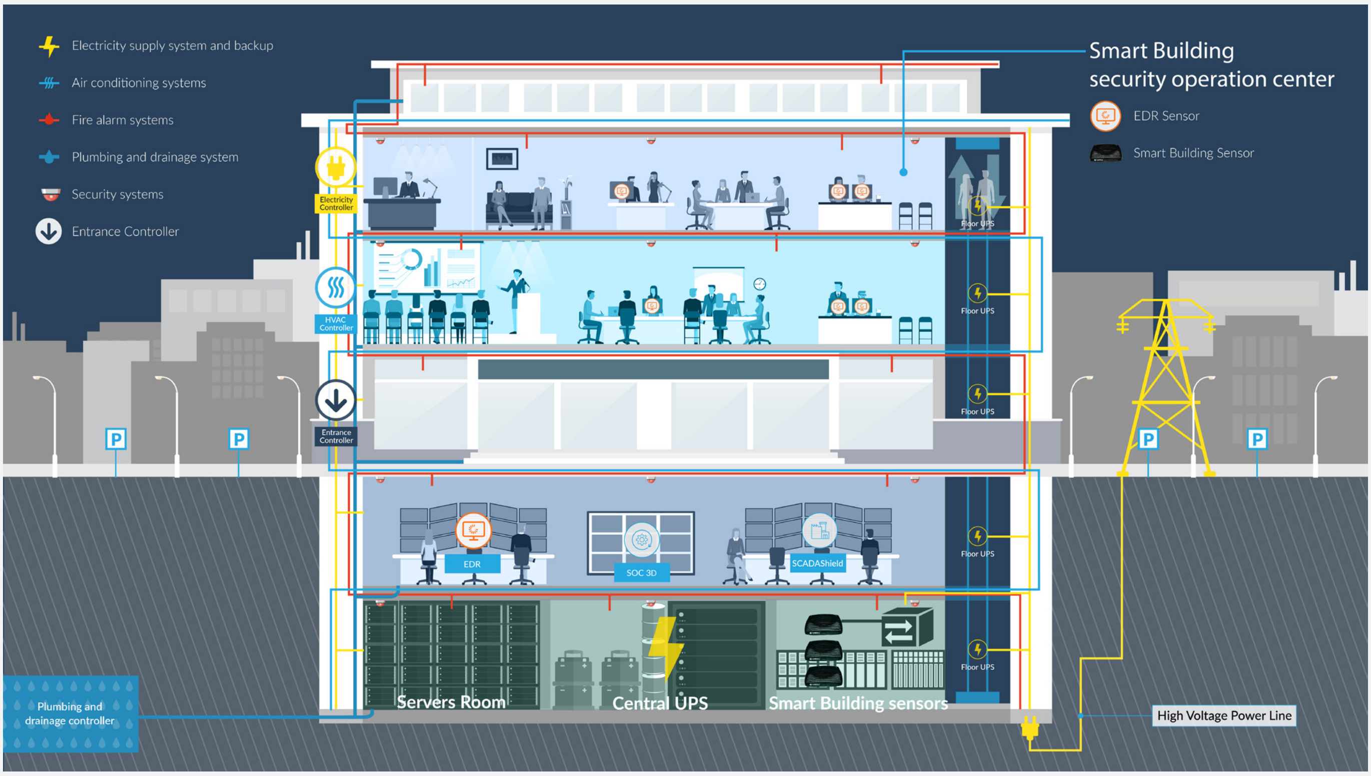
IT Sensors - Cyberbit Endpoint Detection and Response (EDR)

Cyberbit EDR is an endpoint detection and response system, which detects advanced and targeted threats that bypass conventional, signature-based security systems.

The EDR sensor is installed in IT endpoints and continuously records kernel-level data from the operating system kernel level. The data is delivered to the central big-data repository. Data is analyzed by means of behavioral analysis and machine learning algorithms, which detect and alert upon signs of malicious activity. The analysis is then presented to the SOC analyst who can continue the investigation using EDR tools, and determine the root cause of the attack.

OT and IoT Sensors - Cyberbit SCADAShield Sensors

The SCADAShield platform detects cyberattacks and continuity risks in OT networks including IT to OT attack vectors, as well as Machine to Machine (M2M) attacks. The SCADAShield Blackbox is a non-intrusive device, which monitors the entire OT network and industrial IT components such as HMI workstations, SCADA servers and historian servers. It performs passive and non-intrusive Deep Packet Inspection (DPI) of OT network transmissions, with granular analysis down to the field level, including both Ethernet and serial communications. SCADAShield provides out-of-the-box support for the majority of ICS/SCADA protocols, and continuously adds support for new and proprietary protocols. SCADAShield also creates a real-time network map providing full visibility of the OT network, and identifying risky IT/OT touchpoints.



Implementation

Architecture: Layered Approach

Cyberbit uses a layered approach when implementing a smart building project:

Layer 1: Management layer

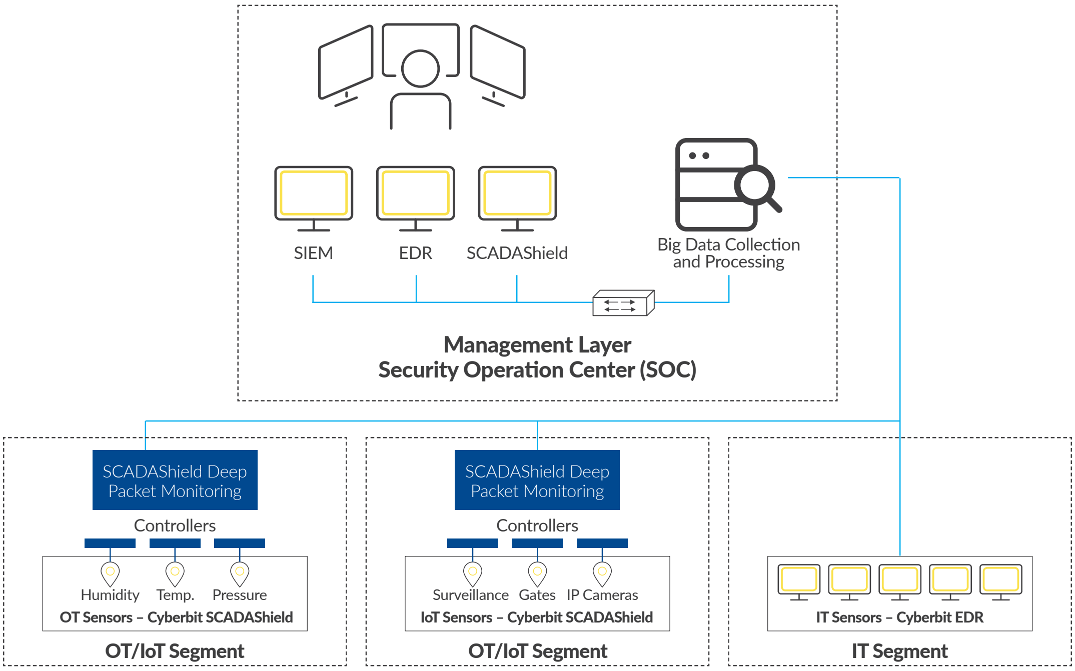
Security operations are centralized in the SOC, which collects all security data from IT, OT and IoT systems, with a SIEM solution as the ticketing system. The management layer includes big-data repositories for IT, OT and IoT based on Cyberbit's EDR and SCADAShield products. They perform behavioral analysis and machine learning to detect threats and business continuity risks, and provide investigation and forensic tools.

Layers 2-5: Structure-Monitoring Layers

OT/IoT security is implemented in 4 layers. Each one includes an instance of the SCADAShield system, with 8 SCADAShield black-boxes providing deep packet inspection across the operational network. Each environment is designed as an isolated network with a 3rd party firewall and switch integrated by Cyberbit.

Layer 6 - Security Staff Layer

This layer monitors all security equipment including IP cameras, motion detectors, and intercom systems. It includes Cyberbit EDR sensors for IT Endpoint Detection, which are installed on all security staff workstations and IT servers.



SIEM
EDR
SCADAShield
Big Data Collection and Processing
Management Layer
Security Operation Center (SOC)
SCADAShield Deep Packet Monitoring
Controllers
Humidity
Temp.
Pressure
OT Sensors – Cyberbit SCADAShield
OT/IoT Segment
SCADAShield Deep Packet Monitoring
Controllers
Surveillance
Gates
IP Cameras
IoT Sensors – Cyberbit SCADAShield
OT/IoT Segment
IT Sensors – Cyberbit EDR
IT Segment

Smart Building - High Level Architecture

CYBERBIT
PROTECTING A NEW DIMENSION

> "Attackers are always looking for the weakest link to exploit, so security must be implemented seamlessly across both the IT and OT networks. We selected Cyberbit due to the technical superiority of its portfolio and ability to provide integrated, end-to-end cyber security across the entire IT/OT stack."
>
> Lior Kalev, information security expert and head of cyber risk services at Deloitte.

ABOUT CYBERBIT™

Cyberbit's battle-hardened cybersecurity solutions detect, analyze and respond to the most advanced, complex and targeted threats. A subsidiary of defense systems provider Elbit Systems Ltd. (NASDAQ: ESLT), Cyberbit has more than 500 personnel on three continents helping organizations protect sensitive assets and maximize security operations performance. Cyberbit solutions empower enterprises to detect advanced threats in seconds, protect critical infrastructure, automate security operations center (SOC) workflows and train staff. With machine learning, big data and continuous technology advancements, Cyberbit maximizes protection against today's signature-less threats and arms organizations for tomorrow's new dimension of attack.

www.cyberbit.com

3800 N. Lamar Blvd. | Suite 200 | Austin, TX 78756
info@cyberbit.com | Tel: +1.737.717.0385

PROPRIETARY INFORMATION
The information here in is proprietary and includes trade secrets of Cyberbit Commercial Solutions Ltd. It shall not be utilized other than for the purpose for which it has been provided.

CYBERBIT
PROTECTING A NEW DIMENSION