SWITCH-CERT
for Industry & Logistics

Company

Business

IT/OT-Security

Business-IT/OT

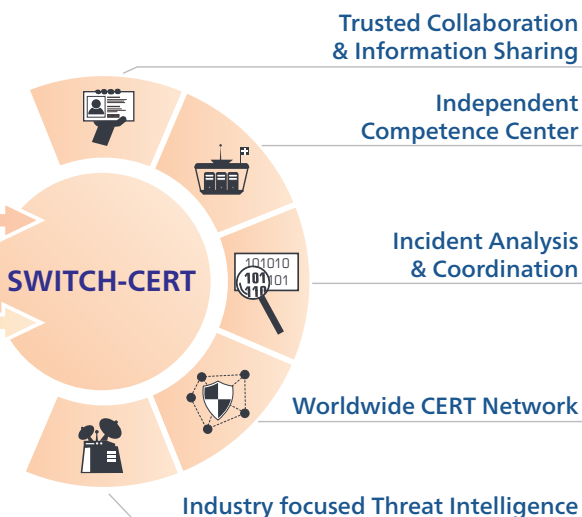Operations, Asset Inventory, Baseline Security

SIEM
Logs/ Security Events

SOC Service
monitor, analyze, remediate, report
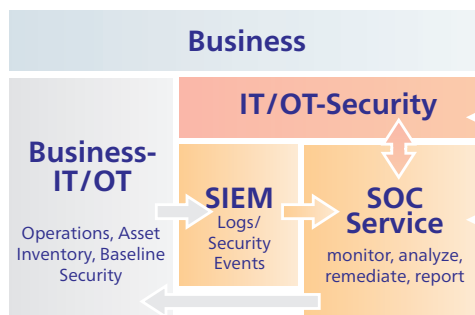
CERT Integration for a State-of-the-Art Cyber Security Solution

SWITCH

SWITCH-CERT

Trusted Collaboration & Information Sharing

Independent Competence Center

Incident Analysis & Coordination

Worldwide CERT Network

Industry focused Threat Intelligence

SWITCH-CERT offers unrivalled threat intelligence, connects experts, and pools resources from the operators of critical infrastructures. Businesses in the fields of energy, industry, and logistics rely on us to handle security incidents and value our product-neutral, interdisciplinary security expertise and access to the global CSIRT/ CERT network.

SERVICES

Incident response

We support you in handling security incidents

- CERT emergency response contact for initial assessment of incidents
- Incident response & coordination
- Malware analysis
- Notice & takedown of fraudulent websites
- Collaborative events with authorities and law enforcement organisations

Security engineering

Access to 20+ security engineers for reviews & second opinion on a variety of topics, such as

- Malware analysis
- Domain security/DNS/DNSSEC
- Network security/IPv6 security
- E-mail security/SPF/DMARC/DKIM
- MISP/threat intelligence

SWITCH

ICS / OT / product security	**Expertise in OT and ICS security**
	• Critical OT threat alerting & advisories
	• OT threat landscape
	• Reviews & second opinion on concepts and architectures
	• Product security based on IEC 62443
	• ICS laboratory for training and research purposes
	• OT network monitoring: open-source based PoC
Threat landscape, critical threat alerting, threat intelligence	**We analyse the current, sector- and Switzerland-specific threat landscape and provide information about critical threats and urgent defence measures**
	• Malware campaign monitoring
	• Ciritical threat alerting & advisories
	• Automated IOC generation relevant to Swiss companies
	• Access to threat intelligence sharing platform (MISP)
	• Password dump & data leak monitoring
CERT / CSIRT access	**Indirect access to our national and international CERT network**
	• Global Forum of Incident and Security Teams (FIRST.org)
	• National CSIRT Forum (Carnegie Mellon)
	• Swiss CSIRT Forum (SWITCH is a founding member)
	• Deutscher CERT-Verbund (German CERT Association; SWITCH has long-standing guest status)
	• Variety of product CERTs
Trusted collaboration & information sharing	**We facilitate trustworthy information sharing within the sector community and between sector-specific CERTs**
	• Secure & trusted collaboration, chat and information sharing
	• Regular information sharing in periodic operation calls and workshops
	• Development and arrangement of workshops based on customer needs (e.g. AD security, cloud security, ransomware prevention)
Forensic analysis	• Advice and initial assessment
	• Data acquisition in SWITCH-CERT lab
	• Image analysis in SWITCH-CERT lab
	• Preparation of a brief report on the evidence found
Security awareness and information about current security issues	**SWITCH-CERT holds regular information events, develops materials and measures, and offers access to national and international security awareness communities**
	• Moderated workshop for supporting the development of internal campaigns
	• SWITCH Security Awareness Adventure: escape room, scavenger hunt or role-play – your employees will learn how to maintain security through play in these training events
	• SWITCH Security Awareness Day
	• Provision of topic-specific content and graphics
	• SWITCH Security Report

Please contact us for a personal appointment

Michael Fuchs

📞 +41 79 930 21 14
✉ cert@switch.ch
🔗 switch.ch/security
📶 securityblog.switch.ch
🐦 twitter.com/switchcert