Thanks to EyeGuard cyber SOC services, organisations have complete visibility on their Internet facing assets regarding malicious activity on a 24/7 basis. Through this service, you will gain access to expert security analysts and a task force in case of a security incident.

EyeGuard Services will give you the ability to monitor your critical assets in real time. EyeGuard Services will also include the management and support of your security devices based on Service Level Agreements.

Cyber incidents are becoming a daily reality for organisations. Excellium has designed EyeGuard to address the following points:

- The lack of IT security skills and resources in organisations,
- Control operational cost, improve visibility, enhance security and reduce risk,
- Monitor critical assets availability and integrity in real time,
- Define efficient incident handling to deal with data breaches,
- Quickly identify and understand signs of potential malicious activities,
- Define correlation use cases and cyber defense strategy to mitigate the threat’s impact,
- Addressing compliance requirements.

Handling incidents in an organisation needs the involvement of different business units. A formal plan with skilled personnel is a must for an efficient Incident Response Service. Therefore EyeGuard includes:

- Evaluate and prepare your incident response plan,
- Train your team to understand current security challenges,
- Connect your infrastructure to Excellium via connection kit and encrypted link,
- Define Service Level Agreements (SLA), responsibility assignment matrix (RACI) and contacts for escalation,
- Put in place 24/7 internal / external security monitoring and management based on your existing SIEM or Excellium’s shared SIEM,
- Escalate only relevant incidents after analysis,
- Provide executive and operational reporting.
EYEGUARD SERVICES BENEFITS
This service should be seen as an extension of your operational security team. In this way, subscribing to EyeGuard Services will bring you the following benefits:

- Extending your security and operation team with our EyeGuard Services team,
- Controlling operational cost thanks to our fixed price offer,
- Recognizing cyber threats and responding in a timely manner according to the Service Level Agreements,
- Challenging your infrastructure with external vulnerability scans and Distributed-Denial-Of-Service tests (DDoS),
- Continually develop the capability to consume and leverage threat intelligence from your past incidents and information-sharing sources,
- Test on regular basis of your email and web security policies thanks to our state-of-the-art technology and analytics tools,
- Advanced monitoring capabilities with user simulation to validate your application,
- Respond to audits thanks to detailed and custom reportings.

SECURITY SKILLS
Gain access to security experts with more than 15 years of experience who can handle sophisticated attacks and threats. We are passionate security specialists and pioneers.

VENDOR NEUTRAL
Our highly skilled security analysts hold industry recognized certifications covering popular SIEM and a wide range of security products.

INTELLIGENCE
Gain near real-time up-to-date Indicators of Compromise (IoC) push on your SIEM thanks to Malware Information Sharing Platform integration (MISP) and our CSIRT.

EVOLUTION
We are continuously developing tools to find threats in your infrastructure. We also challenge your email and web filtering policies.

FAST DEPLOYMENT
We can deploy our solutions quickly in your environment.

SERVICES PROVIDED
EyeGuard Services, the commercial brand of our SOC as a Service offering deliver the following services:

- 24/7 advanced and proactive monitoring based on defined and dedicated SLAs to protect your critical assets,
- Use cases based on your assets and combined with our experience. We are continuously improving our detection capability for new malware or new kinds of fraud,
- Incident handling, threat management and remediation assistance with first Forensic analysis in case of crisis,
- Get “up to date” security alerts from our CSIRT and associated services (like malicious domain take down),
- External and internal scans to ensure you are not exposed to new threats.

Twin Squares, Culliganlaan 1B
B-1831 DIEGEM
Office: +32 2 403 12 81

5 rue de Goell
L-5326 CONTERN
Office: +352 26 20 39 64