computer emergency response team | CERT-EU for the EU institutions, bodies and agencies

# SERVICE CATALOGUE

## Introduction

This Service Catalogue is designed for CERT-EU constituents, especially those CERT-EU starts delivering services to. It provides an overview of CERT-EU services and specifies which information should be exchanged between CERT-EU and the 'Beneficiary' to start operational cooperation. Where appropriate, it provides links or references for useful documents and webpages.

For each service / product, customers will find

- Summary description: a few words describing the service / product
- Service access: key information for accessing or triggering the service
- Cooperation: suggestions in case customers would like to develop specific cooperation with CERT-EU

## Background

The EU Institutions have set up a Computer Emergency Response Team (CERT-EU) on September 11th 2012 after the successful completion of a pilot phase for one year. The team is made up of IT security experts from the main EU Institutions. Its constituency is composed of all the EU institutions, bodies and agencies, 60 organisations with close to 75.000 end users.

CERT-EU's mission is to support the European Institutions to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU. The scope of CERT-EU's activities covers prevention, detection, response and recovery.

## General information

### Contact

**CERT-EU**

Address: CERT-EU - Rue Montoyer, 34 - 1049 Bruxelles
Phone: +3222990005
Website: http://cert.europa.eu
Email (general information): cert-eu@ec.europa.eu
Email (incident response): reports@cert.europa.eu

**Customer (info required)**

- ✓ *Physical / postal address*
- ✓ *Contact person name / phone / email*
- ✓ *Functional mailbox for alerts and incident response*

### Security & Privacy

**CERT-EU**

PGP KeyID: 0x46AC4383
PGP FP: 9011 6BE9 D642 DD93 8348 DAFA 27A4 06CA 46AC 4383
Data Protection: CERT-EU complies with EC Regulation n°45/2001
Privacy Statement: http://cert.europa.eu/cert/plainedition/en/cert_privacy.html

**Customer (info required)**

- ✓ *PGP KeyID*
- ✓ *PGP FP*
- ✓ *Data protection notification (reference)*

### Services categories

Baseline services: service available for any CERT-EU constituent

- ✓ Minimum requirements: none
- ✓ General access conditions: functional mailbox (FMB), PGP key, IP/ASN range

Extended services: service requires financial contribution and linked to a specific service level agreement (SLA)

- ✓ Minimum requirement: Financial contribution and SLA detailing conditions and mutual obligations of 'service provider' (CERT-EU) and 'beneficiary'
- ✓ General access conditions: as described in SLA

# *BASELINE SERVICES*

## 1. Announcements and Advisories

This service includes, but is not limited to, disseminating intrusion alerts, vulnerability warnings, and security advisories to constituents. Such announcements inform constituents about new developments with medium to long-term impact, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.

Also provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include

- reporting guidelines and contact information for CERT-EU
- archives of announcements
- documentation about best practices
- general computer security guidance and checklists
- information that can improve overall security practices

*Service access*

- Specific products: Advisories, CERT-EU White Papers and web portal (http://cert.europa.eu).
- Channel: Website and Email distribution

## 2. Alerts and Warnings

This service involves disseminating information that describes an immediate threat or an on-going intruder attack, specific security vulnerability in your infrastructure, intrusion alert, targeted malware and providing any short-term recommended course of action for dealing with the resulting problem. The alert or warning is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by CERT-EU or may be redistributed from vendors, other CERTs or security experts, or other parts of the constituency.

*Service access*

- Specific products: Alerts
- Channel: Email distribution
- Information required: FMB (where alerts should be forwarded to), PGP key, ASN/IP range, Internet domains owned, email address domain.

*Cooperation*

- Customers are encouraged to notify CERT-EU with any feedback information about alerts they are aware of.

## 3. Incident response coordination

CERT-EU assists and guides the victim(s) of the attack in recovering from an incident via phone, email, fax, or documentation on best effort basis. This can involve technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies. It does not involve direct, on-site incident response actions as described above. CERT-EU instead provides guidance remotely so site personnel can perform the recovery autonomously themselves.

CERT-EU also coordinates the response effort among parties involved in the incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim, such as Internet service providers, other CERTs, and system and network administrators at the site. The coordination work may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis. Part of the coordination work may involve notification and collaboration with an organization's legal counsel, human resources or public relations departments. It could also include coordination with law enforcement.

*Service access*

- Incident should be reported to reports@cert.europa.eu
- At minimum, the following information should be provided in the initial message: name of victim organisation, local incident response contact details (email address, phone), date/time of detection, type of incident, actions taken
- Further information may be asked in the procedure

## 4. Cyber Threat Intelligence

CERT-EU provides a cyber-threat intelligence service which consists in disseminating actionable information on targeted or other relevant attacks. This enables customers to ***detect*** if they have been affected by similar threats, ***prevent*** the occurrence of corresponding attacks on their IT infrastructure, ***react*** appropriately in case of attack, and ***report*** to CERT-EU to assist other customers to counter the threat.

*Service access*

- Specific products:
  - CIMBL (CERT-EU identified malicious blacklist): dissemination of relevant indicators of compromises – technical data to feed IT security tools (IDS, IPS, mailguard, firewalls, etc.)
  - CITAR (CERT-EU identified threat assessment reports): dissemination of threat assessment report – tactical data concerning threat actors, their campaigns, motives, tactics/techniques/procedures and courses of action to defeat them
- Email distribution
- Information required: FMB, PGP key
- More information: see 'CIMBL-User-Manual'

*Cooperation*

- Customers are encouraged to notify CERT-EU any specific threats or attacks they are aware of.

# *EXTENDED SERVICES*

## 5. Incident response and analysis on site

The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. CERT-EU helps to analyse the affected systems and conduct the acquisition of the systems, instead of only providing incident response support by telephone or email (see above). CERT-EU team members would travel to the site and perform the response activities in support of the local team.

CERT-EU may use the results of vulnerability and artifact analysis to understand and provide the most complete and up-to-date analysis of what has happened on a specific system. CERT-EU correlates activity across incidents to determine any interrelations, trends, patterns, or intruder signatures. Sub-services that may be done as part of incident analysis are

- Forensic evidence collection: CERT-EU supports the local team or carries out the collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports via memory forensic analysis; and checking for Trojan horse programs and toolkits.

- Tracking or tracing: CERT-EU supports the tracing of the origins of an intruder or identifying systems to which the intruder had access. This activity might involve tracking or tracing how the intruder entered the affected systems and related networks, which systems were used to gain that access, where the attack originated, and what other systems and networks were used as part of the attack. It might also involve trying to determine the identity of the intruder. This work might be done alone but usually involves working with law enforcement personnel, Internet service providers, or other involved organisations.

*Service access*

- SLA
- Data protection notification and privacy statement

## 6. Artifact analysis and actions

CERT-EU performs or supervises the performance of a technical examination and analysis of artifact found on a compromised system. The analysis might include identifying the file type and structure of the artifact, comparing a new artifact against existing artifacts or other versions of the same artifact to see similarities and differences, or reverse engineering or disassembling code to determine the purpose and function of the artifact. This service also involves sharing and synthesizing analysis results and response strategies pertaining to an artifact with other researchers, CERTs, vendors, and other security experts. Activities also include maintaining a constituent archive of known artifacts and their impact and corresponding response strategies. CERT-EU determines the appropriate actions to detect and remove malware from a system based on identified malware, as well as actions to prevent malware from being installed. This may involve creating signatures that can be added to antivirus software or IDS.

*Service access*

- SLA
- Data protection notification and privacy statement

## 7. Development of security tools

This service involves the provision of specialised tools to improve detection or remediation. This can include developing tools or scripts that extend the functionality of existing security tools to detect artefacts, to cross-correlate logs and to summarise the state of health of the infrastructure. It can also include tools to automatically handle suspicious documents, email, links etc. Finally it can also include tools to automatically handle incoming feeds of abuse and malevolence monitoring.

*Service access*

- SLA

## 8. Intrusion Detection System and Log management Services

CERT-EU makes available a network intrusion detection device in the form of an appliance or software application to be installed in the network of the constituent with the purpose of detecting suspicious or anomalous events potentially related to targeted attacks and produce reports to a management station. CERT-EU uploads specific rules and indicators of compromise during on-going incident and maintains the database of rules and indicators for continuous operation. It reviews the resulting logs, analyses and initiates a response for any events that meet their defined threshold, or forwards any alerts according to a pre-defined service level agreement or escalation strategy.

CERT-EU also makes available tools and services to facilitate log management and correlation using a multi-tier index for searching into past events or for detecting events in real-time using rules applied to log files from multiple sources.

*Service access*

- SLA
- Technical information for IDS installation

## 9. Security Audits or Assessments and Best Practice Review

This service provides a detailed review and analysis of constituent's security infrastructure and procedures, based on the requirements and risk assessment defined by the constituent, on industry standards that apply and on best practices in protecting against targeted attacks. It can also involve a review of the organizational security practices.

CERT-EU will also support security awareness rising at senior management level in order to improve prevention and to obtain support for the improvement plan resulting from the review.

*Service access*

- SLA

# APPENDIX A

# Services summary

| Service | Access | Info from beneficiary |
|---|---|---|
| Announcements | Baseline | None |
| Alerts and Warnings | Baseline | FMB + PGP<br>IP/ASN, Internet domains owned, email address domain |
| Incident response coordination | Baseline | FMB + PGP |
| Cyber Threat Intelligence | Baseline<br>Extended | FMB + PGP<br>NDA |
| Incident response and analysis on site | Extended | FMB + PGP<br>SLA (as appropriate details of IT infrastructure) |
| Artifact analysis and actions | Extended | FMB + PGP<br>SLA |
| Development of security tools | Extended | SLA |
| Intrusion Detection System and Log management services | Extended | SLA |
| Security Audits or Assessments and Best Practice Review | Extended | SLA |

# APPENDIX B

## Resources per extended service (continuously updated)

| Incident response and analysis onsite | |
|---|---|
| **FORENSICS EXPERTS** | CERT-EU offers highly trained and certified personal with daily experience in incident response for onsite coordination. |
| **MISP** | Malware information sharing platform (MISP) to facilitate a central database for storing technical and non-technical information about malwares and attacks. Data from external instances is also imported into your local instance. Automatically creating relations between malwares, events and attributes storing data in a structured format (allowing automated use of the database for various purposes). Exports in absorbable format (CIMBLS), for generating IDS, OpenIOC, plain text, xml output to integrate with other systems (network IDS, host IDS, custom tools). Batch-import from OpenIOC, GFI sandbox etc. Data-sharing for automatically exchange and synchronization with other parties and trust-groups. |
| **RTIR** | Request tracker platform specifically designed for incident response. A typical workflow begins by triaging incoming incident reports and linking them to an existing incident or creating a new one. Each incident is designed to keep track of everything you need to know to solve the problem. From an incident, it's easy to launch investigations to work with law enforcement, network providers, or other organizations. You can also set up blocks to keep track of what's been done to mitigate the issue. |
| **TRAINING MATERIAL** | First line help guide regarding spear phishing detection. |
| **CUSTOM TRAINING** | CERT-EU can develop after specific request stand-alone training modules for first line help desk regarding security threats and abuses. |

| Artifact analysis and response | |
|---|---|
| **SPLUNK** | CERT-EU offers a starter kit licenses for Splunk. Splunk captures indexes and correlates real-time data in a searchable repository from which it can generate graphs, reports, alerts, dashboards and visualizations. Splunk make machine security data accessible across an organization and identifies data patterns, provides metrics, diagnoses problems and provides intelligence for artifact analysis and response experts. |
| **SOURCEFIRE** | CERT-EU offers a starter kit licenses for SourceFire. SourceFire is a network intrusion prevention and detection system utilizing a rule-driven language, which combines signature, protocol and anomaly based inspection methods. Developed in tandem with the Snort open source community. It is the most widely deployed intrusion detection and prevention technology worldwide. |
| **FIREEYE MAS** | FireEye Malware Analysis System (MAS) is a sandbox for malware analysis. Allows threat analysts to configure test environments where they can execute and inspect advanced malware, zero-day, and targeted APT attacks embedded in common file formats, email attachments, and Web objects. It provides automated threat forensics and dynamic malware protection against advanced cyber threats, such as advanced persistent threats and spear phishing. |
| **ACQUISITION TOOLKIT** | CERT-EU offers wide range of very specialized tools for memory, disk, logs and network extraction of digital artifacts. |
| **CUSTOM SCRIPTS** | CERT-EU offers special customized and optimized scripts to trace and analyse malicious files (pdf, java, ms-office etc.). |

| Development of security tools | |
|---|---|
| **SNORT RULES CONVERTER** | Script for converting Snort rules to different IDS systems |
| **MAIL SCANNER** | Semi-automated solution to scan emails for potential malicious active content |
| **LARGE SCALE SCANNING** | Scripts for large scale scanning with the use of MSERT |
| **PGP** | Secure communications with PGP and VPN access |
| **EMM** | Based on JRC's Europe Media Monitor (EMM) technology, EMM server gathers, filters, classifies, extracts and aggregates Information Security related articles. Monitors trends, detects breaking news, and visualizes analysis results, alert users. Also allows customized views with NewsDesk Application for collecting security news. |
| **ABUSEHELPER** | Tool for scraping abuse feeds and sending automatic notifications. These notifications are often normalized per feed (each feed typically uses different formats to report). There is also a lot of information about Internet abuse, available by different feed providers (Zone-H, DShield, Zeus Tracker). This tremendous amount of available information needs to be well utilized, as the amount of information is too big for manual processing. AbuseHelper follows a number of sources and produces actionable reports and dashboard for the people that need to treat all these notifications. AbuseHelper also automates the enriching of information, such as finding the owners of reported IP addresses from public databases (such as Whois). |

| Intrusion Detection System and Log management services | |
|---|---|
| **YARA RULES** | CERT-EU provides YARA rules for detecting signs of malicious activities. YARA is a tool aimed at helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families based on textual or binary patterns contained on samples of those families. |
| **IDS SENSORS** | CERT-EU offers a network intrusion detection solution to be installed in the network of the client for detecting anomalies that could be targeted intrusions. It also includes passive malware monitoring and alert notification. |
| **DETECTION RULES** | Up-to-date rules from multiple non-public, APT relevant sources, incidents in constituency, specialized closed trusted group and paid feeds from specialized IT security companies. |
| **DISTRIBUTED SEARCHES** | CERT-EU can implement distributed Splunk searches through STESTA. STESTA is the European Community's own private, IP-based network. STESTA offers a telecommunications interconnection platform that responds to the growing need for secure information exchange between European public administrations. It is a European IP network dedicated to inter-administrative requirements and providing guaranteed performance. |
| **LOG FILTERING** | CERT-EU offers an optimization procedure for filtering raw log data and uploading them in SPLUNK. The main benefit of the procedure is to minimize the cost per GB used for analyzing malicious activities. |
| **IOCS** | Cert-EU offers an optimized procedure for making lookups for IOCs (Indicator of compromise) and uploading them in SPLUNK. After IOCs have been identified in a process of incident response and computer forensics, they can be used for early detection of future attack attempts using intrusion detection systems and antivirus software. Typical IOCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs of botnet command and control centers. |
| **CROSS CORRELATION** | CERT-EU offers an optimized procedure for cross correlation of log events. Using the same IOCs as the IDS system makes easy the searching for past events in the log files using a multi-tier index. It detecting events in real-time using rules applied to log files from multiple sources. Finally it can search for current events across constituents during incident response. |

| Security Audits or Assessments and Best Practice Review | |
|---|---|
| **IBM APPSCAN** | With IBM AppScan CERT-EU offers web security testing and monitoring services. AppScan tests Web applications for security vulnerabilities and learns the behaviour of each application, whether an off-the-shelf application or internally developed, and develops a plan intended to test all of its functions for both common and application-specific vulnerabilities. |
| **IOC Finder** | CERT-EU offers optimized technics to run IOCFinder across all the workstations in an infrastructure. IOC Finder used for collecting host system data and reporting the presence of Indicators of Compromise (IOCs). IOCs help incident responders capture diverse information about threats. IOC Finder supports collection of full data, sufficient for general IOC matching requirements, using a portable storage device allows collection from multiple hosts, IOC hit reporting in simple text, full HTML, and full MS Word XML formats. Reports can be generated for specific hosts or all hosts. |
| **REDLINE** | CERT-EU offers optimized technics to run REDLINE across all the workstations in an infrastructure. Redline provides host investigative capabilities to find signs of malicious activity through memory and file analysis, and the development of a threat assessment profile. With Redline, CERT-EU can thoroughly audit and collect all running processes and drivers from memory, file system metadata, registry data, event logs, network information, services, tasks, and web history.<br>Analyse and view imported audit data, including narrowing and filtering results around a given timeframe. |
| **MSFT MSRT** | CERT-EU offers optimized technics to run Windows Malicious Software Removal Tool across all the workstations in an infrastructure. Windows Malicious Software Removal Tool is a small, portable utility for checking Windows XP, 2000, Server 2003, Vista, and 7 for infection by a range of known threats, including Blaster, MyDoom, and Sasser, and removes any threats it finds. |