



# Cyber Security

## Managed Security Service Provider for Industrial Control Systems

# Securing your Operational Systems for a fraction of your Downtime Cost.

In 2014 **Cybersecurity entered the top 10 Global risk** on the Allianz Risk Barometer (Biggest Reinsurer). **Now it's ranked as 3<sup>rd</sup> biggest risk.** More than **50% of Cyber Attacks** are conducted on **Country Critical Infrastructure** like Electricity, Water and Oil and Gas and **75% on industrial Processes.** Most of those Industrial Infrastructures were designed for Resilience but never designed with Cyber Security in mind making them a prime target.

Increasingly, traditional Information Technology components are added to the SCADA system (Supervisory Control and Data Acquisition) and PLC (Programmable Logic Controllers), which are increasingly on the Internet, making them prone to Cyber Attacks.

The average cost of downtime across industries is approximately **\$5,600 per minute.**  
 Industrial companies have higher cost of downtime in the range of **\$22'000 per minute**  
 The average reported incident length is around **90 minutes** costing at least **\$500'000 per incident**

According to the latest ICS-CERT report, the Energy and Critical manufacturing are the ones reporting the highest number of breaches of all the sectors analyzed due to weak SCADA security

## THE SITUATION HAS BECOME SERIOUS

- Cyber Attacks are causing severe Business interruptions.
- Massive physical and economical damages.
- Industrial Companies are getting increasingly rejected by Insurers
- Vulnerable and ageing plant control systems, now exposed to Internet.

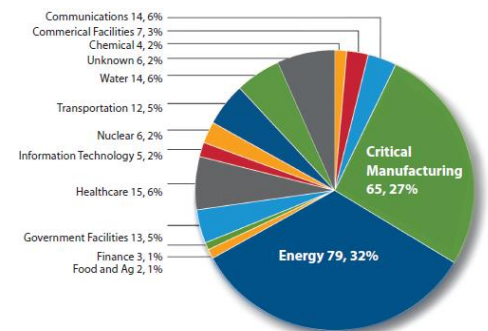


Figure 1. FY 2014 incidents reported by sector (245 total).

## HOW CAN WE HELP YOU?

The ICARE Group is a specialist Services Provider to the Power, Oil & Gas, Petrochemicals, Mining and Utilities Sectors – including Advisory, Project Development, Engineering, Construction, EPC, PMC and Procurement Services. We have deep experience of building Industrial infrastructures globally.

## SIMPLE SOLUTION FOR A COMPLEX PROBLEM

ICARE Cyber Security, a Division of the ICARE Group is a **Swiss based Company**, that has been created specifically to assist Industrial companies to **Protect** and **Prevent** themselves from Cyber Attacks. The main goal and purpose is to help Industrial customers to reduce the amount and associated risk of cyber-attacks by minimizing their vulnerability and providing their employees and managers with information, awareness, as well as technical and operational preventive means.

ICARE MSSP **Managed Security Service Provider** is a complete Cyber Security Solution for fast deployment of Monitoring, Detection, Analytics, Intelligence, Forensic, as well as Training & Drills. If you can't see what is going on in your network, you can't manage it nor prevent it.

The solution is not just **Technology** - it is also **Training and Behaviour** as well as **Emergency Response Processes** that will determine the degree to which customers can protect themselves and mitigate the damage.

## Building a SOC requires a lot of investment and expertise

### OUR APPROACH

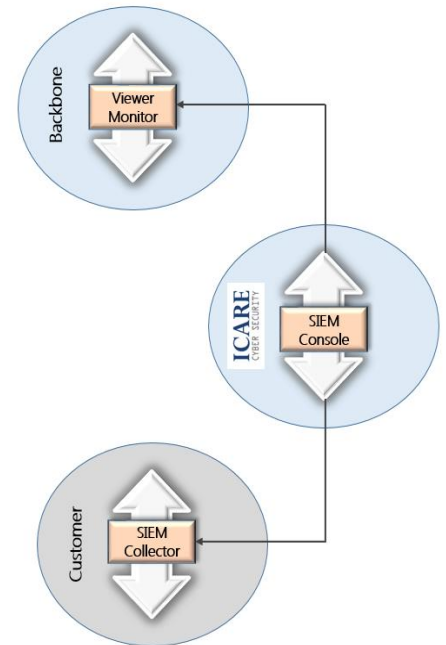
Our approach is to conduct an initial 2 week **Site Survey** to understand the exact topology of customer's SCADA networks as well as the maturity of **People, Processes & Procedures** and **Technology**.

Our **Non-Intrusive** solution connects customers through the SIEM Event Collector/Processor to our data centre and monitoring backbone.

### Services Provided: Visibility Suite

The first step in a Cyber Security Journey starts with giving you back the right visibility on your business. This **Non-Intrusive** approach allows you to quickly understand what the abnormal behaviours in your Industrial network are, detect the intrusions immediately, track and trace the sources and take the appropriate measures to minimize any damage.

Through the Service Backbone we provide the various protection services and take our customers through a transparent, step-by-step approach, to allow them to prepare their organization and protect their critical infrastructure from potentially catastrophic cyber-attacks.



### VISIBILITY SUITE OFFERING INCLUDES:

- SOC Operation, Monitoring 24 x 7 and call centre
- Monitoring for up to 100 events/sec
- Correlation of behaviour to known attack events globally
- Weekly Intelligence reports; Immediate alerts
- A Training session for 5 people
- Response team and Investigation and Forensic Lab availability
- Service Delivery Manager
- Secured Connection and Communication to the Backbone



**GET YOUR VISIBILITY BACK.**  
**YOU CAN'T MANAGE WHAT YOU CAN'T SEE**



## **SECURITY SUITE**



### **SECURITY OPERATIONS CENTRE (SOC)**

The SOC protects organizations from cyberattacks, and utilizes innovative technology that incorporates command and control, intelligence and monitoring capabilities to ensure business continuity for our customer. It's an important investment in Technology and people skills than can only be viable at large scale hence the importance of a mutualized service.



### **INTELLIGENCE AND INVESTIGATION**

For this we team up with leading partners in the area of search, discovery and intelligence solutions with the capabilities of correlating open source intelligence, Media, Social, Professional sites, Deep web, Dark web. From gathering required information to providing a full analysis report after a thorough investigation, we cover all the investigative stages while preserving all of the legal aspects



### **VENDOR SECURITY**

How secure are your vendors and do you know which ones pose the highest risk to your organization? Our diagnostic team will carry out an evaluation of your suppliers and identify those which represent the highest Cyber risks to your organization. We will work with you in establishing the right level of security measures for your existing vendors as well as screening policies for your future ones



### **AWARENESS**

The Awareness modules are classified according to different subjects and aspects of cyber security such as development, forensics, warfare, and according to different levels of personnel – senior managers, officers and operational level.



### **DRILLS AND TRAINING**

Our cyber security professionals offer a wide variety of training and courses covering all cyber and information security aspects. Our training team also performs a variety of drills and cyber-attack simulations. Each event can simulate different threats and evaluate the organization readiness at all levels – technical and procedural. The drills are pre-coordinated with the customer and can utilize various hacking tools, simulators and dedicated "malicious" code in order to safely execute a simulated cyber-attack, in a controlled environment

#### **Contact**

For further details, please don't hesitate to contact us:



[info@icare-cybersecurity.com](mailto:info@icare-cybersecurity.com)



+41 22 960 7602



[icare-cybersecurity.com](http://icare-cybersecurity.com)