Trap attackers.
Detect them early.

A proactive detection layer, operated by the Abilene SOC, that exposes intruders inside your environment with high-confidence signals.

Use cases

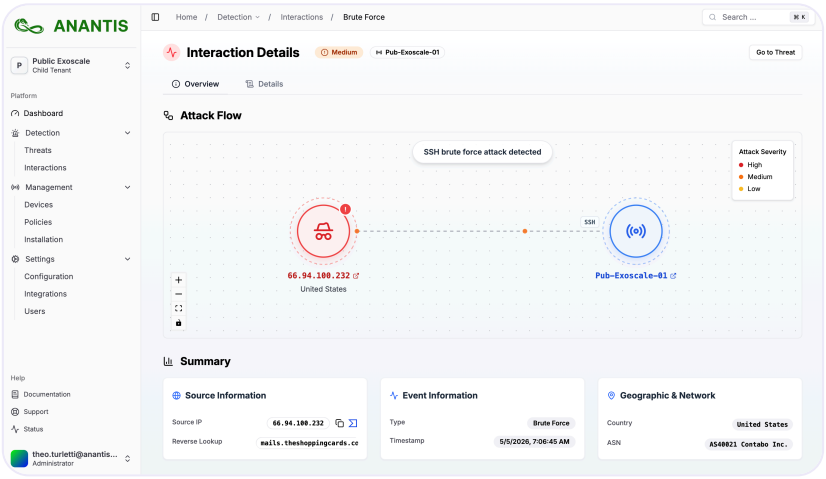
Attackers often remain inside compromised environments for days or weeks before detection. Deception adds dedicated detection points inside the environment, so reconnaissance and lateral movement are exposed before they turn into an incident.

The service is designed for organisations operating sensitive or high-value environments, particularly in the **financial**, **industrial** and **healthcare** sectors, where early detection is essential. It shifts the security posture from reactive to proactive, and complements existing SOC and security capabilities.

The solution

Abilene's Managed Deception Service combines **Anantis TrapEye** with Abilene's SOC capabilities. Realistic decoys and services are deployed across IT and OT environments. As these assets play no part in normal business operations, any interaction with them is a high-confidence indicator of malicious activity.

1. **Deploy:** Abilene places decoys where an attacker would look first, without agents on production systems.
2. **Detect:** Reconnaissance, unauthorised access, credential misuse and lateral movement raise an immediate alert, mapped to MITRE ATT&CK®.
3. **Respond:** The Abilene SOC qualifies the alert and escalates it through your incident response process.



MEDIAN DWELL TIME

14 days

How long attackers stay undetected inside a compromised environment.

Mandiant M-Trends 2026

Service features

Deployment

- Assessment of the environment and selection of decoy locations
- Deployment and configuration across IT and OT

Detection & investigation

- Continuous monitoring of decoy interactions
- SOC investigation and qualification of alerts
- Escalation through your incident response process

What's included

- Initial deployment and configuration
- Ongoing monitoring and service management
- Decoy tuning and optimisation
- Regular reporting and service reviews

Powered by TrapEye

ANANTIS

Developed by **Anantis**, a Swiss company specialising in deception-based threat detection, founded by experienced red teamers. Agentless, integrated with your SIEM, with infrastructure and data hosted in Switzerland.

FAQ

Where can decoys be deployed?

On-premises and in the cloud, as virtual machines, or on distributed infrastructures as containers.

Who handles the alerts?

The Abilene SOC investigates and qualifies every alert, and escalates confirmed incidents through your response process.

Schedule a demo | contact@abilenesolutions.ch
Geneva: Rue de Carouge 28, 1205 Geneva · +41 21 512 1030
Lyon: 16 rue Cuvier, 69457 Lyon 06 · +33 4 12 37 98 93
www.abilenesolutions.ch