



Swiss Cyber Storm 2018 International IT Security Conference

30th October 2018
Kursaal Bern, Switzerland

Gold Sponsor



Partner



Schweizer Armee / Armee Suisse /
Esercito Svizzero
Führungsunterstützungsbasis /
Base d'aide au commandement /
Base d'aiuto alla condotta





WELCOME TO SWISS CYBER STORM 2018



Prof. Dr. Bernhard Tellenbach
President, Swiss Cyber Storm

At the dawn of personal computers, Steve Wozniak said* "Never trust a computer you can't throw out a window." Today, most computers can be thrown out a window. But I fear this did not solve the trust problem. The many serious flaws in hard- and software and the large number of attacks that exploited the (often undeserved) trust of people in technology, let our confidence crumble. Should we use today's hardware and software to build e-voting systems? Should we use it to build pace makers that can be remote-controlled?

I haven't decided yet. But trust me, Swiss Cyber Storm 2018 will shed some light on these and other trust and IT security related questions. I am sure the talks will provide enough material for interesting conversations during the breaks and the flying dinner and bar in the evening. I hope you find the program interesting and that you enjoy our new location, the Kursaal Bern.

* actually, this is only partly true, but he is ok with being attributed with the quote.

INRODUCTION TO SWISS CYBER STORM 2018

Welcome to Swiss Cyber Storm 2018. We have created a tasty menu for you and we are very happy to see you at Kursaal Bern. We have grouped most of our talks around the focus theme "Trust". Let me quote a few highlights!

Our keynote speaker is the famous Canadian author and privacy activist Cory Doctorow who will use his rich background to tell us what he thinks of Trust as the base for all things computing. Authentication is the moment where you build up trust in a session. Lilly Ryan looks at this process through facial recognition and Grzegorz Milka explains how Google is rebuilding said trust once an account has been hijacked.

You think you can trust the authenticity of messages in your secure messenger on your smart phone. Jérémy Matos will explain how this is an attack vector for spear phishing attacks. But you should be able to trust the data of your sensors in your network. Mark Burgess shows how this trust starts to blur the more sensors you deploy. It's a quality problem like with software. Take eHealth for example: here, the confidence in the developers is primordial to people like our speaker Marie Moe. But as hard as it is to trust developers sometimes, there is no way around if you want your project to be successful. Meet Lydie Nogol, who deals with this problem as CISO of the biggest mobile phone carrier in Cameroon.

People trust paper ballots in Switzerland for voting. Now the people at the Federal Chancellery like our speaker Oliver Spycher want us to trust E-Voting in the same way. Most of you will probably say that trustworthy hardware would be a precondition. This is where Robert Rogenmoser comes in: He produces hardware with a trusted local supply chain.

Outside the trust focus theme, Ivan Ristić will tell us about his experience with SSL Labs. Moonbeam Park looks at North Korean cyber campaigns and Oliver Simonnet tells us what he learnt from the various successful attacks on the SWIFT network.

We are hosting the Swiss Hacking Challenge Finals in parallel to the conference again. You should stroll over to watch the finalists compete throughout the day. Another good use of the breaks is to hang out in our networking lounge where we will also host a flying dinner after the conference.

Christian Folini
Programm Chair



NETWORKING LOUNGE

The talks in the three conference tracks are not the only thing that the conference has to offer. Our **Networking Lounge** is a central meeting place with couches, catering for refreshment and, **starting from 17:30**, a **flying dinner** and a **bar** that serves drinks until 22:00. It aims to offer the perfect place to meet, discuss, experiment and socialize. Furthermore, the Networking Lounge features a Raffle and the Mini-CTF where you can **win cool prizes**.

Raffle

Visit the booths of our sponsors and do not forget to ask for a stamp for your raffle ticket. Throw your ticket in the raffle box and you might win one of the many prizes with a value between 50 and 500 CHF.

Mini-CTF (not just for techies!)

You like winning cool prizes? You like exercising your mind? Then you should take a few minutes to look at the riddles of our mini capture the flag game. We have puzzles for everyone - tell us whether you are a techie or not and we point you to the right task(s).

Co-LOCATION WITH SWISS CISO SUMMIT



If you are a CISO and you haven't been at a Swiss CISO summit event yet, you should make use of the unique opportunity to join the co-located summit in the afternoon with your SCS ticket. The topic is "Next

Generation Information Security Strategy: Impact, Data Governance & Implementation".

The summit features two keynotes followed by two rounds of guided discussions and knowledge-sharing in small groups. Check out page 8 in this booklet for more details.

PROGRAM

MAIN TRACK, TECH TRACK
ARENA

MANAGEMENT TRACK
SCENARIO I

SPONSORED TRACK
SCENARIO II

TIME

08:30

 **REGISTRATION**

Welcome

*Prof. Dr. Bernhard Teilenbach, President, Swiss Cyber Storm
Dr. Christian Folini, Program Chair, Swiss Cyber Storm*

Trust as a Base For All Things Security

Cory Doctorow, Author and Activist, Los Angeles

Make your cloud faster, cheaper and more secure with a fully automated cloud environment!

Franck Braunstedter, Senior Manager Cyber Defense & Cloud Security, NTT Security, Basel

10:00

 **COFFEE BREAK**

The Evolving Architecture of the Web and Its Impact on Security

Nick Sullivan, Head of Cryptography, Cloudflare, San Francisco

How I ended Up as a Producer of Trustworthy Hardware in Switzerland

Robert Rogenmoser, Founder and CEO, SecuroSys, Zurich

Internet of Babies - an IoT Security Study

Mathias Frank, Researcher and Incident Responder, SEC Consult

Anatomy of an Account Takeover - And How We Build Up Trust Again

Grzegorz Milka, Software Engineer at Google, Zurich

How Communication Can Make or Break Your Cyber Security Program

Lydie Nagol, Head of Information Security, MTN Cameroon

How companies proactively protect themselves from DNS attacks

Stefan Mardak, Senior Enterprise Security Architect, Akamai Tech.

What Does It Take to Steal \$81m

Oliver Simonet, Security Consultant at MWR InfoSecurity, Manchester

Trust in E-Voting

Oliver Spycher, Federal Chancellor, Bern

Hidden inbox rules in Microsoft Exchange... or how to permanently steal your messages

Damian Plimmatter, IT Security Analyst, Compass Security

12:20

 **LUNCH**

TIME	MAIN TRACK, TECH TRACK ARENA	MANAGEMENT TRACK SCENARIO I	SPONSORED TRACK SCENARIO II
13:20	Practical Facial Recognition or How to Disappear Completely <i>Lilly Ryan, Senior Pen Tester at Assurance, Melbourne</i>	5 months later: Is GDPR a Means to Bring Back Trust to Online Privacy <i>Nicolas Vernaz, Founder RedStone Consulting, Geneva</i>	Penetration Testing: an old practice with new objectives <i>Rick El-Darwish, Senior Cybersecurity Engineer, Kudelski Security</i>
14:00	Embracing DevOps as a Security Professional <i>Astha Singhal, Engineering Manager Application Security, Netflix, San Francisco</i>	A South Korean Perspective on North Korean Cyber Attacks <i>Moonbeom Park, Security Researcher at KRCERT/CC, Seoul</i>	How to combine machine learning with expertise of Security Analysts to enhance SOC performance <i>Urs Ruler, CEO, teirreactive AG together with Vectra</i>
14:40	Deep Learning Blindspots <i>Katharine Jarnul, Founder Karmistan, Berlin</i>	Man in the Contacts - Where Trust in Secure Messenger Leads to Spear Phishing <i>Jérémy Matos, Founder SecurInGApps, Geneva</i>	The 3 most important aspects of (non-)successful incident response <i>Tobias Ellenberger, COO Oneconsult AG, CEO Oneconsult Deutschland</i>
15:20	Trust and Microservices - The Scaling of True and False <i>Mark Burgess, Prof. Emeritus, Oslo</i>	Cybercrime Cases <i>Roger Kneepfel, Digital Forensics Analyst, Kantonspolizei Zürich</i>	Streamlining the security and privacy aspects in IT projects using threat modeling <i>Stéphane Adamiste, Senior Consultant, ELCA Informatik AG</i>
15:50	 COFFEE BREAK		
16:20	Purpose-Driven Design in Computer Security: My SSL Labs Journey <i>Ivan Ristić, Founder Hardenize, London</i>	How to Phish - How does the perfect embedded Training look like? <i>Prof. Dr. Bernhard Tellenbach, ZHAW</i>	Evolving Cyber Threats Detection and Response <i>Kris McConkey, Global Lead for Threat Intelligence and Incident Response, PwC UK</i>
17:00	A History of my Heart - How can I trust the Code inside of Me? <i>Marie Moe, Security Researcher at SINTEF, Norway</i>		
17:30	 FLYING DINNER & BAR 		

MODERATORS



Dr. Christian Folini

Christian Folini serves as Vice President of the federal public-private-partnership "Swiss Cyber Experts" and as the Program Chair of the "Swiss Cyber Storm" conference. He is the lead author of the ModSecurity Handbook and one of the few teachers on this subject. He is also a frequent speaker at national and international conferences, where he tries to use his background in the humanities to explain hardcore technical topics to varying audiences.



Mark A. Saxer

Mark A. Saxer (Politologe, lic. phil I Uni Zürich) is a partner at the public affairs agency furrerhugi. AG. He is one of the founders and the managing director of the Public Private Partnership Swiss Cyber Experts as well as of the association Swiss Police ICT (www.spik.ch).



Dr. Peter Berlich

Peter Berlich CISA, CISM, CISSP-ISSMP, MBA is a senior lecturer at Zurich University of Applied Sciences (ZHAW). He has been developing and leading global security services and security functions at a variety of service organizations and for several global customers. He has been a global Board member of Information Security Forum and (ISC)², led the Security Management group of German Informatics Society (GI) and the Swiss (ISC)² Chapter, with which he established a series of national industry conferences. He holds a doctorate in Physics from University of Freiburg. He is a member of ISACA, (ISC)² and ISSS.

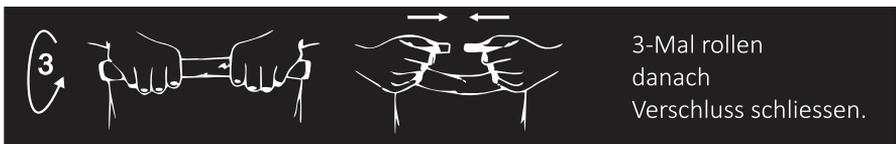
CONFERENCE BAG - IT WON'T LEAVE YOU OUT IN THE RAIN

This year's conference bag brings interesting stuff from our sponsors and it's more than a simple bag -- it's a **waterproof 15 litre drybag!**



Our conference bag won't leave you out in the rain! Or to put it even better: If you are already standing in the rain at least everything will stay dry. Whether in a light drizzle or strong showers: this soft tarpaulin bag is in its element in wet weather. Water-resistant, with welded seams and equipped with a smart roll closure: this bag is the recommended tip for adventure seekers.

Originally developed for professional equipment by divers and sailors, this bag is also ideal for river swimming, paddling, rafting and many other beautiful water activities. As it is fully floatable, clothes, provisions and sensitive equipment stay dry and clean even when your bag falls into the water.



ATTENDING THE SWISS CISO SUMMIT



Another highlight of Swiss Cyber Storm 2018 is the unique opportunity to join the co-located CISO summit in the afternoon.

The topic is "Next Generation Information Security Strategy: Impact, Data Governance & Implementation". The summit features **two keynotes** followed by **two rounds of guided discussions** and **knowledge-sharing** in small groups.

CISO Summit Keynotes

Keynote I: Balancing between continuity and disruption:

A review of effectiveness after 100 days in a new CISO position

Speaker: Marcel Zumbühl

The security strategy of a company is part of the overall company strategy and needs to be endorsed by the board. IT should balance in internal and an external claim. What do you bring to your market clients and what do you bring to your company in terms of security? A vision can be a powerful tool to express what your company stands for in terms of security, it's inherent claim in the field. The security mission is how you see yourselves as a team, what is your purpose and what are the principles guiding you. What kind of security are you as CISO – the enabler or the enforcer?

Keynote II: Social-Technical Strategy for Cyber Security and Risk

Speaker: Professor Stewart Kowalski

The need to manage security and risk in organizations is not new. However, every day newspaper headlines are filled with reports about new growing cyber security threats. Headlines of million dollar frauds and leaks of international corporate secrets appear at least once a week. Neither organization nor nation – no matter how large – seems to be able to defend themselves from such attacks. Are all secure management systems fundamentally insecure in today's cyber world and must we just learn to live with insecurity?

To answer this question, we need to review some of the fundamental principle of socio-technical systems design and risk management. In this lecture simple some socio-technical models and techniques will be introduced and examples of how these models can be used to measure and communicate cyber security risk in your organization will be illustrated.

Please contact the registration desk, if you want to join the summit.

SWISS CYBER STORM PARTNERS



Schweizer Armee / Armee Suisse /
Esercito Svizzero

Führungsunterstützungsbasis /
Base d'aide au commandement /
Base d'aiuto alla condotta

With its services in ICT and electronic operations, the Armed Forces Command Support Organisation (Führungsunterstützungsbasis, FUB) ensures that the armed forces can accomplish their missions. It guarantees the command and control of the armed forces under all conditions and works closely with the assigned conscript units to provide optimal performance. The FUB is **looking for young, talented "cyber soldiers"** who want to contribute to the security of our country through their commitment, creativity and competence.



With its partnership with Swiss Cyber Storm, the Reporting and Analysis Centre for Information Assurance MELANI expresses its support for our mission. Within MELANI, partners work together who are active in the area of security of computer systems and the Internet and protection of critical national infrastructures.



it's all about
technology

The Swiss Academy of Engineering Sciences (SATW) develops recommendations for action on technical topics that are particularly important for Switzerland as a living environment as well as a workplace and research environment.



The Swiss CISO Summit is a platform for sharing information security practices and strategies – leading to important information and Swiss market insights to address today's CISO challenges!

EUROPEAN CYBER SECURITY CHALLENGE

The growing need for IT security professionals is widely acknowledged worldwide. To help mitigate this shortage of skills, many countries launched national cyber security competitions targeting towards students, university graduates or even non-ICT professionals with a clear aim to find new and young cyber talents and to encourage young people to pursue a career in cyber security.



A PAN-EUROPEAN INITIATIVE

The European Cyber Security Challenge (ECSC) leverages on these competitions by adding a Pan-European layer. Top cyber talents from the European Union and EFTA meet to network, collaborate, and finally compete against each other during a unique event: the ECSC final.

This annual event is organised by European Union and EFTA countries and supported by the European Union Agency for Network and Information Security, (ENISA) which aims at discovering young and emerging cyber security talents.

GOAL OF THE ECSC

The goal of the ECSC is to place cybersecurity at the service of mankind, with a view to promoting a peaceful society concerned with the preservation of democratic values, freedom of thought, dignity and critical thinking.

ECSC promotes friendly relations between attending countries, officials and players. ECSC provides the necessary institutional means to promote transparency and fairness of the competition between participants and to resolve any dispute that may arise between players.

TEAMS AND RULES FOR 2018

In 2018, teams from the following 17 countries participate in the ECSC: **Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Greece, Italy, Liechtenstein, Norway, Poland, Romania, Spain, Switzerland, and United Kingdom.**

Each team consist of the top ten young cyber security talents. More specifically, team of five (or more) people aged 14-20 years and five (or less) aged 21-25 years. How these top talents are identified is left to the participating countries.

SELECTION PROCESS IN SWITZERLAND

In Switzerland, the selection process is implemented and run by Swiss Cyber Storm. The process has two-stages. In the first stage, candidates have to enter an online competition where they have to solve security related tasks from domains such as web security, mobile security, IoT security, crypto puzzles, reverse engineering and forensics.



The top ten candidates of each age category are then invited to the second stage, the Swiss final. In the second stage, the Swiss Cyber Storm jury assesses the tech and soft skills of the talents and selects 10 of them to form the Swiss team for the European Cyber Security Challenge.



Swiss team for the ECSC 2018 final in London, UK. Back row from left: Timo Kübler, Yannic Itten, Nicola Stauffer, Anthony Schneiter (team leader), Marc Bollhalder, Valentin Zahnd (coach). Front row from left: Adrian von Arx (coach), Robin Hänni, Simon Kindhauser, Jannis Kirschner, Toni Tanner, Raphael Husstein



<https://www.ecsc.eu>

<https://www.europeancybersecuritychallenge.eu>

ABOUT SWISS CYBER STORM ASSOCIATION

The Swiss Cyber Storm Association was founded in 2012 as a nonprofit organization with the purpose to promote young cyber security talents and regularly carry out cyber security events for professionals and executives.



Swiss Cyber Storm fulfils its purpose firstly with the search and support for young cyber security talents during the annual Cyber Security Challenge and the related participation in the European Cyber Security Challenge. Secondly, the association holds the annual Swiss Cyber Storm IT security conference directed internationally at cyber attacks and defence.

WLAN ACCESS

To make use of the free WLAN access, please do the following: First, connect to the WiFi network "Free Kursaal Allegro". Next, select the "Voucher" tab on the landing page and enter the following information:

User ID: 2304310715

Password: 0560

Now you should be connected and have access to the Internet. Please contact our staff at the registration desk if this does not work for you.



Solutions for Resilient Cyber Security

Whether you need to secure your digital transformation or you want to mature your business resilience, NTT Security provides the right combination of strategic consulting, managed security and technical consulting.

Strategy Consulting

Leveraging experienced, senior experts to help define and communicate risk and security program strategy using real-world data, proven frameworks and understanding of your industry and business.

NTT Security understands the complexity of building a security program that allows the business to achieve its objectives, while meeting the organization's risk tolerance. Our consultants will work with you to define your cyber security defense architecture and shape the transformative changes necessary to adapt to the digitalization of your business.

Managed Security Services

A substantial investment in threat intelligence, advanced analytics and security experts provide a consistent, repeatable and transparent process and platform. Our MSS platform can identify and stop advanced threats while providing insight and metrics into security posture and trends. Trained and certified engineers carry out an efficient, best practice and compliant change management process for your networking and security devices and controls. Experienced SOC threat and incident analysts use the NTT Security purpose-built, proprietary MSS platform or a third-party SIEM to collect, analyze, identify and respond to security incidents.

Technology Consulting

Technical Consulting focuses on assisting with projects and security controls tailored to your organization's context of technical infrastructure, information technology usage and protected information assets. Industry and manufacturer certified security experts understand how to apply security best practices and meet compliance objectives using your infrastructure and leveraging the investments you've made in on premise and cloud-based networking, platforms and controls. Whether it's preventing cybersecurity incidents from occurring or minimizing the impact of incidents through fast, effective incident response, you will always have the necessary skilled resources available to you.



aspectra is a leading Swiss provider of managed services for business-critical IT applications. We develop and operate specialized solutions where our customers need security, availability and performance — in Swiss high-security data centers as well as in the cloud. Whether dedicated physical servers, dedicated virtual servers, dedicated private cloud, Amazon Web Services or containers with Open Shift and Kubernetes: We adapt the infrastructure to our clients' particular needs and requirements. We offer on-premise DDoS mitigation, sophisticated WAF and IAM solutions, regular vulnerability scans, server- and host-based intrusion detection systems and reliable backup solutions. Our team serves customers from all industries personally and with dedication.

aspectra adheres to the highest international and national standards for process and data security: We are ISO 27001 and ISAE 3000 certified, PCI DSS compliant and meet the outsourcing guidelines of the Financial Market Authority FINMA.

aspectra AG | Weberstrasse 4 | 8004 Zürich | www.aspectra.ch

In collaboration with

Akamai Technologies Ltd.



SILVER SPONSOR



OFFENSIVE DEFENSE

Compass Security is a well renowned company specializing in penetration testing, incident response, digital forensics and security trainings with offices in Switzerland and Germany. Compass Security's research and community contributions regularly gain international recognition. A comprehensive attack/defense CTF system, called Hacking-Lab, is provided as infrastructure to European countries to run their cyber recruiting initiatives. Hacking-Lab is licensed to numerous universities worldwide with the aim of building cyber talents as well as encouraging students to pursue a career in cyber security.



Gain Security: Penetration Tests und Security Reviews

Through technical attacks and social engineering, we test infrastructure, systems, and applications. We report vulnerabilities, provide expertise on countermeasures and thus help companies to raise defenses.



24/7 on-site Support: Digital Forensic and Incident Response (DFIR)

Experience, expertise, and a well-maintained toolchain are available for the processing and analysis of information security incidents.



Stay Tuned: Security Lab and Awareness Training

Let us show you the latest attacks, learn about cutting edge technologies, or deepen your knowledge in our lab.



Hacking-Lab: Hands-On & Capture-the-Flag

Our online platform for ethical hacking and security challenges. A perfect fit for Capture the Flags, Universities, and employee training.



FileBox: Solution for secure file transfers

Secure and comfortable sharing and sending of files. Available as a service or as an on-premise appliance installation.



ELCA Informatik AG

ELCA is one of Switzerland's largest independent providers of IT solutions and a leader in IT business consulting, software development and maintenance, and IT systems integration.

ELCA solutions reduce complexity, shorten innovation cycles, improve business results and increase customer satisfaction. The privately held company employs over 920 experts and has offices in Lausanne, Zurich, Geneva, Berne, Paris, Madrid, Basel, Granada and Ho Chi Minh City (Offshore Development), all of which share a common process system.

www.elca.ch

SILVER SPONSOR

InfoGuard

SWISS CYBER SECURITY

InfoGuard is a leading and innovative Swiss company providing comprehensive cyber security and network solutions. Our customers benefit from our long experience in auditing, consultation, architecture and integration of leading network and security solutions as well as state-of-the-art managed and cyber defence services from our ISO 27001-certified InfoGuard Cyber Defence Center.

Security Consulting Services – Identifying and managing risks

Whether cyber security, governance, risk and compliance or cyber risk resilience – the growing challenges can only be met with a holistic cyber security strategy. The modular structure of the services offered by InfoGuard equally takes into account technologies, processes and your employees. Our long-standing experience in the field of security consulting based on ISO 27001 and NIST, penetration testing, attack simulation and awareness, together with the top-class expertise of our specialists ensure the smooth interaction of all elements.

Network & Security Solutions – Protecting and optimizing ICT infrastructures

Efficient network and security infrastructures must achieve an optimum balance of performance, security and costs. This is only possible when all of the components are perfectly aligned with one another. InfoGuard offers a complete portfolio of leading network and security solutions for conventional, highly virtualised and cloud infrastructures. To ensure this, we work with the leading manufacturers in the industry.

Cyber Defence Services – Detecting and eliminating cyber attacks

Today companies have to assume that cyber attacks not only occur, but that they also succeed. Defend against these attacks effectively requires top-class expertise and sophisticated technologies. Certified in accordance with ISO 27001, our Cyber Defence Center in Switzerland combines the latest technologies with the long-standing experience of our security experts and threat analysts.



InfoGuard is ISO/IEC 27001:2013 certified.

InfoGuard AG

Lindenstrasse 10
6340 Baar / Switzerland
www.infoguard.ch



Kudelski Security is an independent provider of tailored cybersecurity solutions to enterprises and public sector institutions, delivering workable solutions to the toughest security challenges they face.

We strive to create and deliver cybersecurity solutions that answer real problems. We help our clients in their journey to design, deploy, and manage effective cybersecurity through a combination of:

- **Advisory services**
- **Technology deployments**
- **Managed security services**
- **Custom research and development**

Our global reach and comprehensive cyber solutions focus is reinforced by key international partnerships. These include alliances with the world’s leading security technology firms as well as with experts in specialized services, so clients have access to all the tools and talent they need in order to plan, deploy, and run effective cybersecurity programs.

Kudelski Security is the cybersecurity division of the Kudelski Group (SIX:KUD.S) and has its international headquarters in Cheseaux-sur-Lausanne, Switzerland, its US headquarters are located in Phoenix, with offices in Zurich, Atlanta, Dallas and Minneapolis.

 Advisory Products and services to design, manage, measure and maintain robust enterprise security programs.	 Technology Resale, implementation, and support of market leading cybersecurity technology products.	 Managed Security Use of proprietary processes and technologies to extend client teams with remote management, monitoring and support.	 Research & Innovation Services to drive cybersecurity innovation into client organizations as well as the development engine for proprietary products.
---	---	---	--

To find out more, please visit us at www.kudelskisecurity.com

SILVER SPONSOR

Oneconsult group is your owner-managed and vendor-independent Swiss cyber security services partner with offices in Thalwil (Zurich), Bern and Munich. The group consists of the holding Oneconsult International AG and its subsidiary companies Oneconsult AG and Oneconsult Deutschland GmbH.

40+ highly qualified specialists – including certified penetration testers (OPST, OPISA, OSCP, OSCE, GXPN), digital forensics experts (GCFA, GCFE, GREM), ISO security auditors (ISO 27001 Lead Auditor, ISO 27005 Risk Manager) and IT security researchers – solve your most demanding information security challenges. Together we address your external and internal threats such as malware infections, hacker / APT attacks, digital fraud and data leakage.

Our core services are:

**Penetration Tests / Ethical Hacking / APT Tests**

Office IT, SCADA and IoT tests

**ISO 27001/2 Security Audits**

Or other standard-based compliance checks

**Incident Response & IT Forensics**

Incl. around-the-clock expert assistance (24 h x 365 days)

Most of our consultants hold a Bachelor's or Master's degree in computer science with a specialization in cyber security and receive continual training.

With the support of our own research team, Oneconsult detects dozens of zero-day vulnerabilities in standard software every year and informs the vendor, but for ethical reasons, this information is often not made publicly available.

Oneconsult is an ISECOM Partner (accredited trainer) and, based on the number of OSSTMM-compliant security audits, the leading OSSTMM security auditor in Europe. Furthermore, Oneconsult is a board member of Swiss Cyber Experts and an OWASP Corporate Member.

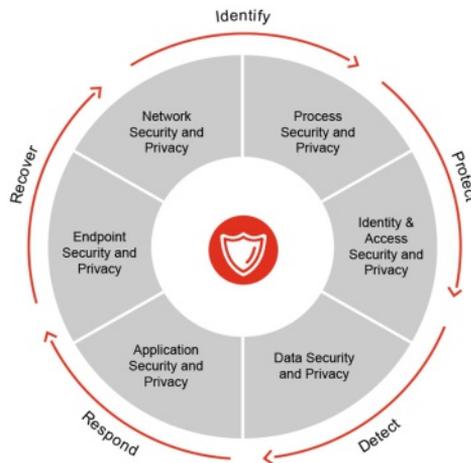
www.oneconsult.com



Making your cyber journey a successful one

Harnessing the advantages of digital technologies presents a whole set of new challenges. It's not enough to implement a good idea or develop a new product: securing the business environment and staying compliant with new security and privacy regulations and best practices are crucial for business success. Our Cybersecurity practice has teams of highly experienced people who can deliver sustainable, future-proof solutions that will help you succeed.

You need different solutions at different stages of your cybersecurity journey. We help you to address the challenges that you face at each stage intelligently and systematically so that you emerge stronger and better prepared to capitalise on opportunities as they arise.



To find out more, please visit us at www.pwc.ch/cybersecurity

SILVER SPONSOR



SEC Consult is a leading consultancy for cyber and application security. Meanwhile, we operate branches in Europe, Asia and North America. In order to efficiently and sustainably improve the security level of an organization, a holistic approach is required. Therefore, it is important to us, to not only prepare our customers for potential cyber-attacks at different levels as best as possible, but also to rapidly detect the attacker in case of a breach and to immediately set up respective measures for remediation.

As one of the few security consultancies in Europe, SEC Consult is both certified according to ISO 27001 and CREST accredited and thus fulfills highest requirements in regard to handling confidential information and conducting professional penetration tests. Furthermore, SEC Consult is member of the Open Web Application Security Project (OWASP). SEC Consult's customers include government agencies, international organizations and leading companies from various industries of the private sector as well as critical infrastructure.

SEC Consult is a specialist for the development of information security management processes and certification processes, external and internal security audits, secure software development and cyber defense.



Security Audits & Assessments

Penetration Tests, DDoS Benchmark Tests, Social Engineering



IoT Inspector

The Firmware Security Analysis Platform



SEC Defence

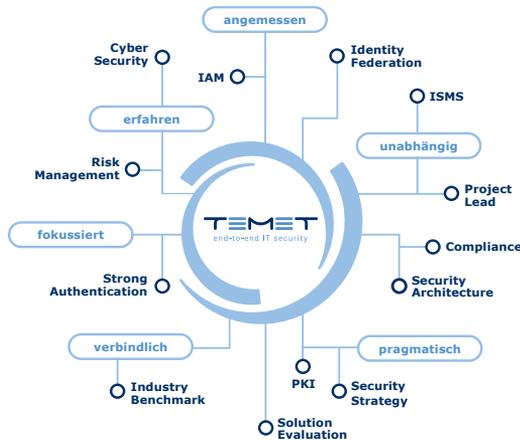
Incident Response (24/7) & IT Forensics

With the Vulnerability Lab, SEC Consult operates its own internal security research lab to gain a head-start in know-how compared to cyber criminals and state-sponsored attackers.

SEC Consult is not only expanding internationally but is also growing in Switzerland. If you are interested to join the team, visit us at our booth and convince us of your talent.



TEMET AG is a privately owned security consulting company located in Zurich, Switzerland. We provide high quality vendor and product independent consulting and project management services in all areas of security, such as Identity and Access Management (IAM), Cyber Security and Information Security Management Systems (ISMS). Further, we also perform Risk Assessments as well as Audits according to the international standards (ISO/IEC 27000 Series, COBIT, NIST CSF, PCI DSS, SWIFT CSP) and act as CISO as a service.



Unique Selling point

Our security consultants combine professional expertise and project management competence. This allows us to achieve success in even your most complex security initiatives. This combination of skills and experience is much sought after and is the foundation for the continual growth of our company.

Since the formation of TEMET AG in 2010, our customer base has continually increased to more than 80 Swiss companies in the areas of financial institutions, public authorities, critical infrastructure, insurers and health services. During this time, we successfully managed or accompanied more than 300 security projects.

SILVER SPONSOR



terreActive provides Cyber Security Solutions with main focus on Security Monitoring and Log Management.

- Swiss engineering company founded in 1996
- 50 employees including 35 engineers for 24x7 support
- Security Operations Center in Aarau, ISO certified

We design sustainable concepts for international enterprises, small e-business companies, private banks, IT service providers and industrial manufacturers. Our services help to make our customers' IT infrastructure secure and efficient.

Performance Analysis
Security Monitoring
Social Engineering
APT Assessments
Architectures
Audits

SOC
Status Reporting
Forensic Analysis
Managed Services
Security Monitoring
Incident Management
Vulnerability Management
Support + Troubleshooting
System Monitoring + Maintenance
Threat Detection + Intelligence + Hunting



Awareness Trainings
Vulnerability Scans
Penetration Tests
Second Opinions
Splunk Trainings
Concepts

VPN
WAF
SIEM
Firewall
Network Security
Log Management
Application Security
Web & E-Mail Security
Performance Management
Privileged Access Control



At **BFH**, Engineering and Information Technology, students are familiarized with the core topics and methods of software development, such as programming, software engineering, databases, operating systems and computer networks and IT security. Students develop software applications and learn to manage software projects.

Research and Development is the second pillar at BFH, Engineering and Information Technology. For companies, various options are provided for the implementation of a project. Four research institutes are of utmost interest: Institute for ICT-Based Management, Research Institute for Security in the Information Society, Institute for Human Centered Engineering, and Institute for Medical Informatics.

Various forms of cooperation exist. Please do not hesitate to contact us for further inquiries.

www.bfh.ch

ACADEMY SPONSOR



The **HSR Hochschule für Technik Rapperswil** offers bachelor, master courses and post-graduate studies in computer science ("Informatik") with a focus on Software Engineering and Human Computer Interaction Design as well as a series of post-graduate courses in Information Security ("Zertifikatskurse für Datenschutzverantwortliche").

www.hsr.ch

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE LUZERN

The Lucerne School of Information Technology is one of the six Schools of the Lucerne University of Applied Sciences and Arts. It is the regional University of Applied Sciences for the six cantons in Central Switzerland and is the biggest educational institution situated in the heart of the country. There are over 6'200 bachelor's and master's students, 9'700 students in continuing and executive education and over 500 projects in research and development.

The Lucerne School of Information Technology offers bachelor's and master's degree programs, continuing and executive education programs, applied research and development, and services in Information Technology and Business Information Technology on a single campus. It is the only dedicated School for Information Technology in Switzerland. The school started operations in Rotkreuz in 2016 and will move into new premises directly at the train station in 2019.

By 2022, there is expected to be a shortfall of 30,000 IT specialists in Switzerland. This shortage in expertise poses major problems for the Swiss economy as an increasing number of companies are digitizing their business processes. For this reason, the Lucerne School of Information Technology is investing in new infrastructures and is also making IT accessible to creative minds with the new Digital Ideation degree program. In addition there is a new unique bachelor's course dedicated to information and cyber security.

The new facilities on the Suurstoffi site in Rotkreuz are a central part of this growth strategy. With the Campus Zug-Rotkreuz, the Lucerne University of Applied Sciences and Arts is creating one of the most advanced learning centers for information technology in Switzerland.

ACADEMY SPONSOR

Zurich University
of Applied Sciences



ZHAW, Institute of Applied Information Technology

The Institute of Applied Information Technology focuses on research and development of smart information technologies, systems and services, to **enable easy and secure access to information** at any time. With our five research groups - Distributed Software Systems, Human Information Interaction, **Information Security**, Information Engineering and Service Engineering we cover both technical and business aspects. We invite you to share your questions, ideas, and problems with respect to smart distributed information systems with us and take advantage of our expertise and experience. A highly qualified team of computer science professors, researchers and research assistants is waiting for you in order to set out for new ways to deal with the ever increasing amount of information.

init.zhaw.ch

THANK YOU

The Swiss Cyber Storm 2018 conference and the Swiss participation in the European Cyber Security Challenge could only be achieved thanks to the superb commitment and generous support from our sponsors and partners as well as the keen interest shown by you, dear conference visitors. Thus, once again a big thank you to everyone involved!

I really hope you enjoyed the event and that you will join us again on October 15th 2019 in the Kursaal Bern. By providing feedback and by telling us what you would like to see changed for 2019, you can help us shape the future of the Swiss Cyber Storm conference: www.swisscyberstorm.com/feedback

Prof. Dr. Bernhard Tellenbach
President, Swiss Cyber Storm

SAVE THE DATE / SUPPORT US

Tue, 15th October 2019 **Swiss Cyber Storm 2019 Conference** (Berne)



Save the date and join us in 2019 when Swiss Cyber Storm is in its second iteration at Kursaal Berne. Please share your ideas on how to improve the conference and tell us, if you have a great idea for a guiding theme to replace this year's "Trust" theme.

Support Us

Support us and become a benefactor ("Gönner")

If you support Swiss Cyber Storm with 1'000 CHF (or more) in a certain year, you get benefactor status for this year. As a benefactor, you get invited to our General Assembly and the subsequent dinner and you get an entrance ticket for the next Swiss Cyber Storm conference. Optionally, we list you as a "Gönner" on our website.

LATEST NEWS, PHOTOS AND PRESENTATIONS



Please visit our homepage for conference photos and presentations. In addition, find information about the next year's Swiss Cyber Storm activities!

www.swisscyberstorm.com