Cyber Defense Center

ARICOMA

With our SOC as a Service, which we've named the Cyber Defense Center, you can fully focus on your business growth while we take care of your cybersecurity.

We will provide you with the ultimate solution for managing cybersecurity events and incidents in the form of a service that will, among other things, minimize your response time to security events or incidents and thus reduce potential damage.

Through the Cyber Defense Center, we deliver services consisting of the continuous collection, detection, analysis and investment of security events and incidents. Along with this, we also offer solutions in the form of response and post-incident activities, including recording and communication to the national authorities and other bodies.

Why should you get our security surveillance?

- We provide comprehensive security solutions whether or not you are under attack.
- We are here for you 24 hours a day, 7 days a week, 365 days a year.
- We have independent expertise and experience.
- We monitor and respond in real time.
- We offer help and partnership when you're unsure what to do.
- Flexible and scalable solution architecture to meet your exact needs and requirements.
- We supply exactly what you need, not one-size-fits-all packages. .

Security is our DNA

We monitor

We continuously monitor and identify anomalies and unwanted or malicious behavior in the protected infrastructure in real time. We correlate all the data or information we obtain with each other, using expert technology solutions. We can help you detect not only security incidents, but also configuration errors and cybersecurity weaknesses.

We analyze

We will determine if it is a false alarm, a security event, or security incident that may have an adverse impact on the infrastructure we protect. From false alarms, we create incentives to improve security. Security events and incidents are passed on for investigation.

We investigate

By examining the security incident in detail, we find out exactly what has occurred, identify the impact and the path used by the attacker to penetrate the infrastructure, and gather all the necessary information to be able to determine accurate and adequate response action.

We respond

By responding immediately, we minimize the impact of security incidents. We also help to coordinate the entire response, sending our Cyber Security Incident Response Team (CSIRT) to deal with the incident on site, or just providing a helping hand and guidance on how to deal with the incident.

We improve

After a successful response, we learn from the incident and initiate a series of corrective measures that we then report on based on our findings, in order to raise awareness. We record the incident and help in communicating it to stakeholders and national the authorities.

Our main services include:

- Cyber Security Incident Response Team (CSIRT),
- continuous security monitoring service (SOC as a Service),
- security technology and infrastructure as part of the service,
- Vulnerability Management as a service,
- structured, unstructured, situational or entity-driven Threat Hunting,
- cyber security consulting services.

CDC

Threat Hunting

24/7 Monitoring

INCIDENT RESPONSE

Vulnerability Management

Threat Intelligence