WHITE PAPER

CYBER DEFENSE FOR CRITICAL INFRASTRUCTURE

CYBERSECURITY.
EVOLVED.

SAPIEN

SAPIEN

CRITICAL INFRASTRUCTURE PROTECTION

Critical infrastructure is now under constant threat from cyber adversaries seeking to exploit vulnerable systems and networks to achieve their objectives. Industries such as banks, government utilities and energy companies are constantly upgrading their cyber defence mechanisms in order to harden their defences against the surge in the global cyber threat environment.

In order to combat this ever growing threat, industries are now expanding their use of innovative cyber defence technologies including hardware, software and cyber security services. It is clear that governments and industries are now aware that over the next decade there will be extreme pressure on existing cyber security programs, and there will be a demand for the latest in intrusion detection technologies. Sapien Cyber has developed its system to meet this growing need within industry. The flagship Sapien Platform boasts cutting edge technology, uses a polylithic architecture and enables its technology to continually evolve and adapt to malicious software and, more importantly, innovative attack strategies implemented by organisations around the world.

INVESTING IN RESPONSE RATHER THAN JUST PREVENTION

A 2018 global[1] survey found that, on average, companies are planning to increase their cyber security budget by 10% within the next 12 months. However, most executives within the industry still believe this is less than half of what is necessary. In addition, these resources are being inefficiently spent as a result of misinformation about the nature of cyber threats. Most of these organisations will invest the majority of the budget on preventing attacks from occurring and whatever is left is spent on incident response. However, it is now becoming clear to the cyber security industry that there is no guarantee to prevent a well-funded and persistent adversary from succeeding. Therefore, companies are beginning to acknowledge that there is a need to invest in mechanisms that are constantly monitoring systems 24/7 to identify vulnerabilities early and detect a sophisticated cyber-attack that may have already breached the network.

COMPANIES ARE PLANNING TO INCREASE THEIR CYBER SECURITY BUDGET BY 10% WITHIN THE NEXT 12 MONTHS.

"Cyber events are extremely dynamic. Vulnerable or Infected systems can become unstable very quickly. It is not just a matter of bringing prevention and recovering systems quickly but also continually monitoring for malicious activity within the network."

THE CHANGING THREAT ENVIRONMENT

- The frequency, scale and sophistication of cyber incidents are increasing
- The attacks are more diverse and innovative to compromise well protected assets
- The number and scale of Distributed Denial of Service (DDoS) incidents is increasing due to ease of access to attack vectors growing disproportionally to the growth of defence technologies
- Cyber criminals are now deliberately targeting specific organizations and tailoring attacks to the situation
- Foreign states are increasing their level of investment in cyber capabilities resulting in well-funded, sophisticated and indomitable attacks

[1] EY Global Technology, EY Global Information Security Survey 2018, 2018. Available from: https://www.ey.com/Publication/vwLUAssets/ey-tmt-global-information-security-survey-2018/$File/ey-tmt-global-information-security-survey-2018.pdf (accessed 7th August 2018).

SAPIEN

THE CYBER RISK THEMES WITHIN INDUSTRY

Many organisations have never performed any form of cyber risk assessment focusing specifically on their integrated and highly networked Industrial Control Systems (ICS). When companies do perform a risk assessment of their ICS, they often use their own internal resources to perform the audit. This organisational bias can potentially hurt the company as it often leads to an inaccurate security assessment.

The traditional approach by many companies in addressing their ICS vulnerabilities is to implement network segmentation or isolation. This "air-gapping" approach is common for ICS security but rarely is it put to the test in identifying any potential cyber-attack vectors that may exist. Today, air-gapping as a sole method for cyber security is considered ineffective and inadequate. However, it is still recommended when used in conjunction with other methods, such as persistent monitoring of the network. For example, if network segmentation is implemented but not monitored there is no inventory of legitimate connected assets or live network access points. This allows the installation of potentially malicious wireless access points to remain hidden from system administrators.

Companies that are performing targeted vulnerability or penetration testing on their ICS are generally conducting it less than once a month. A month proves to be a long time in the cyber security field, as vulnerabilities can be detected, investigated, exploited and then made public in a matter of hours.

Very few companies have implemented a Security Incident Event Management (SIEM) system or Security Operations Centre focused on Operations Technologies (OT) such as Industrial Control Systems, Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) or Programmable Logic Controllers (PLCs). A dedicated real-time response team is vital to preventing exploitation of new vulnerabilities, as well as for mitigation of breaches in security.

A DEDICATED REAL-TIME RESPONSE TEAM IS VITAL TO PREVENTING EXPLOITATION OF NEW VULNERABILITIES.

In addition to lack of damage mitigation practices, many companies do not employ effective ICS focused hygiene and security policies. Simply preventing employees from connecting their own hardware to a company's network is no longer enough to maintain a systems integrity. Security policies need to be comprehensive and regularly updated to effectively combat modern attack vectors.

SAPIEN CYBER

Sapien Cyber has developed a polylithic security architecture for the assessment, monitoring and threat response for Operational Technologies. The solution combines the latest threat intelligence with its real time data gathering technologies to identify, classify and provide actionable intelligence.

SAPIEN THREAT INTELLIGENCE

Sapien Cyber employs experienced and resourceful individuals who regularly evaluate and adapt to the constantly changing cyber threat environment. The Sapien Platform uses advance cyber-security technologies, machine learning and Artificial Intelligence to detect anomalies and significantly improve 'zero-day attacks' detection capability.

SAPIEN SECURITY OPERATIONS CENTRE

The Security Operations Centre provides actionable intelligence back to the customer. Our dedicated team analyses data collected and managed by the Platform, and presents it to the client in an easy to understand format.

SAPIEN

SAPIEN SECURITY PLATFORM

The Sapien Analytics System monitors network traffic in real time to provide complete visibility of inventory, vulnerabilities, threats or attacks. The Platform presents data on a client-side dashboard for a comprehendible snapshot of network security.

SAPIEN SERVICES

Access to the Sapien Portal is provided to the customer for the delivery of network status, inventory analysis, incident investigations and threat profiles.

SAPIEN PLATFORM

Sapien's Platform is an innovative threat detection and response system tailored specifically for Operational Technology. It provides its client's security teams with in depth knowledge and visualisations of their ICS landscape to help strengthen existing defences and act upon the detection of a threat or attack. The system uses polylithic software architecture that brings together their security environment and globally trusted threat information to provide the end user with actionable intelligence.

ASSET INVENTORY LISTS AND STATISTICS

The system passively identifies all assets communicating throughout the network and displays a searchable and customisable list of attributes. Constant monitoring of connected devices is integral to detecting an intrusion into the local network.

THREAT MAPS AND VISUALISATION TOOLS

Passive network discovery visualisations are automatically updated with dynamic data to show the existing network topology for devices actively communicating throughout the network. This is particularly beneficial for large and dynamic networks with integrated equipment from multiple vendors.

The cyber-threat detection and visualisation tools provided by the Sapien Platform are some of the most technically comprehensive within the ICS cyber security market today. They provide IT/OT security teams with the context they need to protect and defend against active adversaries and inherent system vulnerabilities. They provide a level of visibility and situational awareness into the industrial control system that is created by passively collecting data from every device communicating through the entire network.

THE CYBER-THREAT DETECTION AND VISUALISATION TOOLS ARE SOME OF THE MOST TECHNICALLY COMPREHENSIVE WITHIN THE ICS CYBER SECURITY MARKET TODAY.

VULNERABILITY AND THREAT DISCOVERY

Vulnerability and threat detection dashboards provide the user with the context they need to understand the extent of the risks associated with their Operational Technology.

The platform provides threat maps to indicate where a compromise has occurred which enables the user to understand how an attack may propagate throughout the network. The maps give a very intuitive visualisation for attack information that users relate to very quickly. The visualisation tool provides an indication of the location, severity and nature of the attacks.

SAPIEN

ACTIONABLE INTELLIGENCE

The Sapien Platform analytics, tools and practices enables the detection, containment, eradication and recovery from cyber-attacks on Operation Technology. It is able to detect threats that are specifically targeting ICS/SCADA networks and provide actionable intelligence to tactical defenders of the industrial network infrastructure.

The actionable intelligence is used for network security monitoring, forensics and incident response. This vulnerability assessment, intrusion response and cyber threat intelligence gathering functions with the Sapien Platform continually build upon a knowledge bank of cyber-attacks, vulnerability and threat intelligence.

CYBERSECURITY FOR OPERATIONAL TECHNOLOGY

INDUSTRIAL PLANTS /
PUBLIC INFRASTRUCTURE /
TRANSPORT SYSTEMS /
CRITICAL INFRASTRUCTURE NETWORKS /
UTILITIES /

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