SANS EMEA

SANS ICS SECURITY EUROPEAN SUMMIT

Amsterdam, Sept 21st-22nd 2014

Chaired by Michael Assante and Markus Braendle

GIAC Certification:
Global Industrial Cyber
Security Professional

Program Guide

DAY 1 - SUN 21 SEPT

9:00 - 10:00 am

Welcome

Michael Assante
Director, ICS & SCADA, SANS Institute

Markus Braendle
Group Head Of Cyber Security, ABB

The Heartbleed bug and its buddies where they come from and how to get rid of them

Rauli Kaksonen
CTO, Codenomicon

The Heartbleed bug was a simple programming mistake in OpenSSL library, which left millions of services and devices vulnerable. OpenSSL was widely considered to be a very reliable piece of code, as it is a widely used open source component and thus exposed to scrutiny of the masses. Unfortunately it took two years to find the vulnerability. Hearbleed is not by any means the only vulnerability found from respected open source security components. Some of the other recent examples have been Strongswan VPN component and GnuTLS library. The lesson to learn from Heartbleed is that we should not assume any software is perfect. We should have strategies for assuring the security of all used software components. The components should be developed with security in mind. The components should be well tested for security. We can test them ourselves or expect our suppliers to test them for us. We should consider vulnerability mitigation strategies such as sandboxes and firewalls. Finally there should be a path to fix flawed software components and to apply those fixes into deployed systems.

10:00 - 10:45 am

Lessons learnt in traditional APT incidents and their relevance for the ICS sector

Freddy Dezeure
Head of CERT-EU

The IT security community has gained plenty of experience in handling traditional APT in the area of cyber espionage. However, the same infection vectors and techniques are more and more frequently found in attacks against critical infrastructures with apparent motives that seem to extend beyond espionage. This presentation will illustrate infection vectors used in recent APT attacks and highlight their relevance for the ICS sector. It will also present APT risk mitigation strategies that can be applied in the ICS environment.

10:45 - 11:05 am - - - - - Networking Break and Vendor Expo - - - - - 10:45 - 11:05 am

11:05 - 11:50 am

The RIPE Framework

Ralph Langner
CEO, The Langner Group

Traditional cyber security frameworks such as ISA-99 or the NIST CSF contain great ideas, but little advice on the how-to of implementation. They also fall short of measurable empiric evidence of progress and security posture relative to peers (benchmarking). These are the major shortcomings addressed by RIPE, an acronym for Robust ICS Planning and Evaluation. RIPE provides detailed step-by-step guidance in eight domains that have a deterministic impact on sustainable ICS security: System procurement, plant planning, policies and SOPs, network diagrams, data flow diagrams, system inventory, workforce information database, and training. Activities in all eight domains are a prerequisite for establishing cyber security capability that is required for every asset owner, no matter how high or low the given security posture may be. The RIPE program is presently being implemented in a European nuclear power plant.

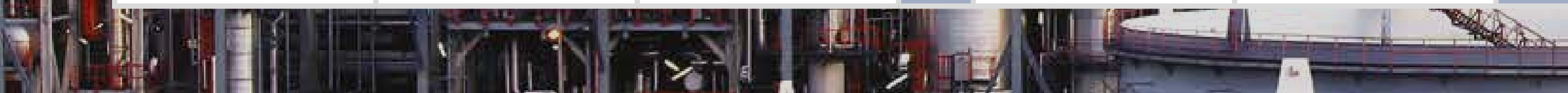
11:50 am - 12:30 pm

Smart Grid implementations: Issues and roadmap

Dr Klaus Kursawe
European Network For Cyber Security (ENCS)

The ongoing digitalisation of the electricity grid is an important step for the future-proofness of our electricity supply, but also presents a huge engineering challenge. In terms of security, the issues faced in the smart grid setting pose a culture shock both for grid providers and for IT security experts. This presentation will discuss the practical security issues in Smart Grid deployment, both on a technical and an organization level, and demonstrate where the normal IT security approach comes to its limits. We will then propose a roadmap to gradually increase the security level of the smart grid.

12:30 - 1:15 pm - - - - - Lunch Break - - - - - 12:30 - 1:15 pm



DAY 1 - SUN 21 SEPT

1:15 - 2:00 pm

Panel Discussion: What are the real risks we are facing and how should they be effectively addressed?

Rauli Kaksonen
Codenomicon
Ralph Langner
Langner Group
Doug Wylie
Rockwell Automation
Michael Assante
SANS

This session will begin with the panelists sharing what they consider to be the key risks and will then lead on to a discussion around what should be done to mitigate and tackle those risks. The session will also cover real risks vs. those risks that are prominent in the media (e.g. how bad was Heartbleed really for ICS?).

2:00 - 2:45 pm

Cyber Security, or Cyber Safety Culture? How to convert the weakest link

Slava Borilin
Critical Infrastructure Protection, Kaspersky Lab

People are the weakest link in information security. Relations between a few IT Security Officers, and thousands of "weakest links" are often far from adequate, and no investment security controls can help - as people are extremely creative in finding ways around the limitations of their understanding. We know we we need a "cyber security culture", however, there is little practical advice on how to achieve this. Industrial Automation has the advantage here, thanks to the existing Safety and Reliability Programs in place. Here we look at the 3 whales of safety culture (Zero Incident, Near Miss Reporting, Behavioral Analysis) as the role model for including cyber aspects into safety programs, and to give to cyber security that which the industry is dreaming about: C-level attention, funding, and organization-wide support.

2:45 - 3:05 pm - - - - - Networking Break and Vendor Expo - - - - - 2:45 - 3:05 pm

3:05-3:45 pm

Breaking and fixing critical infrastructure

Justin Searle
Managing Partner, UtiliSec

New ICS technologies bring greater benefits for both providers and consumers of critical infrastructure, however often these benefits come at a cost from a security perspective. Unlike the over-hyped messages we usually hear from the media, the sky is NOT falling. However, just like any other technology, the systems and devices that make up the world's critical infrastructures will have weaknesses and vulnerabilities. It is important for us to understand these vulnerabilities, how they can be attacked, and what we need to do to defend against those attacks. This presentation will explore a testing methodology that owner/operators and vendors can use to perform penetration testing on their equipment to identify and remediate vulnerabilities before they are exploited by the bad guys.

3:45-4:45 pm

Defending ICS from Cyberthreats with next-generation security

Del Rodillas
Sr. Product Marketing Manager, SCADA & Industrial Control Systems, Palo Alto Networks

This solution workshop will help provide a better understanding of:
The different kinds of cyberthreats to SCADA and Industrial Control Systems, ranging from advanced targeted attacks, protocol exploits to unintentional insider error or misappropriation of resources;
The kinds of frameworks and capabilities required to effectively address these cyberthreats and the shortcomings of legacy technologies in meeting these requirements;
Next-generation firewall technologies and how they can be used to increase situational awareness, implement IEC 62443-style segmentation and access control, and deter advanced persistent threats (APT) in control systems environments

4:45-5:30 pm

You Don't Know What You Can't See: Network Security Monitoring in ICS

Rob Caldwell
Principal Consultant, Mandiant (FireEye)

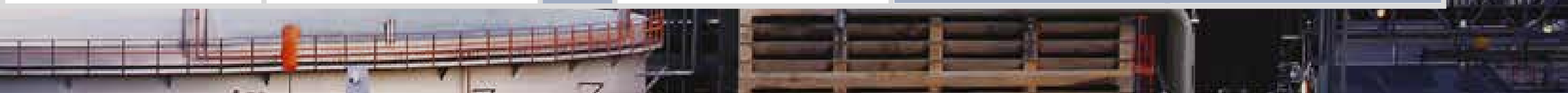
The current state of security in Industrial Control Systems is a widely publicized issue, but fixes to ICS security issues are long cycle, with some systems and devices that will never have patches available. In this environment, visibility into security threats to ICS is critical, and almost all ICS monitoring has been focused on compliance, rather than looking for indicators/evidence of compromise. The non-intrusive nature of NSM is a perfect fit for ICS, and this presentation looks at using NSM as part of an incident response strategy in ICS.

6:00 - 8:00 pm

Evening Reception sponsored by Rockwell Automation

Free drinks and buffet in a relaxed, networking environment

Rockwell Automation



DAY 2 - MON 22 SEPT

9:00 - 9:45 am

Implementing a strategic roadmap for securing critical infrastructure

Tips and techniques from over 10 years in the ICS / SCADA Security field

Jonathan Pollett

Founder, Red Tiger Security

Securing ICS, SCADA, and Operational Technology (OT) that empowers national critical infrastructure systems can appear to be a large challenge at first. These systems generally lack the security features found in business and enterprise IT environments, yet they provide a critical role to the organization as well as the economic health of the region. Over the past 10 years, Jonathan Pollet and his team at Red Tiger Security have been actively involved in setting industry standards for ICS and SCADA security, and have worked in over 250 industrial plants around the world. Through this process they have developed a strategic roadmap for securing critical infrastructure that identifies the key processes and activities into a prioritized phased methodology. This process cuts through any confusion in the industry to provide clear guidance that allows both the Operational Technology (OT) and Information Technology (IT) teams to work together towards a common goal and objective - to secure the critical systems required to maintain the availability of operations. During this educational session, Jonathan will walk through this strategic roadmap, explain why certain activities are ordered and staged into phases of work, and relate interesting stories from implementing this plan for many organizations in the Oil and Gas, Energy, and Critical Infrastructure Sectors. This high-level presentation will also set the stage for additional topics/discussion in the conference covering areas like Identifying Risks on Critical Assets, Integration of Process Control and IT Systems, Identifying Vulnerabilities in critical ICS systems, and more.

9:45 - 10:30 am

10 Steps on the road to a successful cyber security program

Markus Braendle

Group Head of Cyber Security, ABB

The complexity of cyber security is constantly increasing, requiring organizations to build cyber security programs that address the evolving challenges in a holistic, effective and sustainable way. This presentation will discuss 10 ingredients that are key factors in the success of a cyber security program and should be of the highest importance to any stakeholder.

10:30 - 10:50 am ----- Networking Break and Vendor Expo ----- 10:30 - 10:50 am

10:50 - 11:30 am

Panel Discussion: Securing the Human

Charles Hosner, KPMG
Markus Braendle, ABB
Tim Conway, SANS
Tyler Williams &
Auke Huistra
Shell

This session will begin with panelists providing short examples of where they have seen security struggle or fail because of human errors, mistakes or misconceptions and will be followed by a discussion covering the steps that are necessary to address this and "deal with the human element" on all levels of the organization from the plant floor to the board room.

11:30 am - 12:15 pm

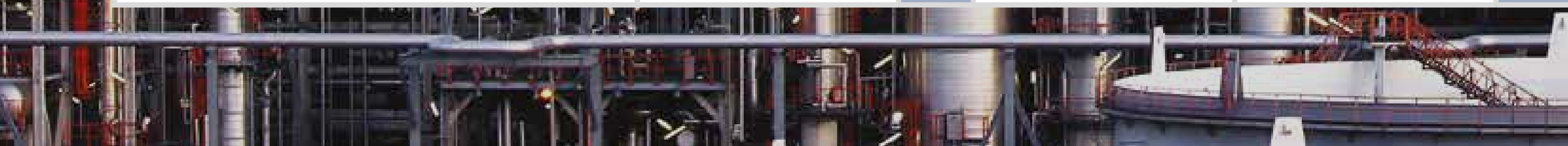
BACNet research and BotNets

Steffen Wendzel

Head of Secure Building Automation Systems, Fraunhofer FKIE

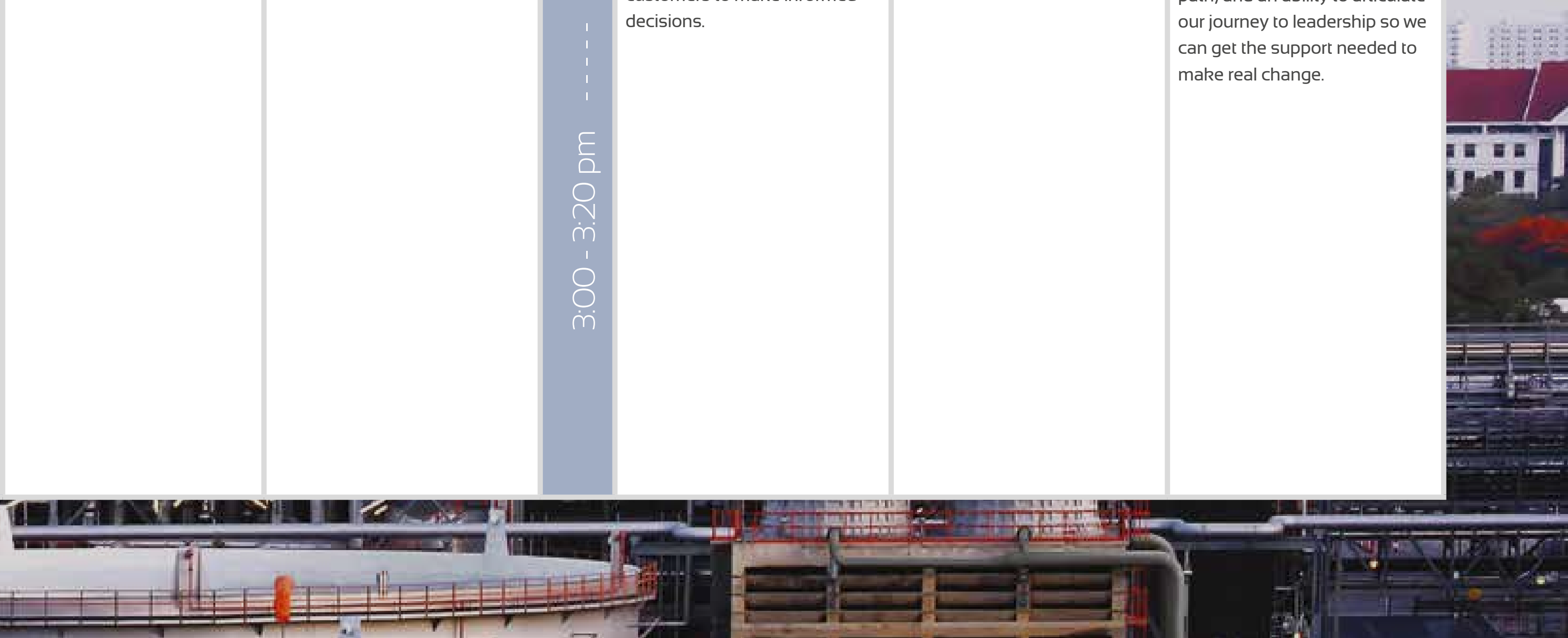
This session covers the feasibility of smart building botnets (SBB), including ways to realize such botnets as well as their possible impacts. The talk highlights the role of network steganography for future malware, especially in the context of SBB, and presents the integration of traffic normalization into building automation environments.

12:15 - 1:30 pm ----- Lunch in the Hotel Restaurant ----- 12:15 - 1:30 pm



DAY 2 - MON 22 SEPT

1:30 - 2:15 pm	2:15 - 3:00 pm	3:00 - 3:20 pm ----- Networking Break and Vendor Expo ----- 3:00 - 3:20 pm	3:20 - 4:15 pm		4:15-5:00 pm
Experiences from setting up a cyber security lab	Cyber threats towards ICS - just the tip of the iceberg		Security of SCADA Systems in Industry and Energy Management	Deep Dive on Patch Management for SCADA Systems	How to avoid the number one risk in cyber security today: A 12 step program for recovering technoholics
Robert Malmgren Senior Security Consultant, ROMAB	**Erik Johansson** Management Doctors AB		**Stefan Woronka** Siemens AG, Industry Division	**Sebastian Ranft** Siemens AG, Smart Grid Division	**Charles Hosner** Partner, KPMG
In this presentation Robert describes his experiences drawn from building a full scale SCADA / ICS security test lab using new and used equipment. He will discuss the reason why it was needed and the drivers to build the lab, the struggles encountered to get it working and plenty of some interesting stories from the installation and once the lab was operational.	Based on experience gained from security assessments of several critical ICS-systems, this presentation relates the need to maneuver your company more safely in a world where critical vulnerabilities are revealed at a much higher rate than the speed and take-up of standards and recommendations. Erik will highlight how the obvious cyber related vulnerabilities are just the tip of the iceberg when it comes to the security and robustness of ICS.		Given the evolving threats and trends in the industrial environment such as the Internet of Things a vendor has to face up to these challenges and go through a change process to adapt to them. This presentation will cover the current Industrial Security Process Improvement Project and the results that have been implemented within Siemens Industry. The key aspects are improvements in processes such as the R&D process, amendments to product functions and features and training of people. In addition a continuous monitoring and management of security vulnerabilities helps to provide valuable information that allows customers to make informed decisions.	Providing secure and reliable energy supply is the core business of electrical utilities that operate critical infrastructure. With the increased usage of information and communication technology connected to the grid, Vulnerability Monitoring and Patch Management is becoming a crucial element in operating SCADA systems. This presentation will discuss the state-of-the-art implementation of SCADA Vulnerability Monitoring and Patch Management.	Whether it's IT Security or ICS, people all want to know what the number one risk is today in cyber security. Is it my 3rd parties? Compromise of my web apps? Data theft from foreign nation states? Bumbling or malicious insiders? The real top risk is much worse and evolves from our emotional response to dealing with security issues. In this talk we'll explore that top risk, the ways we tend to react to it, and consider methods and techniques to defeat this behaviour. We will review a disciplined model that will help us break out of the spin that new security threats drive in our organizations. We'll also explore developing a purpose, a path, and an ability to articulate our journey to leadership so we can get the support needed to make real change.



EXHIBITORS

Rockwell Automation

www.rockwellautomation.com

Rockwell Automation, the world's largest company dedicated to industrial automation, makes its customers more productive and the world more sustainable. Every day we help solve automation challenges and help support the safe, secure and reliable operation of industrial control systems that are owned and operated by private companies and local, state and national governments. In the normal course of business, we supply customers around the world with industrial products, services and capabilities to automate and optimize critical processes, enhance productivity and increase the value derived from these systems. Cybersecurity for processes and manufacturing automation is integral to the Rockwell Automation industrial control system philosophy and we are committed to constantly evolving our security solutions to best meet the needs of our customers and industry alike.

Palo Alto

www.paloaltonetworks.com

Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats.

The company's next generation network security platform uniquely offers the ability to identify, control, and safely enable applications while inspecting all of your content for all threats continuously. Its end-to-end integrated and automated platform provides sophisticated, real-time, threat prevention from network to endpoint to cloud. It can detect unknown threats, share intelligence, and protect against both endpoint- and network-based attacks.

Unlike fragmented legacy products, Palo Alto Networks' security platform safely enables business operations and delivers immediate protection based on what matters most in today's dynamic computing environments: applications, users, and content.

Lockheed Martin

http://id.lockheedmartin.com

As part of Lockheed Martin, Industrial Defender products and services deliver leading solutions for cybersecurity, compliance and change management for industrial control systems (ICS). Over the last decade, we have successfully delivered a single unified platform to secure and manage heterogeneous control environments for critical infrastructure operations. With deep domain expertise built-in, Industrial Defender ASM ™ has become the de facto standard to ensure the availability and reliability of key industrial processes amid escalating cyber threats, increasing regulatory burdens and accelerating ICS management challenges. Industrial Defender products and services enable customers to reduce costs, manage risks and enhance operational excellence. Over 400 companies in 25 countries rely on Industrial Defender products and services to keep their critical infrastructure operations up and running safely and efficiently.

Iguana

www.iguanasecurity.com

The IGUANA family of solutions protects critical networks and data assets against modern cyber-attacks.

IGUANABlue provides resilient security for Industrial Control Systems, customised specifically for the requirements of ICS. Tailored directly to the risk and criticality of your plant function, IGUANA Blue balances the need for security whilst still maintaining business efficiency, providing a cost-effective 'fit and forget' data guard solution against growing cyber threats.

Based on the same architecture and security aspects of the award-winning CATAPAN range of Government Grade IP Encryption solutions, IGUANAGreen has been designed to provide commercial organisations the capability to securely send and receive sensitive information whilst harnessing the flexibility of local IP networks and protecting data from the increasing threat of cyber-attack.

Atkins

www.atkinsglobal.com\security

Atkins works at the forefront of developing security capability within the UK through our assignments in the public and private sectors. We play a key role in the defence of UK critical infrastructure assets across Energy, Water, Transport, Telecommunications, Defence and Central Government. The combination of our planning and design expertise with our holistic security approach gives us a unique view of organisational vulnerabilities, risks and mitigations.

Our teams build the appropriate physical, personnel, cyber and industrial controls into the fabric of organisations. We ensure that you can deter, detect and defend the inevitable attempts to compromise your operations. We also provide the tools necessary to create a resilient operation, respond to incidents effectively and if necessary, adapt your security posture.

ICS
410

Hands On | Five Days | Laptop Required | 30 CPE/CMU Credits | GICSP Certification

ICS/SCADA SECURITY ESSENTIALS

You will be able to...

- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, ect) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/ security of systems
- Better understand various industrial control systems and their purpose, application, function, and dependencies on network IP and industrial communications
- Work with operating systems (system administration concepts for Unix/Linux and/or Windows operating systems)
- Work with network infrastructure design (network architecture concepts, including topology, protocols, and components)
- Better understand the systems security lifecycle
- Better understand information assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation)
- Use your skills in computer network defense (detecting host and network-based intrusions via intrusion detection technologies)
- Implement incident response and handling methodologies

Who should attend?

The course is designed for the range of individuals who work in, interact with, or can affect industrial control system environments, including asset owners, vendors, integrators, and other third parties. These personnel primarily come from four domains:

- IT (includes operational technology support)
- IT security (includes operational technology
- security)
- Engineering
- Corporate, industry, and professional standards

www.sans.org/emea

Course Details

SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

The course will provide you with: (1) An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints. (2) Hands-on lab learning experiences to control system attack surfaces, methods, and tools. (3) Control system approaches to system and network defense architectures and techniques. (4) Incident-response skills in a control system environment (5) Governance models and resources for industrial cybersecurity professionals.

When examining the greatest risks and needs in critical infrastructure sectors, the course authors looked carefully at the core security principles necessary for the range of tasks involved in supporting control systems on a daily basis. While other courses are available for higher-level security practitioners who need to develop specific skills such as industrial control system penetration testing, vulnerability analysis, malware analysis, forensics, secure coding, and red team training, most of these courses do not focus on the people who operate, manage, design, implement, monitor, and integrate critical infrastructure production control systems.

With the dynamic nature of industrial control systems, many engineers do not fully understand the features and risks of many devices. In addition, IT support personnel who provide the communications paths and network defenses do not always grasp the systems operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle.

When these different groups of professionals complete this course, they will have developed an appreciation, understanding, and common language that will enable them to work together to secure their industrial control system environments. The course will help develop cyber-secure-aware engineering practices and real-time control system IT /OT support carried out by professionals who understand the physical effects of actions in the cyber world.

Take this course at a live training event...

SANS London (2014)	15 - 24 Nov
SANS München	23 Feb - 7 Mar
ICS London	27 April - May 2
SANS Bahrain	2 - 7 May
SANS London	9 - 14 Nov

Although we rarely amend the schedule, all dates/courses are subject to change. See www.sans.org/emea for up to date schedule.

*(minimum attendee numbers apply)

410 also available as:

OnSite*

OnDemand

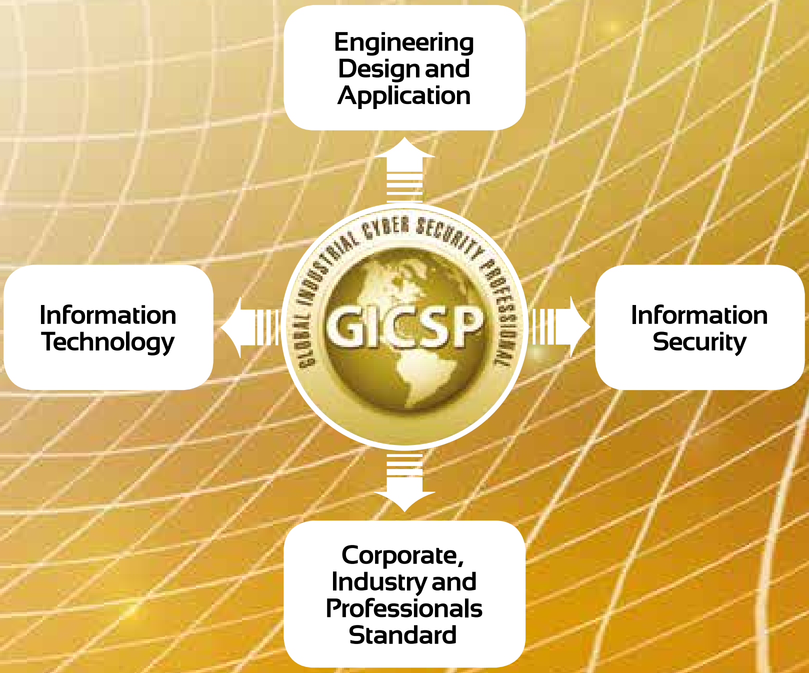
GIAC Global Industrial Cyber Security Professional (GICSP)

The GICSP exam has 115 questions and a time limit of three hours. Once achieved, the GICSP certification is valid for four years.

The GICSP certification focuses on the knowledge of securing critical infrastructure assets. The GICSP bridges together IT, engineering and cybersecurity to achieve security for industrial control systems from design through retirement.

This unique vendor-neutral, practitioner-focused industrial control system certification is a collaborative effort between GIAC and representatives from a global industry consortium involving organizations that design, deploy, operate and/or maintain industrial automation and control system infrastructure. GICSP will assess a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments.

This certification will be leveraged across industries to ensure a minimum set of knowledge and capabilities that IT, engineering, and security professionals should know if they are in a role that could impact the cybersecurity of an ICS environment.


Engineering Design and Application
Information Technology
GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL
GICSP
Information Security
Corporate, Industry and Professionals Standard

GICSP Certification Objectives

- ICS Architecture
- ICS Security Assessments
- Industrial Control Systems
- ICS Modules and Elements Hardening
- Cybersecurity Essentials for ICS Configuration/Change Management
- ICS Security Governance and Risk Management

For a complete list of GICSP certification objectives, visit **www.giac.org**

ABOUT SANS

SANS is the most trusted and by far the largest source for information security training and security certification in the world.

The SANS Institute was established in 1989 as a cooperative research and education organization. Our training programs now reach more than 200,000 security professionals around the world.

SANS provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats - the ones being actively exploited.

SANS courses are full of important and immediately useful techniques that you can put to work as soon as you return to the office. They were developed through a consensus process involving hundreds of administrators, security managers and information security professionals. Courses address security fundamentals and awareness as well as the in-depth technical aspects of the most crucial areas of IT security.

SANS-certified instructors are recognised as the best in the world. To find the best teachers for each topic, SANS runs a continuous competition for instructors. Last year more than 100 people tried out for the SANS faculty, but only five new potential instructors were selected.

SANS provides training through several delivery methods, both live & virtual: classroom- style at a conference training event, online at your own pace, guided study with a local mentor, or onsite at your workplace. SANS courses are taught in English by our world class SANS instructors, or in French or Spanish if you attend one of our excellent partner training events in France or Spain.

In addition to top-notch training, SANS offers certification through the GIAC security certification program and numerous free security resources such as newsletters, whitepapers, and webcasts.

Why SANS is the best training and educational investment

- Intensive, hands-on immersion training with the highest-quality courseware in the industry.
- Incomparable instructors and authors who are industry experts and practitioners fighting the same cyber battles as you and discovering new ways to thwart attacks.
- Training that strengthens a student's ability to achieve a GIAC certification, which is unique in the field of information security certifications because it not only tests a candidate's knowledge, but also the candidate's ability to put that knowledge into practice in the real world.

How to register for SANS training

The most popular option for taking SANS training is to attend a training event. SANS runs public training events in Europe and the Middle East (and globally) offering students the opportunity to take a SANS course across an intensive 5 or 6 days. SANS training events provide the perfect learning environment and offer the chance to network with other security professionals as well as SANS Instructors and staff. Students should register online by visiting www.sans.org/emea

Registration for OnDemand training, French and Spanish language training (under Community) and Mentor training can also be accessed via www.sans.org/emea

www.sans.org

Contact SANS directly for information regarding OnSite training or for any general enquiries:
Email: emea@sans.org • Tel: +44 20 3384 3470
Address:
SANS EMEA, PO Box 124, Swansea, SA3 9BB, UK

SANS EMEA

FUTURE SANS EMEA TRAINING EVENTS 2015

For a full list of training events, please visit www.sans.org

		AUDITS	DEVELOPER	FORENSICS							ICS/SCADA	SECURITY																		
		6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	5 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS	6 DAYS
LOCATION	DATE	AUD507	DEV522	FOR408	FOR508	FOR518	FOR559	FOR572	FOR585	FOR610	ICS410	SEC401	SEC501	SEC502	SEC503	SEC504	SEC505	SEC506	SEC511	SEC540	SEC542	SEC560	SEC561	SEC566	SEC575	SEC579	SEC617	SEC642	SEC660	SEC760
OMAN	JAN 3rd - 8TH			●																		●								
BRUSSELS	JAN 26TH - 31ST				●											●			●									●		
DUBAI	JAN 31ST - FEB 5TH									●						●					●									
MUNICH	FEB 23RD - MAR 7TH	●						●			●	●										●							●	
ABU DHABI	MAR 14TH - 19TH				●							●																		
OSLO	MAR 23RD - 28TH											●													●					
COPENHAGEN	MAR 23RD - 28TH			●												●														
STOCKHOLM	MAR 23RD - 28TH				●																	●								
ICS LONDON	APR 27TH - MAY 2ND										●																			
BAHRAIN	MAY 2ND - 7TH										●	●																		
SECURE EUROPE	MAY 11TH - 23RD				●				●			●			●	●			●						●	●				
DUBLIN	JUN 8TH - 13TH			●								●																		
BERLIN	JUN 22ND - 27TH																				●	●					●	●	●	
LONDON IN THE SUMMER	JUL 13TH - 18TH	●	●		●			●		●		●				●		●		●			●		●					
DFIR PRAGUE	OCT 5TH - 17TH			●	●	●	●	●	●	●						●														
TALLINN	SEP 21ST - 26TH											●										●							●	
GULF REGION	OCT 24TH - NOV 5TH		●							●					●							●		●	●					
LONDON	NOV 9TH - 14TH										●	●	●	●	●	●	●		●		●	●			●	●				●

Dates, Locations and Courses offered subject to change