



CERT - XLM

Computer Security Incident Response
Team of **Excellium Services**

With the expertise of CERT-XLM you may react in realtime to security incidents. Networking and data intelligence of CERT-XLM also help you to improve drastically your threat survey.



“

DATA BREACH [n]: Breach of security leading to accidental, unlawful destruction, loss, alteration, unauthorized disclosure or access to private data.

”

CUSTOMER CHALLENGES

Organisation face daily attempts to get access to their data or systems. This creates a new form of expertises which needs to be deployed across the different teams in order to respond to the following :

- Manage intrusions and security incidents,
- Neutralize or contain attack,
- Elaborate intrusion response plan,
- Gather information on discovered malicious file,
- Assessment of controls in place,
- Damage's evaluation,
- Keep evidences,
- Maintain chain of custody,
- Train team to incident handling,
- Stop data leakage,
- Amorphous threats.

OUR APPROACH

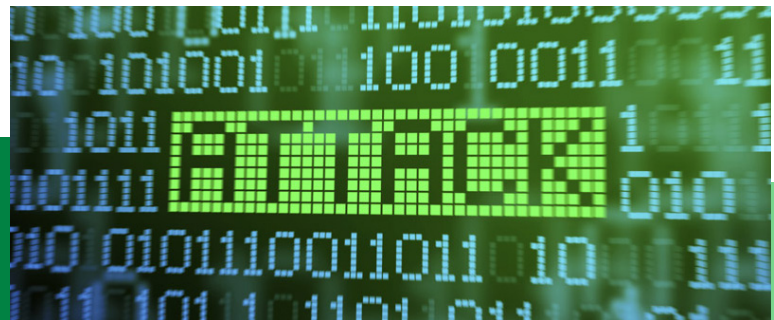
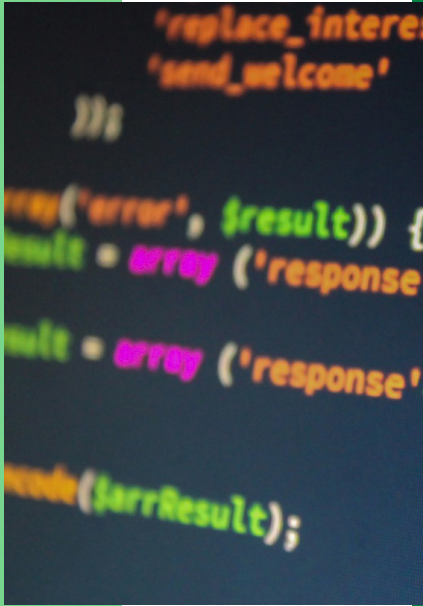
The Excellium CSIRT helps organisations to respond efficiently to IT incidents by providing the following services :

- Help customer with incident handling,
- Malware analysis (Windows, Unix & Mobile),
- Vulnerability Monitoring,
- Prepare and evaluate your incident response plan,
- Server "takedown",
- Forensic Investigations,
- Malicious document analysis,
- Phishing monitoring,
- Log mining,
- Breach analysis,
- Doubt removal,
- CERT collaboration and intelligence sharing.

CERT BENEFITS

A Computer Security Incident Response team is like a fireman unit, they help organisations to be prepared to handle and mitigate intrusions. Customer benefits of the Excellium CERT can be summarised by the following :

- Threat Anticipation,
- Outsourcing of incident management to a rapid response team,
- Cyber response capability development,
- Incident reoccurrence prevention,
- Realising cyber maturity improvements by aligning people, processes image and technology,
- Strengthening the human factor in cyber security,
- Managing incident handling,
- Be confident about cyber security choices.



SECURITY SKILLS

CERT-XML is composed of Security experts that can handle sophisticated attacks and threats.

INTELLIGENCE

CERT-XLM gathers, aggregates, integrates and analyses intelligences feeds.

RESEARCH

CERT-XLM develops tools to find threats for your infrastructure.

NETWORKING

CERT-XLM is member of the CERT.LU initiative and accredited member of Trusted Introducer.

CONFIDENTIALITY

CERT-XLM as Excellium is PSF accredited since 2016.

SERVICES PROVIDED

Example of Excellium engagements :

- Detailed incident report,
- Security recommendations based on intrusion analysis,
- Focused security's alerts,
- Setup recommendation for data mining,
- Malicious website's «takedown»,
- Digital evidences,
- Browser forensic autopsy,
- Product vulnerabilities with real time advisory,
- Vulnerability management based on clients assets.

