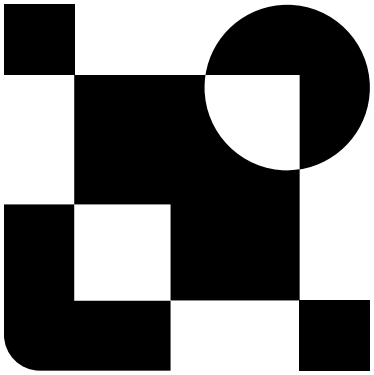
CWATCH ON CHRONICLE SOAR

Managed Cyber Security Services



All companies, whatever their size and activity, are now regularly confronted with cyber-attacks and must be prepared, deploy an active defense, adapted to constantly evolving threats and information systems, and know who to count on in case of a major incident.

CWATCH services are the **managed SOC/CERT** services delivered by Almond, based on **Chronicle SOAR**, aimed at anticipating, deploying an active defense adapted to constantly evolving threats and information systems and being at your side in case of a major incident.

CWATCH SERVICES

Anticipate and protect

- **Anticipate the threats** that concern you and prepare yourself
- **Reduce the attack surface** and vulnerabilities
- **Identify adversaries**, prepare crissi mangement and good security posture

Detect cyberattacks

- SOC CWATCH based on **Chronicle SOAR**
- Monitor and detect **attacks early**
- **External monitoring and vigilance**

Respond to security incidents

- **CERT CWATCH**
- **Respond to major security incidents** and restore your operations in the best conditions

OUR KEY FIGURES

SOC and CERT since 2016. Member of InterCERT-FR since 2020

Team of 30 analysts in France (all N1/N2/N3) in rotation by shift SOC/CERT

More than 80 customers billed in 2022 for protection, detection and incident response activities

CHRONICLE SOAR BENEFITS

01. One dedicated environment per customer

02. Automation on remediation for rapid response

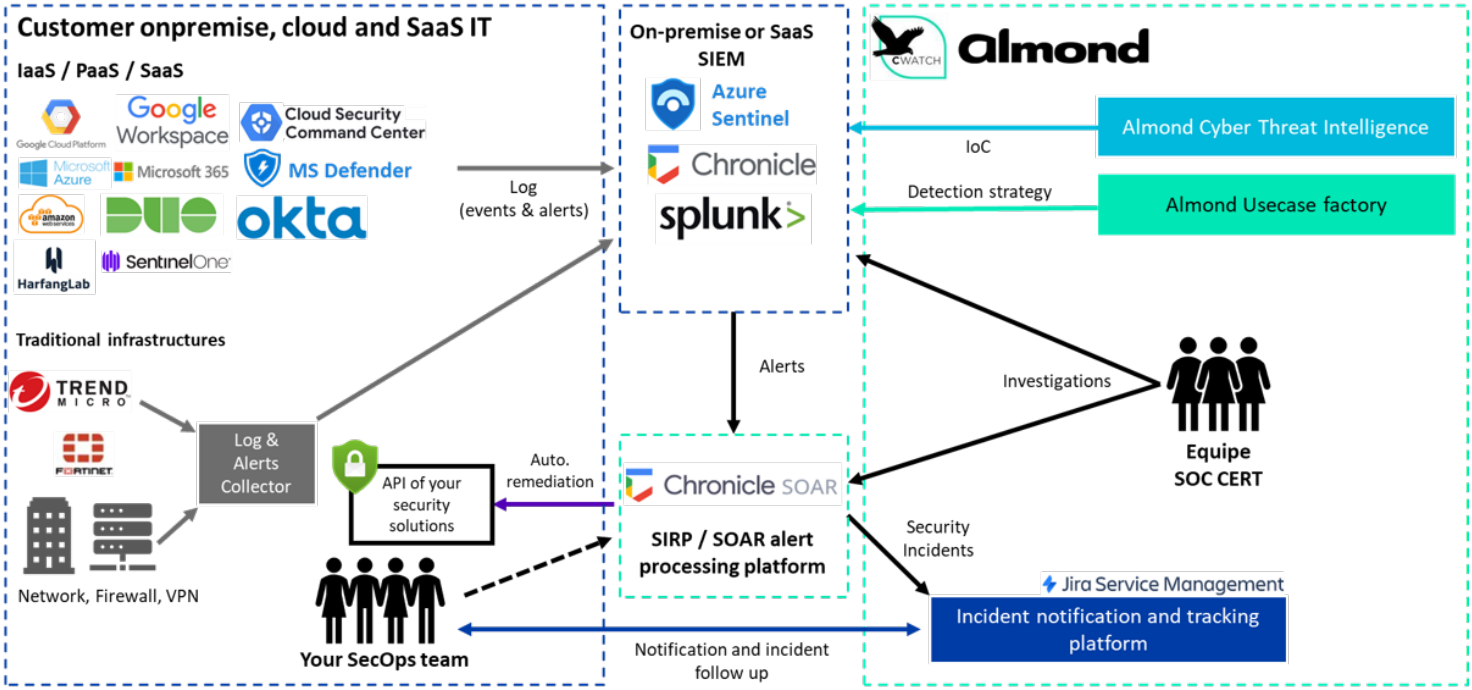
03. Possible access to Chronicle SOAR by our customer (Managed User License)

contact@almond.eu
www.almond.eu

CWATCH ON CHRONICLE SOAR

Managed Cyber Security Services

ARCHITECTURE



CWATCH SOC/CERT MANAGED SERVICES

SERVICES MANAGÉS

ANTICIPATE

- Cyber defense program consulting
- Threat intelligence and risk assessment (Ebios RM) with GRC experts
- Phishing campaign
- Security awareness and crisis management exercises
- Participation in redteam / purpleteam audits
- Continuous assessment (Security Rating)

PROTECT

- Vulnerability scanning and managed vulnerability scanning
- Optimization of the security functions of solutions (WAF, IDS/IPS, EDR...)

DETECT

- External Vigilance Services
  - Detection of security events on your external technical assets
  - Detection of usurpation of your legitimate assets
  - Detection of exposure of sensitive information on the Internet
- Internal attack detection service
  - Monitoring and detection by log correlation / SIEM
  - Log collection / entralization on local or shared Almond datalake

RESPOND

- Intervention on request of the CERT
  - Response to a major incident
  - Forensic
  - Reverse engineering of malware
  - Research of compromise
  - Crisis management
- Implementation and operation of dedicated internal CSIRTs
- Automated response solutions

contact@almond.eu
www.almond.eu