

BLUEPRINT

Anomaly Detection

Catch what rules and signatures can't see.

Modern attacks often don't use known malware. An attacker logs in with stolen credentials, moves through the network like a regular user and exfiltrates data slowly and quietly. That's why anomaly detection doesn't just look for known patterns – it looks for deviations from normal behaviour.

How it works

- we collect data on network traffic and on the behaviour of users, devices and applications
- this builds a picture of what normal looks like in your environment
- the system flags unusual deviations – a login at an odd hour, a new communication pattern or an unexpected volume of data leaving the network
- every alert comes with context, so it can be quickly assessed as a real threat or not

What it can uncover

- misused or compromised accounts
- attackers moving laterally inside the network
- data leaks and unauthorised transfers
- infected devices communicating with an attacker
- misconfigurations and unexpected changes in traffic

What you get

- early warning even for attacks that have no signature yet
- visibility into what is really happening on your network
- fewer blind spots between your other security tools

AI

AI in practice Machine learning learns what normal traffic looks like and flags deviations that fixed rules would miss.

Who it's for organisations whose data and operations are a target and who need to see beyond the network perimeter.

Let us show you what's happening on your network.

info@anomalis.cz · +420 603 106 456 (24/7 for urgent cases) · www.anomalisit.cz

Anomalis IT s.r.o. · Korunní 2569/108, 101 00 Prague 10, Czech Republic · Company ID 09717404 · VAT ID CZ09717404