Atea SOC

What is it?
Do I need one?

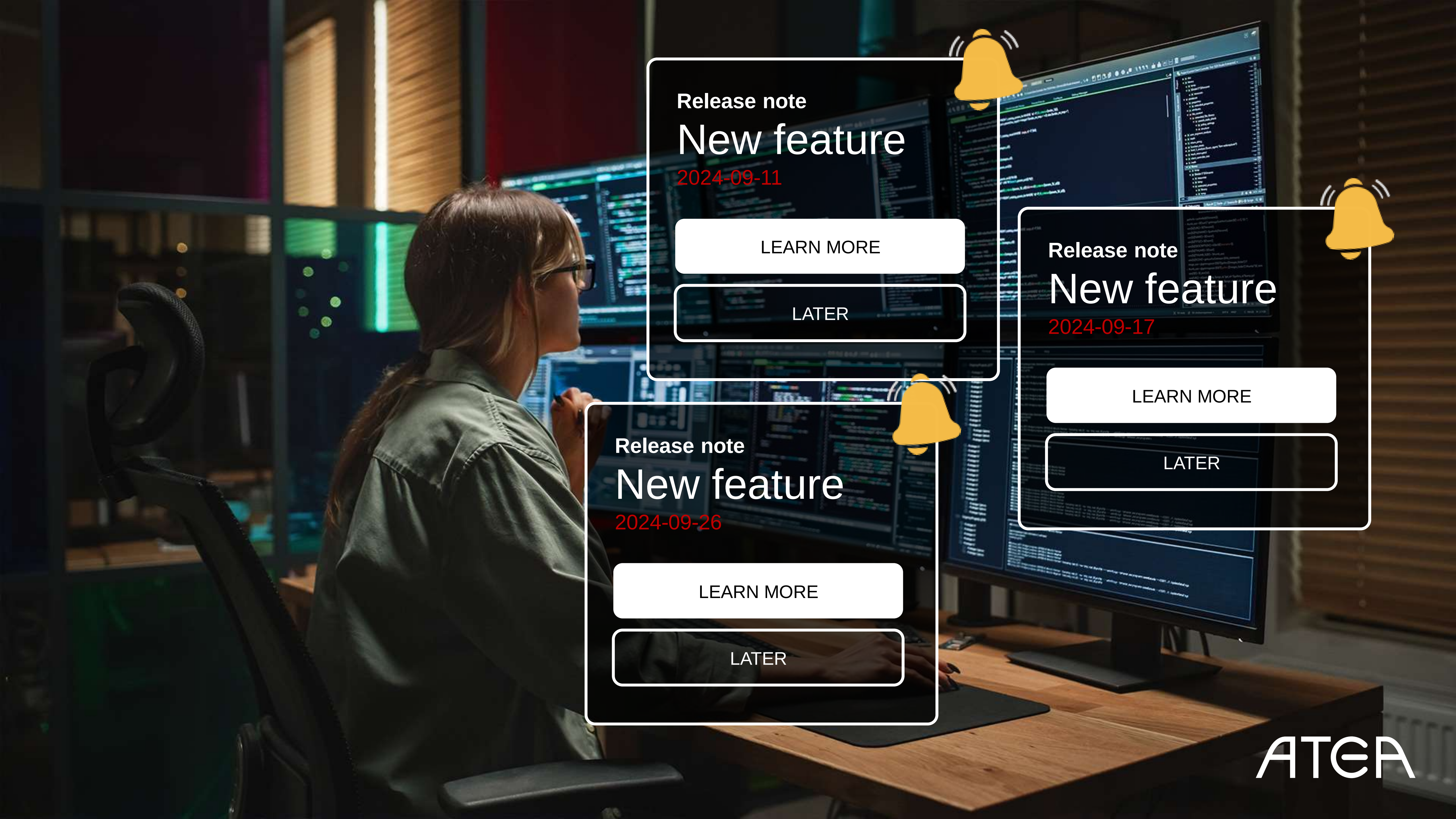
Christian Nordve

Head of Security offering AMS

On
SOS

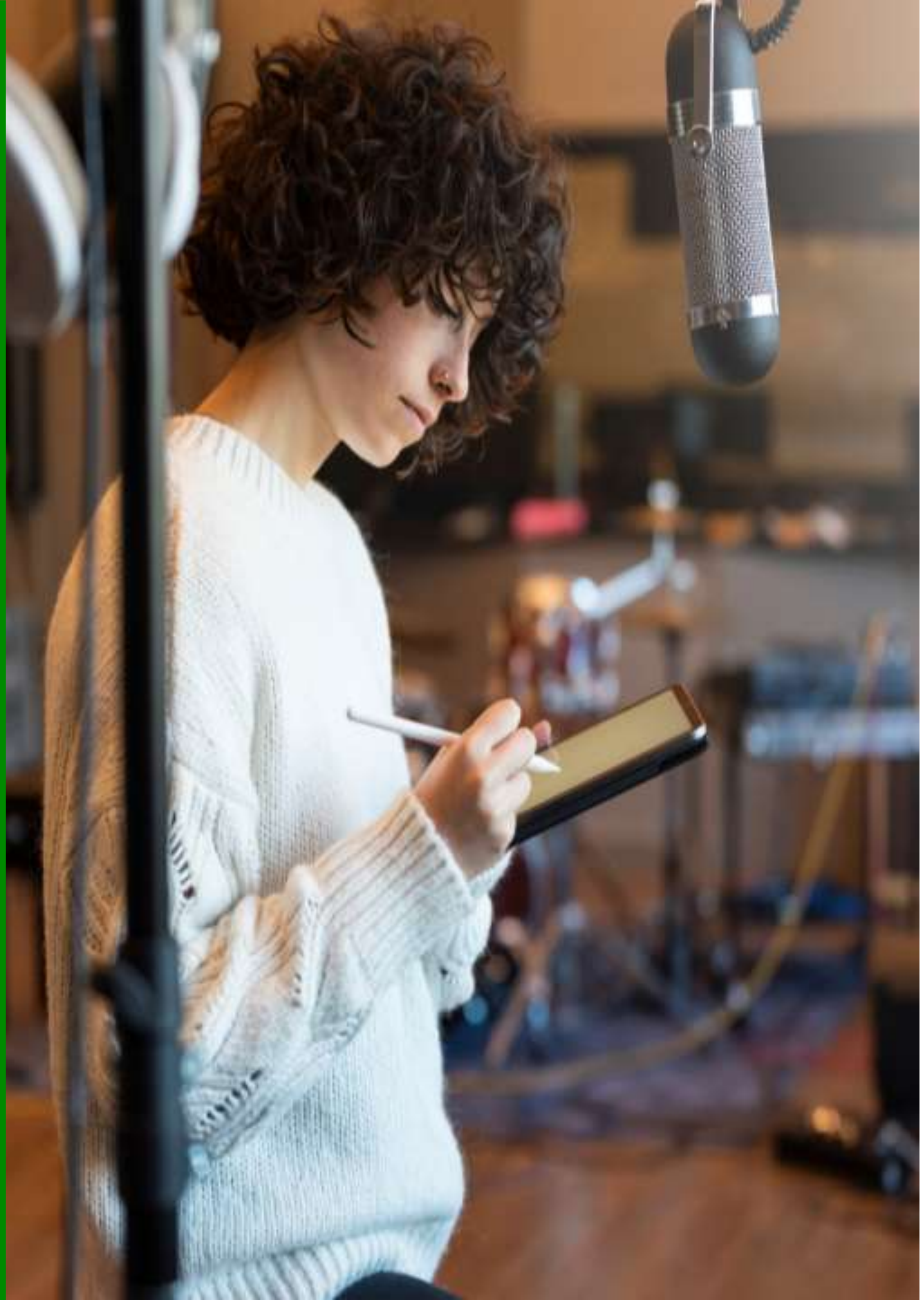
OpenAI

watsonx


Release note
New feature
2024-09-11
LEARN MORE
LATER
Release note
New feature
2024-09-17
LEARN MORE
LATER
Release note
New feature
2024-09-26
LEARN MORE
LATER

SOC

Monitoring Security incidents in real time to detect and react fast



The purpose with the **SOC+** service is to be **proactive and detect** possible cyber attacks and **minimize the time** from an attack is detected at a customer and helping them to **isolate, stop and investigate** the attack.

ATEA

Facts about Atea SOC service

3 main locations

100+
customers

Service Desk
10+ languages
7 locations

Secure 24/7
Service

Approx 50
employees

ISO
9001

ISO
14001

ISO
27001

ISO
37001

Atea SOC+

Project Management

- Pre-meeting
- Expectations
- Delivery details
- Clarifications
- Project plan
- Project meetings

Data collection

Brings together security logs and user behavior from on-prem, hybrid and cloud solutions

Detection tools

Uses XDR, SIEM / SOAR to detect abnormal events and activity in real time.

Security Operation Center (SOC)

Analysts monitor alarms, evaluate threats, automated response and take immediate action 24/7/365

Incident Response Team (IRT)

Responds to limit damage, remediate and restores to normal operation

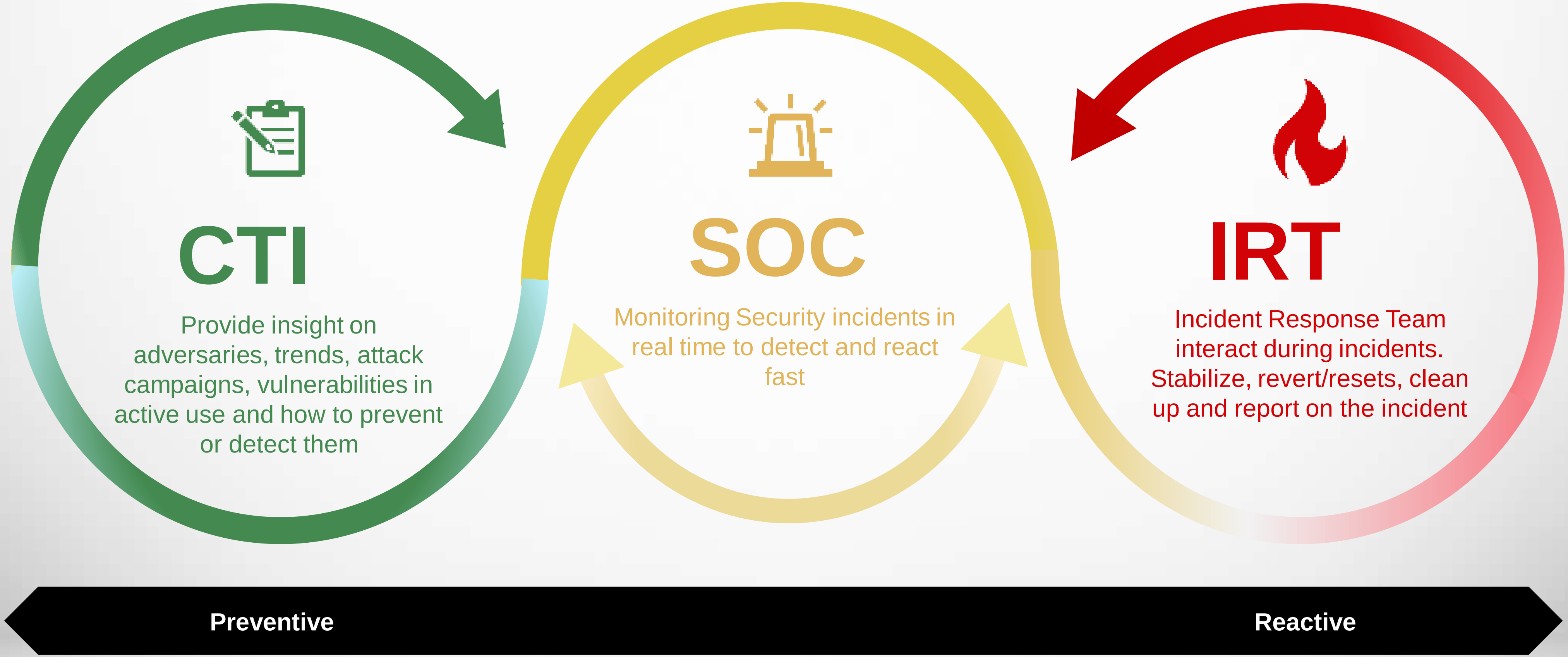
HyperCare

2 weeks of extra close follow-up after Go-Live

Customer Succsess (CSA)

Monthly customer meetings, reporting, improvements and updates

Project Management



CTI

Provide insight on adversaries, trends, attack campaigns, vulnerabilities in active use and how to prevent or detect them

SOC

Monitoring Security incidents in real time to detect and react fast

IRT

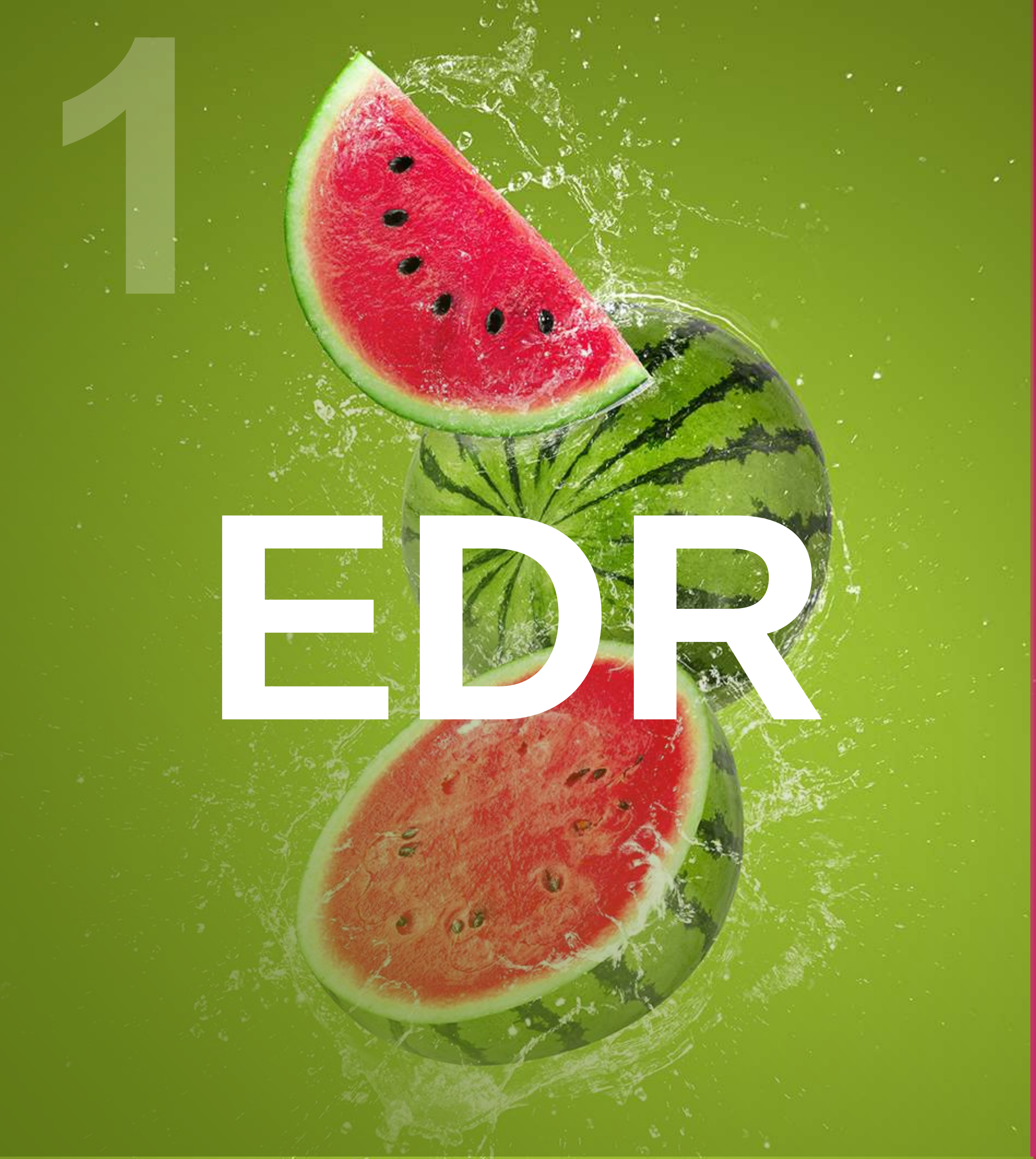
Incident Response Team interact during incidents. Stabilize, revert/resets, clean up and report on the incident

Preventive

Reactive

Atea Managed Endpoint Security

- Optimized configuration on your solution
- Update on Configuration over time
- Surveille and analysis of incidents and alerts
- Automatic incidents handling
- Competence



1

EDR

2

XDR

Automatic response

Automatic action on unwanted behavior
A combination of playbooks and personnel
Damage limitation

EDR:

- Isolate client and perform an AV scan

XDR:

- EDR +
- Isolate sender, force password change
- Isolate user and block IP
- Block app and deny access

Peace of mind and time to focus on other stuff…