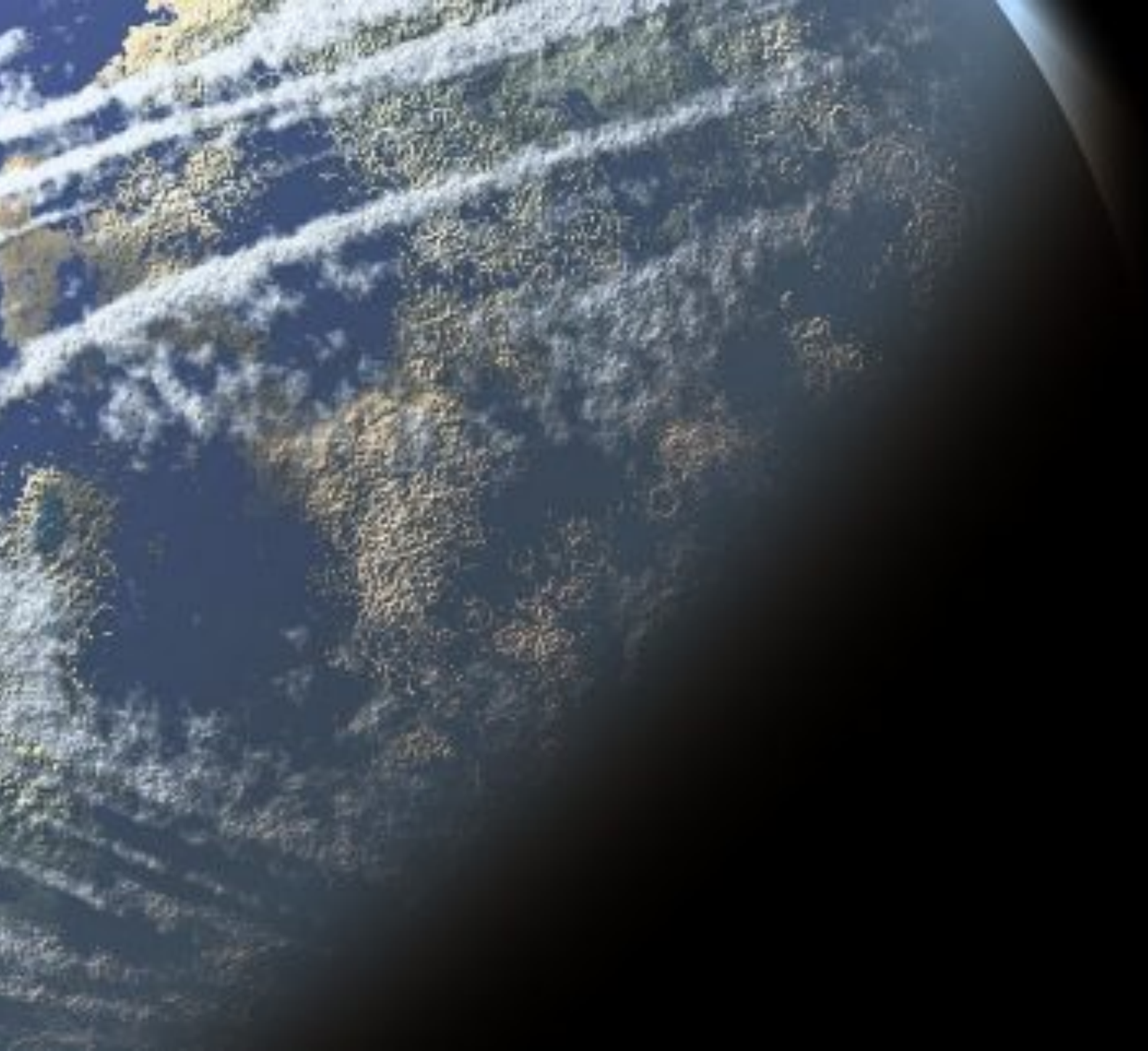

ASPEN

NG SIEM Platform

With cyber-attacks on the rise, companies are transforming their approach to security monitoring **from reactive towards intelligence-driven security**. We can help you empower your security teams, and your business, to perform better in the digital world with a **N**ext-**G**eneration Security Information and Event Management (**SIEM**) platform and Security Operations Centre (**SOC**).

Proud of our team and solution

Built by a team of security professionals with **20+ years** of experience in cyber threat prevention, **ASPEN** is a leading next-gen **SIEM** (Security Information and Event Management) solution that brings features for security data collection, analysis and automated threat remediation.

We operate globally

(team&product references over the years)

Greece for Olympic Games
Italy for Olympic Games and Telecom Operator
China for largest ever Olympics
Singapore for Youth Olympic Games
Malaysia for regional ATOS SOC services
Poland for Global Siemens Security Operations
Kazakstan for TSC Corporation (banking, insurance)
Serbia for Government of Serbia
Thailand for commercial SOC services

ASPEN CAPABILITIES

ASPEN creates digital clones as active traps
ASPEN performs both historical and real time (<5ms) correlation
ASPEN offer visual reconstruction (“forensics on a click”)
ASPEN do data anonymisation and pseudonymisation in real time
ASPEN performs real time correlation with Threat Intelligence data
ASPEN integrates with 80+ anti-viruses
ASPEN performs automatic noise events elimination
ASPEN offer real time auto remediation

ASPEN KEY FEATURES

Deception: a trick or scheme used to force an attacker to think he is accessing real assets in order to confuse him and detect his action. We provide traps at every possible step of an attacker, from traps deployed at external services to traps deployed at internal memory of every workstation or IoT device

Threat intelligence: evidence-based knowledge, including context, mechanisms, indicators, implications, and action-oriented advice about an existing or emerging menace or hazard to assets. Threat Intelligence is the process of gathering information about cyber attacks around the world for purpose of recognising similar attacks against your customers

Cyber security monitoring&surveillance: real-time visibility into an organisation's security, by constantly monitoring of people, processes, systems and network events and performing real time correlation with external and internal data for purpose of detection of cyber security incidents

Auto remediation: responds to security events with automations able to fix, or remediate detected cyber attack

Automated penetration testing: penetration testing performed by artificial intelligence algorithms, using knowledge based on attack vectors and exploits collected from our traps

SERVICES

System Analysis: Our cyber security team will examine every nook and cranny of your IT environment in order to understand the architecture of your systems, pinpoint weaknesses and offer recommendations on how to redesign the systems.

Vulnerability Assessment and Penetration Testing: Our RED Team of ethical hackers will simulate real-world attacks to test the vulnerabilities in your IT environment. We will identify security gaps and flaws in your business-critical systems, as well as their potential impacts. Afterwards, we will create a report with detailed information about your weak spots and recommendations for improvement

System Dimensioning and Planning: Working closely with you, our team will rank critical indicators according to importance and will implement event correlation rules. During this stage, we will create an estimated timeframe for ASPEN implementation

Implementation and Go-live: The implementation of ASPEN includes a number of different steps, which will vary based on the number of correlation rules and the client's needs

Monitoring: After go-live, our team of security analysts will provide 24/7 monitoring of your IT systems. This includes end-to-end monitoring, incident alerts and reporting based on real-time log data. Depending on your requirements, we can also help you set up automated responses to specific security incidents

User Training and Development: The end-user training is a fundamental step in any SIEM implementation. The goal is educating users about ASPEN - its threat intelligence, forensics, digital traps and threat remediation capabilities. You can benefit on various types of education on demand, including cyber awareness and cyber analytics training

BUSINESS MODEL

SOC can be operated by us or by one of our local partners or, on-prem, by the client's team

We combine **ASPEN** with its **SOC** (**S**ecurity **O**perations **C**entre) services to a solution that addresses the widest spectrum of internal and external threats organisations face today

Any **SOC** that is not operated by us benefits on:

- our high quality services
- ASPEN platform and continuous updates
- Key security experts as needed
- professional trainings