

## Semperis and Trellix Partner to Accelerate Cyber Breach Containment

Semperis and Trellix bring unprecedented visibility into the identity system with comprehensive extended detection and response (XDR), significantly reducing time to detect and contain attacks involving Active Directory (AD) and Entra ID.

Semperis adds rich, ML-based contextual identity attack intel and continuous threat monitoring to Trellix's best-in-class XDR platform, along with powerful change tracking, auto-rollback, and recovery capabilities. Our joint solution takes a layered approach, mitigating risk at each step of the kill chain.

## **How It Works**

Here's a simple integration use case to illustrate the power of seeing from the endpoint and the identity system:

1

Trellix identifies an infected workstation and sends loggedin identities to Semperis 2

Semperis pulls forensics to see all activities performed by the compromised identities in the IDP(s), disables accounts, and reverts malicious changes

3

Semperis detects password spraying, Golden Ticket attacks, and other IOAs 4

Semperis sends workstation details to Trellix to quarantine 5

Semperis maps service accounts to servers, so Trellix blocks, and Semperis disables, accounts trying to log in from an unauthorized machine

"When an endpoint such as a workstation is compromised, Trellix's XDR provides critical information about endpoint attacks, including who was logged in when the incident occurred. From that point, Semperis DSP can analyze forensics data of changes made to the identity system, follow the path of activities made by the compromised account, and automatically undo those changes, dramatically reducing response time."

MICKEY BRESMAN Semperis CEO LEARN MORE

