

PLATINUM

C I B E R - S E G U R I D A D

www.platinumciber.com | info@platinumciber.com | Tel. +5411 21283279

SOC - SIEM - CSIRT

Platinum Ciber-Security provides the complete cycle of SOC/CSIRT (Security Operation Center / Computer Security Incident Response Team) services through a team of professionals with experience in cyber-security, with the use of their own tools and third parties that achieve the highest level of service.

We cover the three standard areas of a SOC/CSIRT: a team of highly trained professionals; efficient and proven processes; and appropriate, state-of-the-art technologies. As a differential, our service includes a fourth area: Business Context information.

[GO TO WEBSITE](#)

Prelude is a SIEM (Security Information & Event Management), a security control tool. It collects and centralizes the company's security information to provide a command center, through log analysis and correlation. It also alerts the user of attacks and intrusion attempts to the system in real time.

Prelude offers a variety of big data research and reporting tools to identify weak signals that may appear as Advanced Persistent Threats (APT). Finally, Prelude has all the tools to assist and facilitate operator work and risk management.



BUSINESS CONTEXT

We consider that the company's business context information is fundamental when making decisions about asset protection measures. Our experience of more than 10 years in the market developing risk analysis, allows us to offer this unique additional component for a SOC/CSIRT, of great value when establishing the necessary protective measures and actions.



PROCESSES

We have proven and efficient processes in the definition of a SOC/CSIRT in daily operation, defining subprocesses of preparation, identification, containment, eradication and recovery, immersed in a scheme of continuous improvement. Likewise, our operational processes are optimized to have visibility into the cyber-environment of the company, analysis of events and rapid and adequate response actions.



OUR TEAM

We have extensive experience in carrying out the tasks of the SOC/CSIRT. From the most basic tasks such as monitoring alerts or triage, to the most advanced ones such as analysis, correlation and threat hunting.



TECHNOLOGY

Our partnership with the company C-S® that produces SIEM Prelude® allows us to have the latest technology to meet the requirements necessary in today's cyber-environment, which we complement with other components to provide the precise service that our customers need.