CYBER DEFENCE FOR BUILDING MANAGEMENT SYSTEMS

SECURE OPERATIONS OF BUILDING MANAGEMENT SYSTEMS THROUGH REAL-TIME ALERTING AND THREAT RESPONSE - ALL ON A SINGLE PANE OF GLASS

Building Management and Building Automation Systems (BMS), are computer-based control systems used to manage, monitor and support critical infrastructure and the critical systems found in a variety of facilities, including corporate buildings, industrial facilities, warehouses, data centers, hospitals, airports and even vessels.

BMSs fall under the broader categories of industrial control systems, or ICS, and operational technology, or OT.

The use of BMS is now commonplace and found in any new building design or refurbishment. This design or transformation of facilities into smart buildings has seen a convergence with enterprise corporate networks and led to the optimisation of control and monitoring processes coupled with dramatic increases in productivity and improved cost efficiencies. However, with these benefits comes increased exposure to cyber risk for organisations.

BMS is now being used by attackers as a vulnerable entry point to corporate networks as well as these systems themselves being considered easy targets to cause loss of critical services and possbile safety concerns. The risks associated with these vulnerabilities grow exponentially with the adoption of **Smart Grid** and **Smart Cities** now stretching the BMS ecosystem across city sized environments.

BMS is now being used by attackers as an vulnerable entry point to corporate networks as well as these systems themselves being considered easy targets to cause loss of critical services and possbile safety concerns.

CYBERSECURITY.
EVOLVED.

SAPIEN

Sapien Cyber has created the world's most sophisticated cyber threat detection system that uses a system of systems architecture to centrally monitor and protect operations for diverse Building Management Systems

BMSs are used to supervise different systems including:

- Environmental controls - heating ventilation and air-conditioners (HVAC).
- Lighting - control of lighting and light schemes
- Energy monitoring - energy metering, automatic monitoring and targeting systems.
- Parking management.
- Utilities management.
- Critical system monitoring and alarm notification systems- fire safety, backup power, flood and leak detection.
- Elevator/escalator systems.
- Physical access control systems.
- Physical security/ surveillance (CCTV).
- Computer data suite environmental controls

The transformation of these facilities into smart buildings is leading to dramatic increases in efficiencies, such as reduced energy consumption, and assists with ensuring the safety of employees.

WITH THE BENEFITS OF BUILDING MANAGEMENT SYSTEMS COMES INCREASED RISK

This integration of previously isolated systems has also resulted in increased cyber risk for organisations in terms of the BMS being used as a pivot point for attacks on the corporate network, as well as the BMS itself being targeted to cause loss of critical services and possible safety concerns. Think of a hospital unable to treat patients or a fire caused by the shutting down of a data centres cooling system combined with fire safety systems not operating. Threats to these systems are now very real.

70% **Schneider reported a 74% increase in the number of attacks on Industrial Control Systems since 2011.**

40 million payment card details stolen from Target US in 2013. Hackers used the BMS to access the corporate network. **40m**

A cyber attack on Building Management System can have impact both financially, environmentally and can threaten human life, with disastrous outcomes if control systems fail or do not respond during an emergency event.

SAPIEN PROVIDES AN INTELLIGENT SOLUTION FOR SMARTER BUILDINGS

Sapien Cyber provides a systems of systems solution to monitor, detect and protect Building Management Systems.

OUR SYSTEM DELIVERS REAL-TIME OPERATION-WIDE MONITORING WITH DASHBOARDS TAILORED TO SUIT EXECUTIVES, IT AND OT PROFESSIONALS

HARNESS THE BENEFITS OF SMARTER BUILDINGS WHILE SAPIEN PROTECTS YOUR ENTIRE BMS ENVIRONMENT FROM ADVANCED THREATS

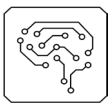
Our sophisticated solution meshes advanced cyber security technologies, advanced malware detection, Machine Learning and Artificial Intelligence, paired with cyber security and industry knowledge to rapidly detect threats and attacks occurring within your network traffic.

All traffic is monitored in real-time to identify system anomalies, investigate issues, determine the threat, and discover where they originated from and how they infiltrated the system so immediate and effective action can be taken to maintain network security.

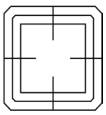
The system is in operation 24/7, proactively hunting threats and identfiying attacks with alerts generated in real-time. Our team of expert IT/OT cybersecurity analysts perform an in-depth security assessment for each alert against our clients operational priorities.

Whether you are managing a data center, government agency, medical centre, refinery or manufacturing plant, Sapien ensures that even the most sophisticated cyber attack elements are detected. Our platform also ensures that security analysts have the information and technology within a single intuitive, easy to use portal to proactively defend your organisation from evolving cyber threats.

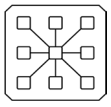
SAPIENS 'SYSTEM OF SYSTEMS' SOLUTION



MULTI-ALGORITHM MACHINE LEARNING FOR THREAT DETECTOIN

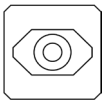


VULNERABILITY MANAGEMENT



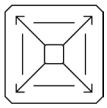
ASSET/INVENTORY DISCOVERY AND MAPPING

MULTI-SENSOR DETECTION TECHNOLOGY

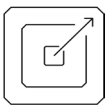


ADVANCED MALWARE DETECTION CAPABILITY

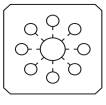
24/7/365 SECURITY OPERATIONS CENTRE



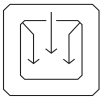
ACTIONABLE, CONTEXTUALISED THREAT INTELLIGENCE



PASSIVE DATA INGESTION



THIRD PARTY RESTFUL API INTEGRATION



SYSTEM AND SYSLOG INTEGRATION

CLIENT PORTAL

The Sapien solution provides unparalleled visiblity accross your entire enterprise - assets, alerts, analysis, responses and reports all visualised on a single screen.

INGESTION

To effectively manage and secure assets within a network it is vital that they are identified, their location determined, and their function understood.

Real time network visibility that provides both data and situational awareness for assets communicating within the network. Users can export data to conduct audits and update device details within the system to enrich the details maintained within the system.

AUTOMATED ASSET TRACKING WITH OUR 'INVENTORY DASHBOARD' KNOWING WHAT IS ON YOUR NETWORK WITH REAL-TIME VISIBILITY IS CRUCIAL FOR NETWORK SECURITY

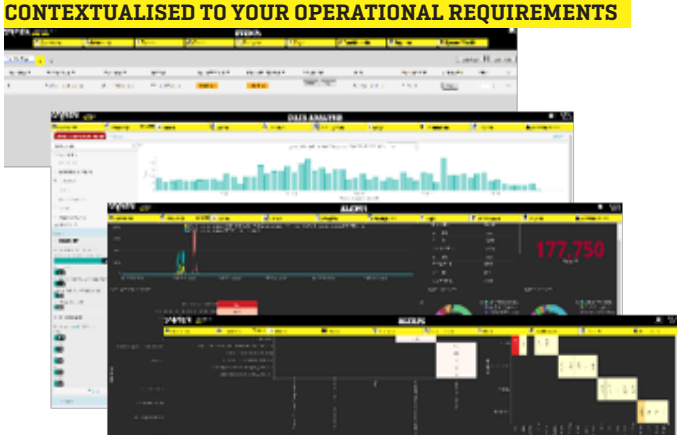
ALERTS

Security analysts are provided with the necessary information, tools and workflows to investigate and manage alerts as efficiently and effectively as possible.

Data is being ingested in real time with the system automatically generating alerts by using multiple intrusion detection sensors. This technique significantly increases the detection rate and minimises any false positives that could be generated. The result is meaningful alerts with no event fatigue.

Our technology platform simultaneously analyses network traffic with sensors that are using different detection algorithms to achieve a high detection rate and low false alarm rate. Any alerts that are detected by the sensors are automatically correlated and pre-processed to create a case that is to be investigated by security analysts. After the thorough investigation is completed all details, including contextualised repsonse recommendations, are provided to the client through the intuitive user interface.

ADVANCED REAL-TIME THREAT DETECTION WITH ALERTS CONTEXTUALISED TO YOUR OPERATIONAL REQUIREMENTS



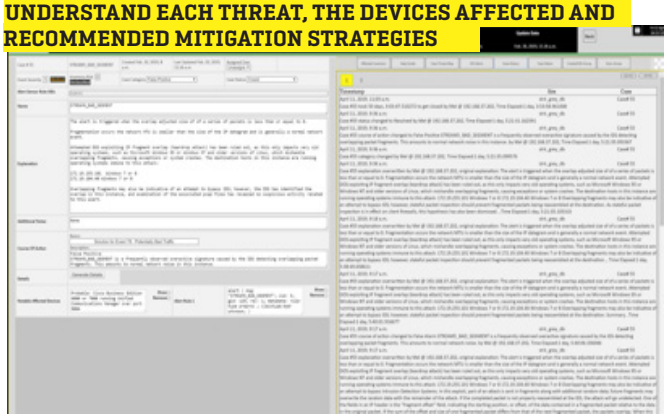
RESPONSE

Security analysts provided with the accurate information, tools and technology to perform incident response and investigate potential cyber threats, providing actionable intelligence.

The Sapien Security Operating Centre (SOC) comprises a team of cyber security and industry system experienced practitioners that provide continuous network visibility and contextualised actionable alerts to rapidly prioritise, investigate and resolve threats across your entire system.

The SOC works together with the Sapien Cyber Incident Response team to rapidly identify and address threats or incidents that may affect critical control systems.

UNDERSTAND EACH THREAT, THE DEVICES AFFECTED AND RECOMMENDED MITIGATION STRATEGIES



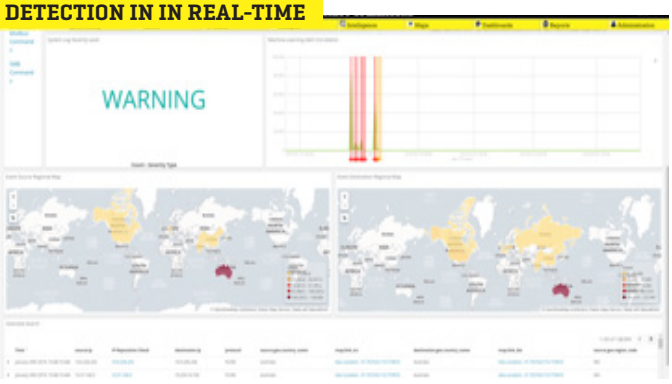
MACHINE LEARNING

Sapiens' Machine Learning uses a combination of clustering, time series decomposition, Bayesian distribution modelling and correlation analysis algorithms to identify anomalies.

In the Sapien platform, protocol specific network commands and event increases between source and destination IP addresses generate behavioural patterns for each device which participates in the given network. Using our multi-algorithm approach when deviations in values occur alerts are raised to identify suspicious behaviour on your network that may be indicative of cyber attack activity.

Our system of systems approach allows correlation of all alerts against signature alerts detected at the Sapein acquisition sensor, thereby eliminating known anomalies and prioritising what requires further investigation by Security Analysts.

MACHINE LEARNING' DASHBOARD: ADVANCED ANOMALY DETECTION IN IN REAL-TIME



DEPLOYMENT OF SAPIENS TECHNOLOGY PLATFORM WILL AUTOMATICALLY ELEVATE YOUR ORGANISATIONS CYBERSECURITY CAPABILITIES AND REDUCE YOUR ORGANISATIONS THREAT EXPOSURE.

ABOUT SAPIEN - DEVELOPED BY THE WORLD'S FOREMOST CYBER SECURITY TEAM

An Australian owned and based company, Sapien Cyber is powered by the internationally recognised cybersecurity team at Edith Cowan University,

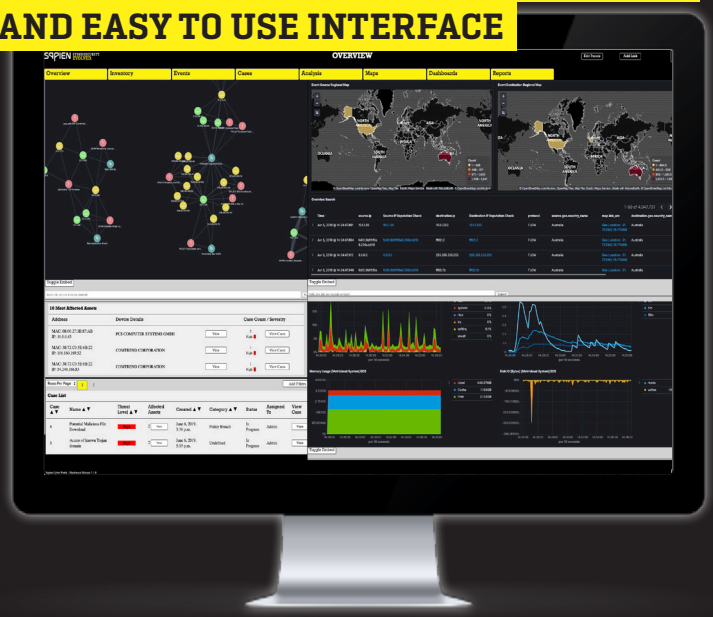
Sapien's sophisticated cyber security solution detects cyber-attacks within OT or IT networks once deployed and configured on site.

Sapien provides a 'systems of systems' approach to cyber security backed by our 24/7 SOC . Our world leading sophisticated solution meshes advanced cyber security technologies, advanced malware detection, Machine Learning and Artificial Intelligence, paired with unparalleled cyber security and industry knowledge to rapidly detect threats and attacks occurring within your network traffic.

Sapien's secure customer portal provides unprecedented visibility and awareness of your entire enterprise network through an intuitive and easy to use interface.

A solution that can be scaled and tailored to meet our clients specifc operational requirements. Sapien's technology allows clients to establish their existing security posture before developing an effective long-term strategy for asset protection, system health checks and hygiene actions.

EXCEPTIONAL NETWORK AWARENESS AND THREAT VISUALISTION PROVIDED BY OUR CUSTOMISABLE, INTUITIVE AND EASY TO USE INTERFACE



EVOLVE WITH US | sapiencyber.com.au

SAPIEN CYBERSECURITY. EVOLVED.

Sapien Cyber Corporate Headquarters
Building 6, ECU 270 Joondalup Drive
Joondalup, WA, Australia, 6027

1800 378 200
info@sapiencyber.com.au
sapiencyber.com.au