exprivia

future. perfect. simple.

CyberSecurity

Optimize investment and reduce the overall risk

Reduce the risk of a security incident

Exprivia is particularly active in the Cybersecurity area. We are a member of the European Cyber Security Organization (ECSO) and are involved in a European project (ECHO) generated by the H2020 program.
We have a whole Digital Factory dedicated to Cybersecurity (DCFY) and we also can leverage on our own Security Operations Centre.
Exprivia has an offering on cybersecurity addressing the main security controls around the Identify,
Protect, Detect, Respond and Recover areas designed according to the NIST framework.
The cybersecurity unit has a mix of junior and senior talents hired with proper competence and certification fitting the needs of the security controls in terms of knowledge and experience.
The Exprivia Cybersecurity strategy has been developed with the aim to support clients in the digital transformation process reducing the risk of cybersecurity threats and being compliant with the existing regulations according to budget constraints.
The offering covers all the aspect of the cybersecurity projects, starting with the most appropriate risk assessment to identify the proper security controls to be implemented in the area of prevention, detection, response and recover of the service, up to the implementation and management of the security controls.
For each control, Exprivia suggests the most appropriate and effective technology in the specific context, implements the service and provides support to processes and technologies using the most appropriate delivery model, either in house of the client or from our Security Operation Centre (SOC).
Exprivia offering in the area of cybersecurity is based on information sharing, competence and awareness, consulting services and industry knowledge.

exprivia

future. perfect. simple.

OT Security Services

OT Policy review
We help customers to implement an actionable plan to improve compliance to ISA/IEC 62443

OT Vulnerability assessment
Asset identification and security posture snapshot for the IT/OT environment

OT Security Monitoring
OT security solutions implementation on premises and eventually remotely managed from our SOC

OT Global response Team
We prepare and train the blue team to improve resilience and prepare for incidents, with training and cyber-range activities.

OT Policy Review

- IEC62443 goal is to secure the IACS, which is composed by:
  - Hardware
  - Processes
  - Internal and external People, which executes various processes within policy bounds
- This service helps the customer through the various phase of the IACS lifecycle
  - Specification
  - Integration/commissioning
  - Operation/maintenance
  - Decommissioning
  - Report of findings and recommendations
- Action plan

Vulnerability Assessment

- Identification of assets
  - IT, OT and IOT architecture documentation
  - Asset discovery & inventory
  - Passive and active scan
  - Communication lines
  - Assessment
  - Misconfiguration of assets
  - Vulnerabilities
- Report of findings and recommendations
- Action plan

OT Security Monitor

- Identification of assets
  - IT, OT and IoT architecture documentation
- Identification of vuln product architecture
  - Sizing
  - Procurement
- Installation
  - Creation of first policy according to business goals, standards and other requirements
- Fine tuning
  - Policy tuning according to results
  - Report creation
- Integration with SIEM
- Report of findings and recommendations
- Action plan

OT Global response Team

- Blue Team creation and training
- Preliminary activities for successful Incident handling
- Cyber range exercises
- Post exploitation recovery and analysis

exprivia

future. perfect. simple.

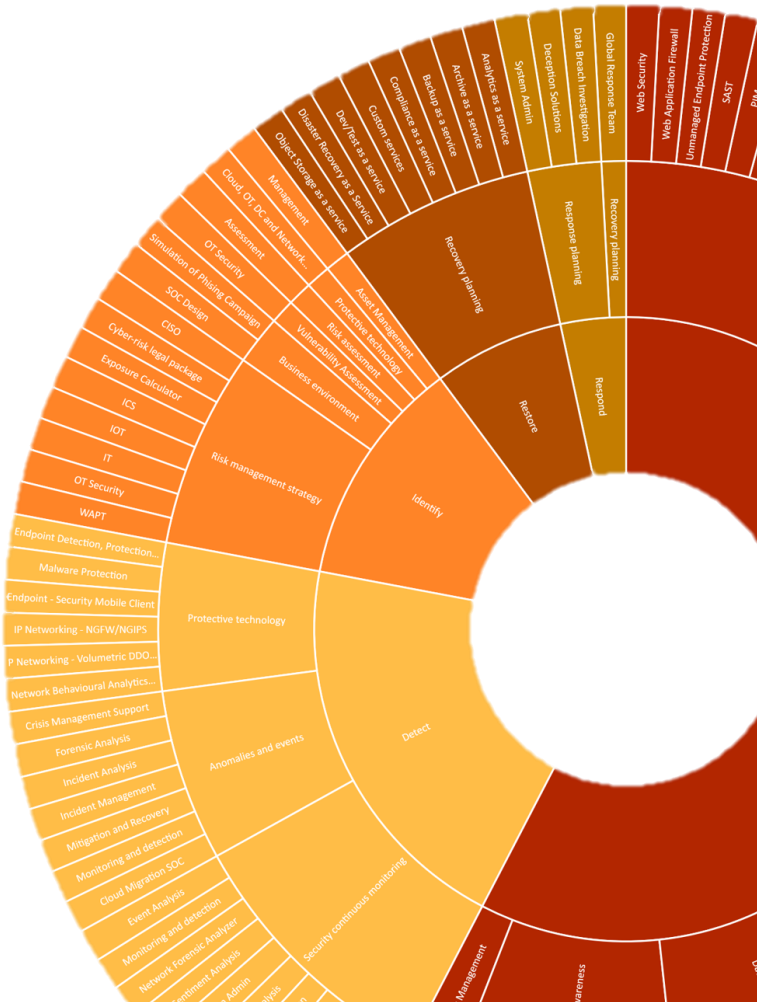
Information sharing - Security is a continuous process requiring the capability to adapt to what attackers are using, evolving continuously. Selecting the proper technology or which process to implement must be integrated with the knowledge of the context, information on the malware and the attack techniques used. Sharing information between people specialized on the defense increases the effectiveness of the investments. Exprivia believes in the value of information sharing and therefore has stuffed a team of Security Researcher (Osservatorio) to analyses incidents, attacks and violations of privacy. The information analyzed are shared every three months with a threat intelligence report, but feeds are available on demand. Furthermore, data collected and analyzed are used to customize the security services Exprivia offer to the market.

Awareness - The most vulnerability exploited by attackers is the human factor. The human is often unaware of the risks and lazy in adopting easy measures that could protect himself by a security incident. The lack of awareness is a consequence of the rapid acceleration in the digitization process that has not given the human being the opportunity to have experiences to build a proper cybersecurity culture. It would take years, experiences on millions of security incidents, to ensure that risk awareness becomes part of the DNA of the human being, but the digitization process is irreversible and non-stoppable. There is a gap that must be closed by working with institutions and schools. Exprivia has a cybersecurity catalog of courses that can be used on demand through a learning platform. The courses aim to transform complex concepts into elements and practices that are easy to use even for not-experts. Exprivia has also developed games that can be used to speed up the learning process (based on the model of "capture the flag".

Services

The services that Exprivia makes available are designed on the security controls of the National Institute for Standard and Technologies (NIST). All services share the data provided by the Cybersecurity Observatory and are divided into:

- **Identify** – The services are including consultancy activities, risk assessments, vulnerability and Penetration Test (VAPT), simulations of malvertisement campaigns to analysis and research of data possibly stolen and exposed on the deep and dark web. The objective is to suggest to customers the processes and controls to reduce the overall risk by optimizing investments.
- **Protect** – Implementation and management security controls focus on protection from incidents, segmentation, micro-segmentation, identity and access management, identity governance, privileged identity management, Static Application Security (SAST) and Dynamic application security testing (DASD), security, obfuscation and masking data at rest and in transit.
- **Detect –** Continuous monitoring using SIEM and sophisticated AI tools capable of identifying the symptoms of an attack before the attack begins.
- **Response** - A security incident should never happen, but if it happens it is better to rely on the hands of experts who can limit and sometimes eliminate the damage. Exprivia has a team that can be hired to respond to a security incident (Global Response Team).
- **Restore** - Restoring a service after an attack is not the same as restoring service caused by bad weather. The GRT can only be used to respond to an attack, but to restore the service.



For all services Exprivia is able to use the most suitable **delivery model**, managing technologies and processes at its customers but also managing the processes and services from its own offices.

Knowledge of Industries

Cybersecurity has general concepts but requires very specific knowledge on the architectures and processes used in the industry.
Exprivia has developed much of its success on the knowledge of industrial processes and architectures and today this knowledge has been made available to cybersecurity services.