EXTENDED SERVICES

Service Level Agreement

Remote Security Services for IDS

Version 1
22/10/2013

TABLE OF CONTENTS

Service Level Agreement
Remote Security Services for IDS

1 SCOPE

CERT-EU makes available a network intrusion detection device called “Sensor” 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.

The Sensor is a dedicated Intrusion Detection System called “IDS” and should not be used for any other purpose while under management by CERT-EU.

CERT-EU Remote Security Services for IDS is designed to provide monitoring and support of the intrusion detection sensor network across a variety of platforms and technologies.

CERT-EU will provide wide range of services in support of the product features like:

a. Project kick-off, assessment, and implementation. During deployment of the Network IDS, CERT-EU will work with the Constituent to help define appropriate security policies, assist with installation and configuration of the Sensor(s), and verify proper device operation prior to transition of the Sensor(s) to the SOC/NOC.
b. Policy management. CERT-EU provides policy management services to help the Constituent keep Sensors configured with a valid security policy.
c. Device management. CERT-EU will maintain the Sensor by monitoring its system health and availability and applying vendor updates to the Sensor.
d. Security alert management. CERT-EU Sensor with its constantly updated rules and feeds detects malware targeting hosts in constituent environment or malicious outbound Command and Control (C2) network traffic and automatically sends security incident alert for investigation. If the constituency has 24x7 monitoring capabilities then a personalized web based console can be used to assess the alerts alternatively a mechanism can be created for automated e-mail alerting.
e. Web interface. A Web interface which serves as the Constituent interface to management of the Sensor, alerts, logs, reports, policy change requests, and other types of service tickets will be provided upon request.

2 ACTIVITIES

2.1 PLANNING

2.1.1 Initiation

During initiation, it will be confirmed if CERT-EU will either work with the Constituent to deploy a new Sensor or begin management of an existing Sensor.

In both cases Constituent will assign a contact person responsible for the Sensor and officially inform CERT-EU.

2.1.2 Project Kick-off

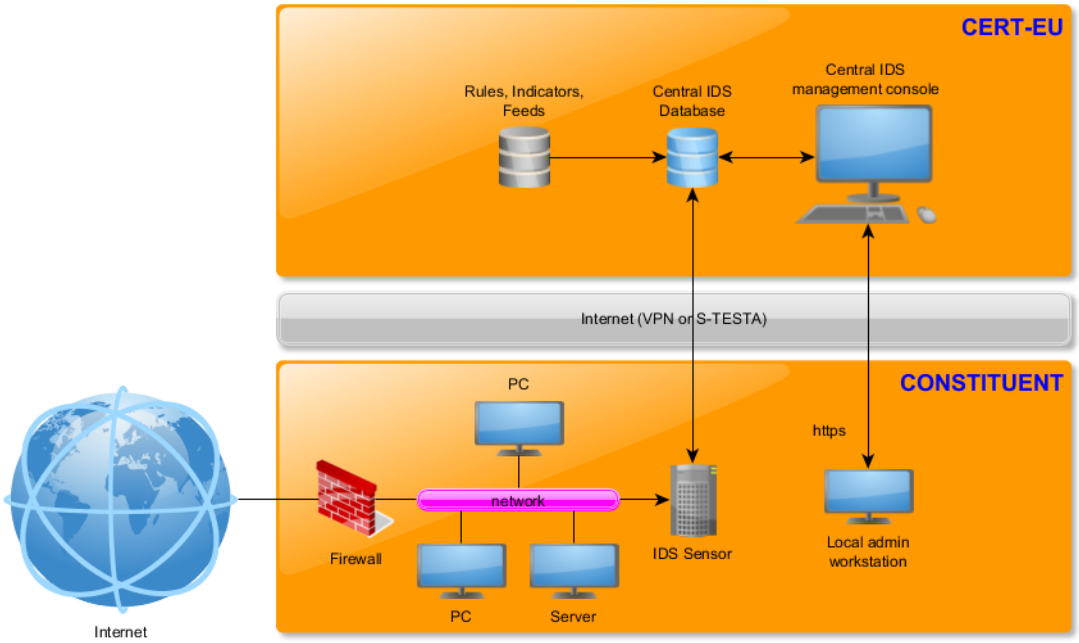
CERT-EU will send the Constituent a welcome e-mail and conduct a kick-off call to:

- Introduce the Constituent contacts to the assigned CERT-EU deployment specialist.
- Set expectations.
- Begin to assess the Constituent requirements and environment.

CERT-EU will provide a document called *"Network Access Requirements"*, detailing how CERT-EU will connect remotely to the Constituent network, and any specific technical requirements to enable such access.

Typically, CERT-EU will connect via standard access methods through the Internet; however, a site-to-site VPN like S-TESTA may be used, if appropriate.

A typical architecture is presented in the following diagram:



2.1.3 Environment Mapping

CERT-EU will provide an information collection form for the Constituent to document detailed information for the initial setup of the Sensor and associated service features. Most of the questions will be technical in nature and help determine the layout of the Constituent network, Hosts on the network, and desired security policies. A portion of the requested data will reflect the Constituent organization, and will include security contacts and escalation paths.

2.1.4 Environment Assessment

Using the provided information, CERT-EU will work with the Constituent to understand the existing Constituent environment, and build a configuration and security policy for the Sensor. If migrating from an existing Sensor to a newer Sensor, CERT-EU will use the configuration and policy on the existing Sensor.

During this assessment, CERT-EU could make recommendations to adjust the policy of the Sensor or the layout of the portion of the network that the sensor will connect to.

CERT-EU recommends that all Sensors be deployed out of line, at the network perimeter, behind the firewall.

CERT-EU will work with the Constituent to help determine an optimal Sensor configuration based on the current infrastructure.

CERT-EU may tune the policy to reduce the number of erroneous alarms, if required.

2.1.5 Existing Sensor Assessment

In case of existing Sensor CERT-EU should take over the management because it must assess the Sensor to be sure it meets certain specifications. CERT-EU may require the Sensor software or security content to be upgraded to the most current versions in order to provide the service. Other required criteria may include the addition or removal of applications and user accounts.

2.2 IMPLEMENTATION

2.2.1 Configuration at CERT-EU

For Sensors purchased through CERT-EU Extended services agreement most of the configuration and policy setting will take place at CERT-EU facilities.

While physical installation and cabling are Constituent responsibility, CERT-EU will provide live support, via phone and e-mail, and will assist the Constituent with location of vendor documents detailing the installation procedure for the Sensor. Such support must be scheduled in advance to ensure availability of a deployment specialist.

At the Constituent request, on-site installation may be provided by CERT-EU.

2.2.2 Remote Configuration

When taking over management of an existing Sensor, CERT-EU will typically perform the configuration remotely.

The Constituent may be required to physically load media.

All managed Sensors will require some remote configuration, which may include the registration of the Sensor with CERT-EU Remote Security Services infrastructure.

2.2.3 High availability

To help protect against hardware failure and provide high availability, two managed protection Sensors may be configured and deployed; one fully operational and the other waiting as a backup to take over should the first Sensor fail

In some cases sensors can also be deployed as clusters, such that both Sensors operate and share network load.

2.2.4 Transition to Security Operation Center (SOC)

Once the Sensor is configured, physically installed, implemented and connected to the CERT-EU central management station, CERT-EU will provide the Constituent with the option of having a demonstration of the CERT-SOC capabilities and performance of common tasks.

The final step of services deployment occurs when the CERT-EU SOC takes over management and support of the Sensor and the relationship with the Constituent. At this time, the on-going management and support phase of the services officially begins. Typically, CERT-EU will introduce the Constituent via phone to the SOC personnel. The Constituent will provide CERT-EU with the following

- Contact details for personnel in key places.
- Network diagrams of the segment where the sensor will monitor traffic.
- Services offered by the Constituent seen by the sensor with relevant technical details (service, server IP, OS, etc.).
- A written Incident handling escalation policy containing at least :
    - a procedure to respond to events when to notify the client
    - automatic send of e-mails
    - send events to SIEM
    - rule suppression strategy

2.2.5 Security alert management

Sensors are regularly polled by a central management station, keeping CERT-EU security analysts informed of potential problems as they develop.

A personalized web based console will be used to assess the alerts or alternatively a mechanism can be created for automated e-mail alerting Constituent.

Constituent can choose to manage all Sensor alerts or authorise CERT-EU to manage them on their behalf.

In case CERT-EU is responsible for the Sensor management additional monitoring and analysis can be provided by CERT-EU security analysts on working hours to assess which alerts may be significant, validating these alerts as probable Security Incidents and escalating the probable Security Incidents to the Constituent.

2.2.6 Web interface

A Web-based interface will be available to the Constituent for monitoring real time and past alerts. Also it will be possible to download alert packet captures and generate custom reports. Historical data such as alerts and connections will be held for at least 6 months.

2.2.7 Reporting

One time per month, CERT-EU will produce a summary report. The reports frequency and content will be customised according to constituent needs.

2.2.8 Optimisation

Sensors default rule sets for detecting malicious traffic will be customised and optimised to address the specific needs and environment of the constituent.

2.2.9 Policy Management

If CERT-EU is responsible for management of the Sensor the Constituent may request policy changes. Policy change requests are subject to approval by CERT-EU. Such approval will not be unreasonably withheld; however, among other reasons, a request will be denied if the policy change would result in a large number of false alarms.

If the Constituent is responsible for management of the Sensor, the CERT-EU is solely responsible for facilitating the application of all policy changes and filters and providing expert help and guidance and the interpretation of CERT-EU custom rules.

2.3 MAINTENANCE

2.3.1 On-going Policy

CERT-EU will work with the Constituent to maintain protection strategies.

On a quarterly basis, CERT-EU will audit the Constituent policy settings to verify accuracy.

One time per quarter (at the Constituent request) CERT-EU will work with the Constituent to review all Sensors under management and identify recommended changes to the network protection strategy.

2.3.2 Device Management

Typically, CERT-EU will be the sole provider of software-level device management for the Sensor. With root/super-user/administrator level access to the device, CERT-EU will maintain system status awareness, apply operating system (“OS”) patches and upgrades, troubleshoot problems on the device, and work with the Constituent to help ensure the device remains available. CERT-EU will monitor for availability of the Sensor, notify the Constituent when certain utilization thresholds have been met, and monitor the device during working hours.

Regular, automatic updates will be provided for the software and firmware.

For non-Appliance based Sensors, the Constituent is responsible for all OS-level management.

For Appliance-based Sensors, CERT-EU will assume responsibility for the OS-level management.

2.3.3 Connectivity Management

All security logs, events and management data travel between the SOC and the managed Sensor via the Internet. Data travelling across the Internet is encrypted using industry-standard strong encryption algorithms.

Requests for connectivity through alternate means (e.g., S-TESTA) will be addressed on a case-by-case basis.

2.3.4 Platforms Management

CERT-EU will use a management platform on CERT-EU premises to manage the Sensors.

2.3.5 Log Storage

The logs are migrated to a physical backup media such as tape or DVD. Backup media is archived in a secure, environmentally controlled facility. Archived data will be available for one year from the date of log creation or according to Environment Assessment results.

At the Constituent request, CERT-EU will submit a request for media location and retrieval.

2.3.6 Health and Availability Monitoring

The health and performance of the sensor is monitored natively. The devices are regularly polled by the Central management station, keeping CERT-EU security analysts informed of potential problems as they develop. Key metrics analysed by the monitoring Sensor include:

- Hard disk capacity (if applicable)
- CPU utilization
- Memory utilization
- Process availability

In addition to system health metrics, CERT-EU will monitor device uptime and availability.

2.3.7 Outage Notification

If contact with a managed device is lost, additional time-based checks will be initiated to verify a valid outage has been identified.

If the Sensor is not reachable through standard in-band means, the Constituent will be notified via telephone using a predetermined escalation procedure. Following telephone escalation, CERT-EU will begin investigating problems related to the configuration or functionality of the managed device.

2.3.8 Notifications Handling

In the event system health problems or an outage has been confirmed, a trouble ticket will be created and a CERT-EU security analyst will be notified to begin research and investigation. The status of all system health tickets is available through the CERT-EU-SOC.

Any unresolved notification more than a month old will be suppressed.

2.3.9 Application/Operating System Updates

Periodically, it will be necessary for CERT-EU to install patches and software updates to improve device performance, enable additional functionality, and resolve potential application problems. The application of such patches and updates may require platform downtime or Constituent assistance to complete. If required, CERT-EU will declare a maintenance window in advance of any such updates, and the notification will clearly state the impacts of the scheduled maintenance and any Constituent-specific requirements.

2.3.10 Security Content Updates

To help ensure the most current threats are properly identified, CERT-EU will update security platforms with the most current Security Content. Such Security Content, delivered in the form of new checks or signatures, antispam and antivirus modules, and new feeds for the security intelligence module, enhances the Sensor's security capabilities. Local detection rules will be uploaded when available and updated accordingly. Local detection rules are CERT-EU property and they cannot be shared without the explicit consent of CERT-EU.

At the discretion of CERT-EU, Security Content updates may be downloaded and installed onto the security platform at any time. Such an operation is transparent to users.

3 REMEDY

If the Sensor does not perform as expected, or is identified as the potential source of a network-related problem, CERT-EU will examine the device configuration and functionality for potential issues. A trouble ticket will be created and a CERT-EU security analyst will be notified to begin research and investigation. Troubleshooting may consist of an offline analysis by CERT-EU, or an active troubleshooting session between CERT-EU and the Constituent. CERT-EU will attempt to resolve any technical issues as expediently as feasible. If the Sensor is eliminated as the source of a given problem, no further troubleshooting will be performed by CERT-EU.

The status of all tickets is available through the CERT-EU-SOC.