LAYER8

Team Introduction

67th TF-CSIRT Meeting

28-29 September 2022

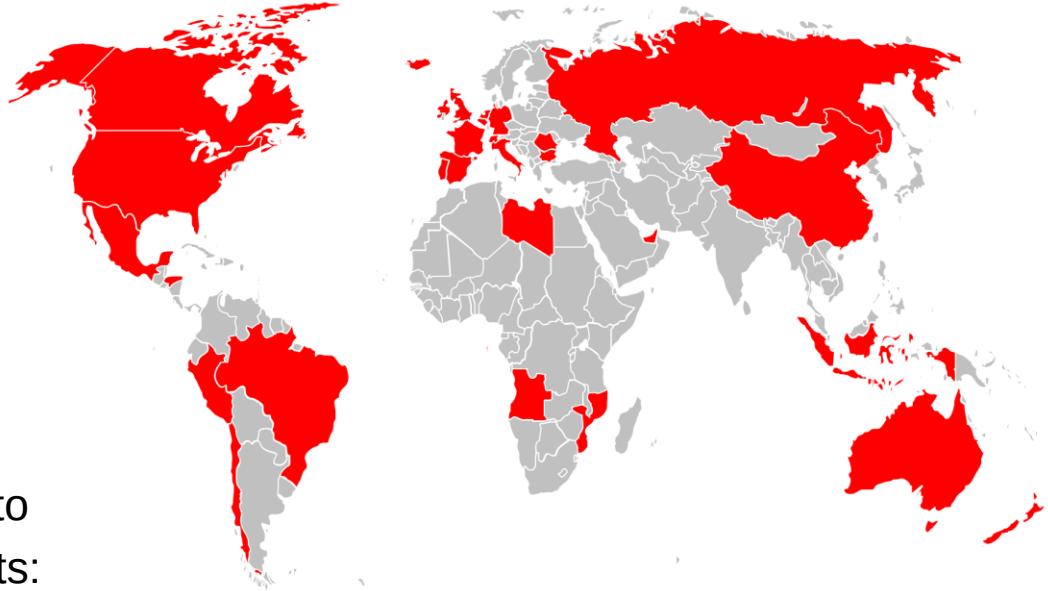
Vilnius

TLP:CLEAR

LAYER8 is a Portuguese company incorporated in November 2011 totally focused in the Information Security and Compliance Management business.

Some info about the company:

- ~80 employees
- +350 clients
- Projects in 5 continents
- +10M€ revenue
- 3 business units
- 1 R&D center
- Lack of imagination when it comes to inventing names to our own products:
  DNS8 LEARNING8 VULN8 FISH8 SOC8



CONSULTING

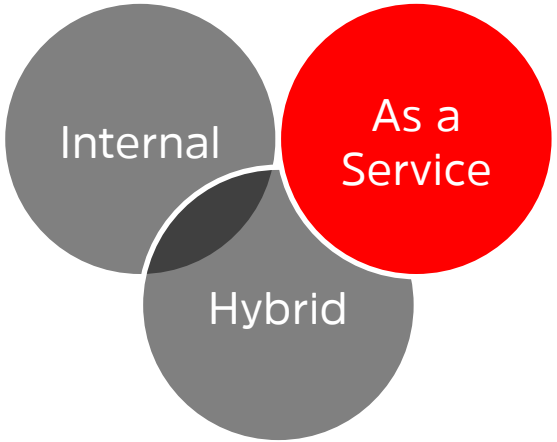
TECHNOLOGY

MANAGED SERVICES

R&D

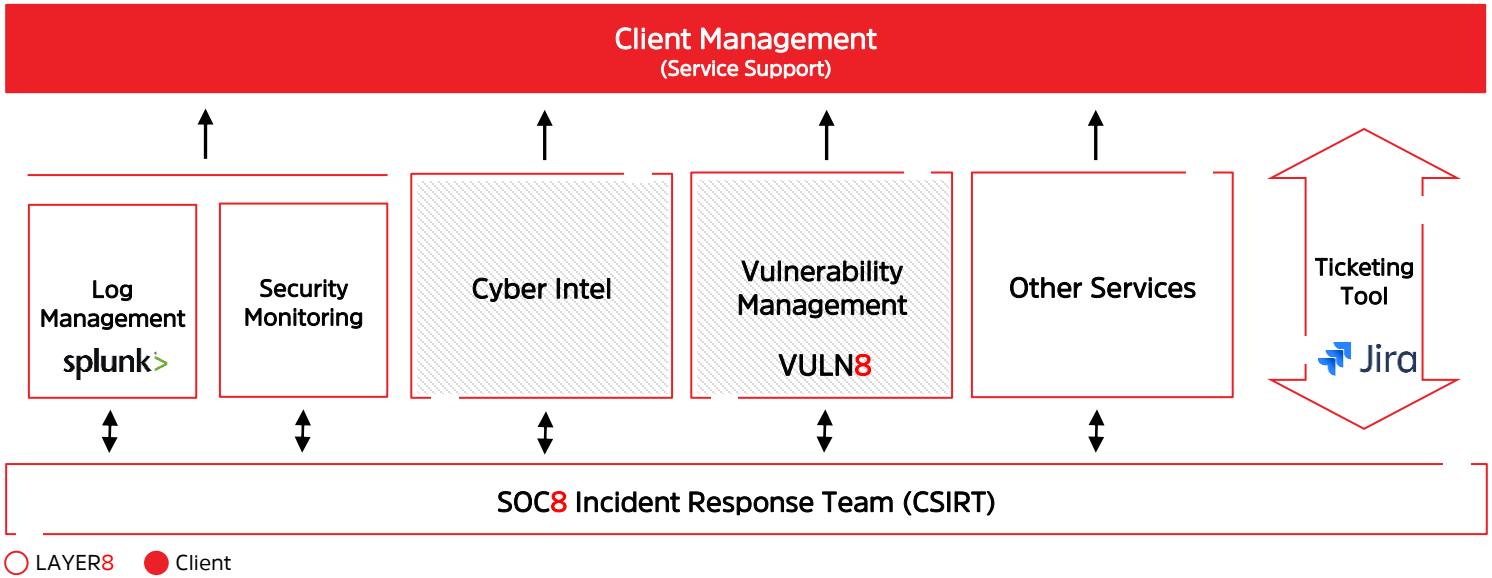
SOC8 Service Model

The CSIRT service can be provided in 3 different models. The service can be managed and executed internally in the Organization, can be provided “as a service” by an external supplier that is responsible for the Operation and Management or, by an hybrid model of the last two.
In recent years, LAYER8 has participated in several projects with different service models, gaining relevant experience in all of them.



SOC8 Service Components

Our CSIRT-as-a-service model encompasses a set of capabilities typically distributed between **LAYER8** and the Client, from continuously monitoring of infrastructures and services to Cyber Threat Intelligence and Vulnerability management.



LAYER8
PROTECTING YOUR BUSINESS

SOC8 Team

Our service is composed by a senior service **coordinator**, an **engineering** team and an **operations** team with TIER1 and TIER2 analysts. A DFIR team ensures Forensics and TIER3 requirements. In addition, a DEV-OPS team provides Automation and Optimization support.

ENGINEERING & DELIVERY

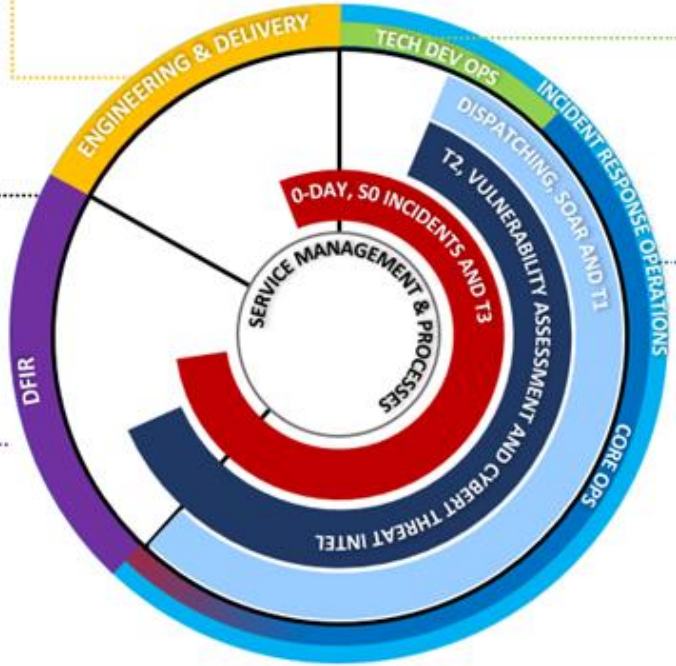
- SIEM & Log Management Projects
- T3 and Forensics Support
- Infrastructure Maintenance
- Blue Team Support
- Use Cases Integration and Optimizatio
- DR and Backups

SERVICE MANAGEMENT & PROCESSES

- Service Management
- Team Management
- Pre-Sales
- Service Reporting
- SOC Framework and Processes

DFIR

- Forensics
- T2/T3 Support
- SOC Assessment and Processes
- S0 / 0-Day Management



TECH DEV OPS

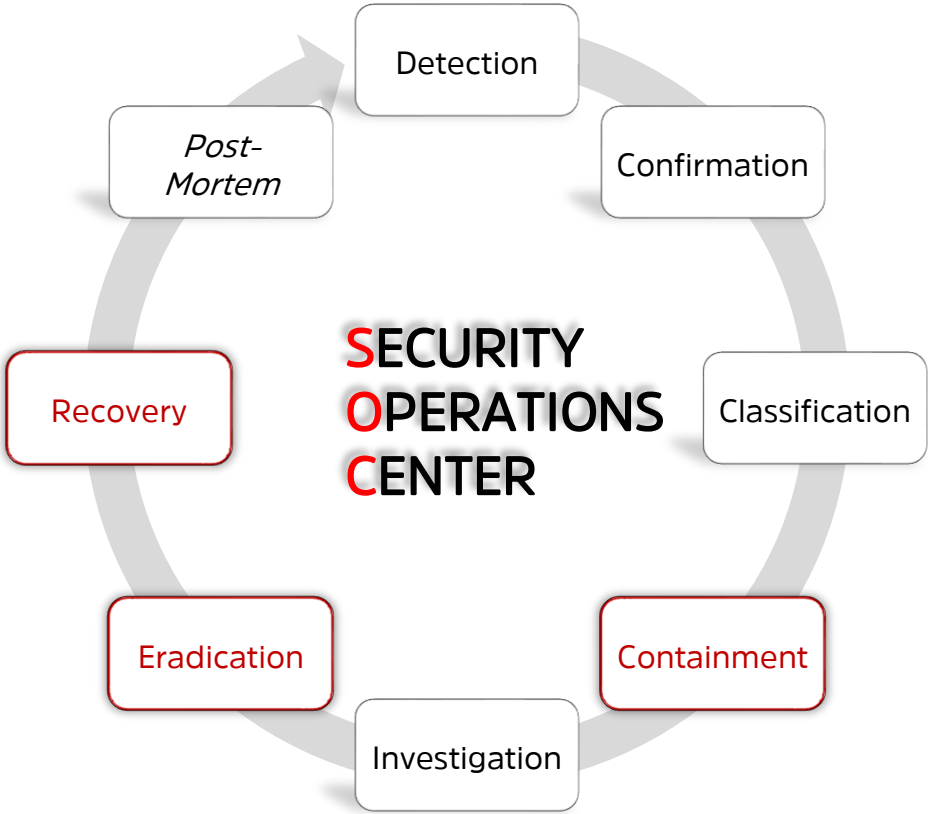
- Use Cases Automation
- Scripting
- Tasks Optimization

CORE OPS

- T1 / T2
- Vulnerability Assessment
- Cyber Threat Intel
- Use Cases Definition and Maintenance
- Client Management

LAYER8
PROTECTING YOUR BUSINESS

SOC8 Incident Lifecycle



1. **Detection** - a Security Incident can be generated automatically or manually (analyst detects anomalous behaviour);
2. **Confirmation** – Screening of alerts and confirmation whether it is a false positive or effectively a Security Incident;
3. **Classification** – According to the Incident and Impact type, a Category and Incident Severity are confirmed;
4. **Containment** – Recommendation of measures to minimize the impact of the Incident;
5. **Investigation** – Analysis of existing information in order to assess the Root Cause of the Incident, the correct measures of Eradication and the entire Impact Analysis;
6. **Eradication** – Recommendation ot the measures to be applied to eliminate the Root Cause of the Incident;
7. **Recovery** – Recovery of affected systems, if any.
8. ***Post-Mortem*** – Report where all evidences of the Incident are compiled. This report also includes a set of measures that will allow the Client to prevent, monitor and act in similar situations.

LAYER8
PROTECTING YOUR BUSINESS

SOC8 Incident Taxonomy

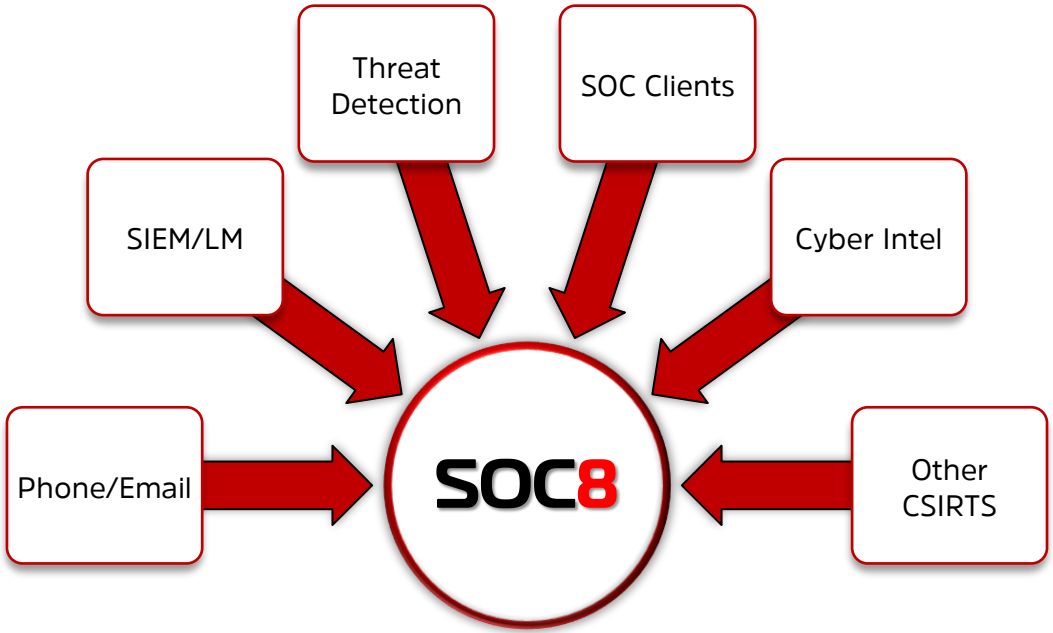
LAYER8 is a member of the Portuguese National CSIRT Network and uses the European Union Agency for Network and Information Security (ENISA) Incident Classification Taxonomy.

Category	Subcategory
Malicious Code	Infected System
	C&C
	Malware Distribution
	Malware Configuration
Abusive Content	SPAM
	Harmful Speech
	Child / Sexual / Violence / ...
Availability	Denial of Service
	Distributed Denial of Service
	Service Interruption
	Sabotage
	Outage (no malice)
Fraud	Unauthorized use of resources
	Copyright
	Masquerade
	Phishing
Intrusion	Privileged account compromise
	Unprivileged account compromise
	Application compromise
	Bot
Other	Other

Category	Subcategory
Maintenance	Maintenance
	Configuration
	Internal
	Other
Privacy	Data Leak
	Data Subject Requests
Information Gathering	Scanning
	Sniffing
	Social Engineering
Information Security	Unauthorized Access
	Unauthorized Modification
	Data Loss
Intrusion Attempt	Vulnerability Exploitation
	New Attack Signature
	Login Attempt
Vulnerability	Weak Criptography
	DDoS Amplification
	Undesired accessible services
	Information Disclosure
	Vulnerable System
Other	Undetermined

SOC8 Incident Sources

Being a Security Incidents Detection and Response service SOC8 can be activated on proactive and reactive ways. Tickets to the service can be created automatically through a Security Event launched by SIEM, proative monitoring using Cyber Threat Intel feeds, by phone or email or by participating Entities.



LAYER8
PROTECTING YOUR BUSINESS