BREACH DETECTION & INCIDENT RESPONSE SERVICE
Traditional security technologies (Network Firewalls, Antivirus, URL Filtering, Intrusion Prevention Systems, etc.) are no longer effective at stopping cybercrime attacks. Thanks to an innovative technology platform and to a team of highly specialized security professionals, Certego identifies and manages cyber attacks before they can have severe impacts on the business.

Certego Breach Detection & Incident Response Service

OVERVIEW

In recent years, the complexity and range of new IT security threats has grown rapidly. Conventional computer protection technologies have become less effective and are no longer able to guarantee the protection of company assets. An effective defence strategy should be based on an intrusion detection platform which uses adequate tools managed by specialised and expert resources within a framework of structured and contextualised processes.

Certego Breach Detection & Incident Response is a Certego IT security service which provides the client with support in the detection, analysis and response phases of security incident management processes and those preventing **cybercrime**.

The service uses **Certego PanOptikon** platform for the detection, analysis and management of incidents and is supported by a dedicated Incident Response Team available 24/7, whose members are professional experts with certified experience in the management of IT security incidents and digital forensics investigations.

CERTEGO PANOPTIKON

Certego PanOptikon platform comprises technological instruments, a team of analysts and processes needed to provide an effective Breach Detection & Incident Response service. Certego continually monitors the network and systems using sensors to analyse network traffic and information supplied by devices looking for anomalies and signs that a system is compromised or under attack.

- **Certego Malware Labs** gathers, classifies and analyses IT threats by following them as they evolve 24/7. It generates detailed information useful for the detection of any suspect activity relating to security incidents and integrates this into third party information flows. The Threat Intelligence flow, which is constantly updated, feeds into Certego monitoring sensors.

FEATURES

- Team of experts with certified experience in Incident Response Processes and Procedures, available “as a service” 24/7
- Threat Intelligence integrated into the Certego PanOptikon platform
- Passive monitoring of network traffic and systems
- Can be integrated with pre-existing technologies
- Effective against:
  - Malware
  - IT Fraud
  - Zero-day attacks
  - Application attacks
  - Advanced Persistent Threats
  - Distributed Denial of Service
  - Data Leakage

BENEFITS

- Rapidly identifies IT attacks and attempts to compromise
- Develops the most suitable response procedures to contain an attack, remove the threat and reduce its impact on the business
- Supports the client in management activities by tracing security problems back to IT administration activities
- Optimises the client’s Security Posture over time by carrying out an Evidence-Based Risk Assessment

Certego S.R.L. · via Perlasca, 25/E Modena (MO) - Italy · P.I. 03517100362

Certego Breach Detection & Incident Response

- Certego **Network Sensor** integrates different analysis and monitoring tools in a single appliance and can be integrated with pre-existing technologies, incorporating security incidents from various sources.
- Certego **Host Sensor** is installed as a light software agent designed for the most sensitive clients and servers, and also monitors devices when they are used outside the company.
- Certego **Cloud Analytics** is a correlation and analysis infrastructure which gathers together anomalies detected by sensors and generates the alerts that are sent to the Incident Response Team.
- The **Incident Response Team (IRT)** analysts check every alert to assess the nature of the anomaly and classify any verified incident according to level of seriousness and priority, and evaluate the threat and associated risk. The IRT lastly designs a detailed and customised response plan, highlighting appropriate containment, removal and system recovery procedures.

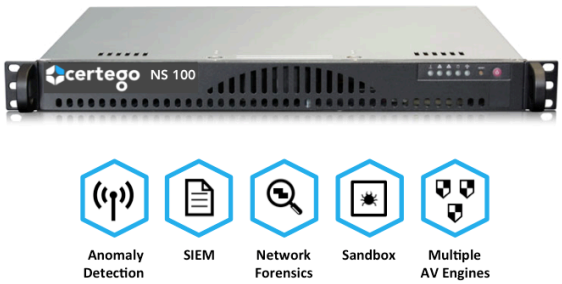
PANOPTIKON SERVICE PORTAL

Through PanOptikon portal, the client can constantly keep a check on the security status of its own systems and monitor the development of IT threats.

The portal provides the client with direct access to support from Certego Incident Response Team and to incident management procedures (Remediation Proposals), which are designed around the type of the security problem and the client's requirements in order to reduce any impact on the business.

Furthermore, the Risk Assessment features make it possible to detect the most serious threats and verify the effectiveness of the prevention systems.

Certego PanOptikon Service Portal



Certego Network Sensor NS100

Certego PanOptikon platform uses the following network appliances for the anomaly detection and security monitoring functions:

	Internet Bandwidth	Users
NS50	50 Mbps	250
NS100	400 Mbps	2500
NS200	1 Gbps	>3000

ADVANCED THREAT PROTECTION

PanOptikon components, i.e. the Network and Host Sensors, ensure that Breach Detection & Incident Response Service is able to provide the following advanced IT security functions:

- **Advanced Intrusion Detection**: In order to detect the presence of anomalies in network traffic and active processes, Certego sensors use around 18,000 correlation rules, which are updated on a daily basis.
- **Botnet Protection**: Thanks to its own Threat Intelligence platform and the Anomaly Detection functions, Certego sensors can detect and analyse the presence of bots within the client's organisation.
- **Extended Virus Detection:** Certego sensors are able to capture potentially malevolent objects (i.e. executable files, PDFs, Office documents, etc.) and analyse them using 50+ Antivirus engines, thus significantly improving on the anti-malware functions which a client may already be using.
- **APT Detection**: The use of the advanced sandbox platform created by Certego Malware Labs enables sensors to detect malevolent software components even when they are completely unknown to major antivirus vendors.