



SECURING DATA WITH AGENTIC AI

AUTOMATIC VULNERABILITY DETECTION

SEP. 2026

ANDRÉ LEAL | INNOVATION LAB

RAFAEL FERREIRA | CYBERSECURITY

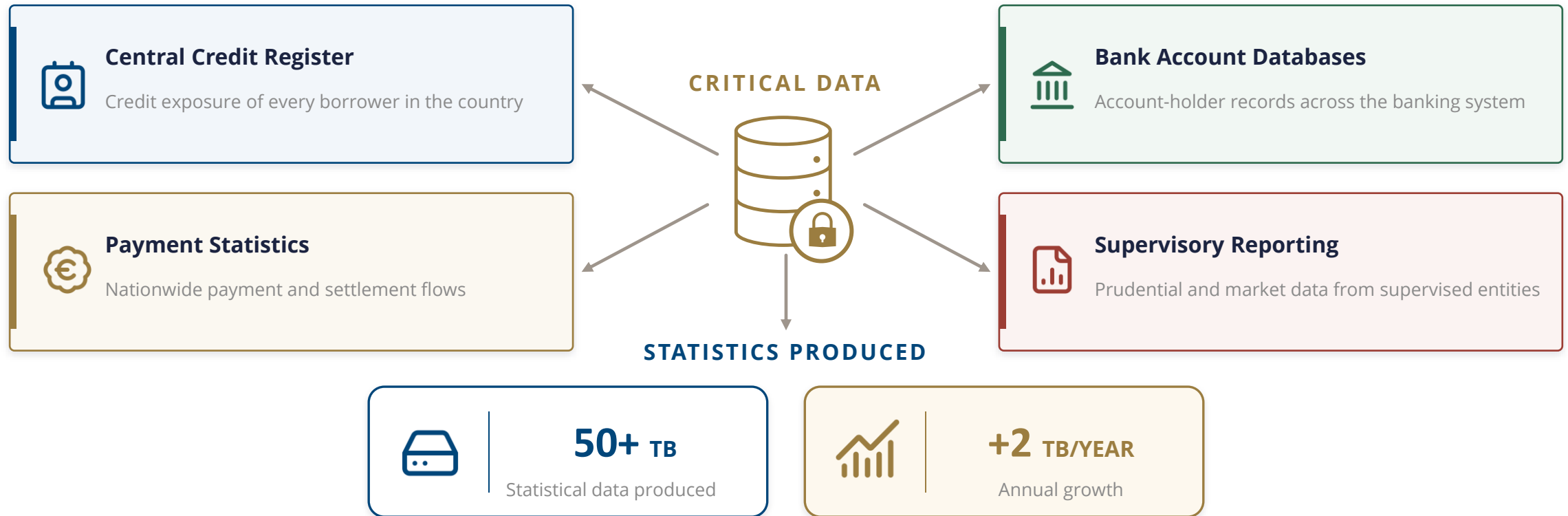


BANCO DE
PORTUGAL
EUROSISTEMA



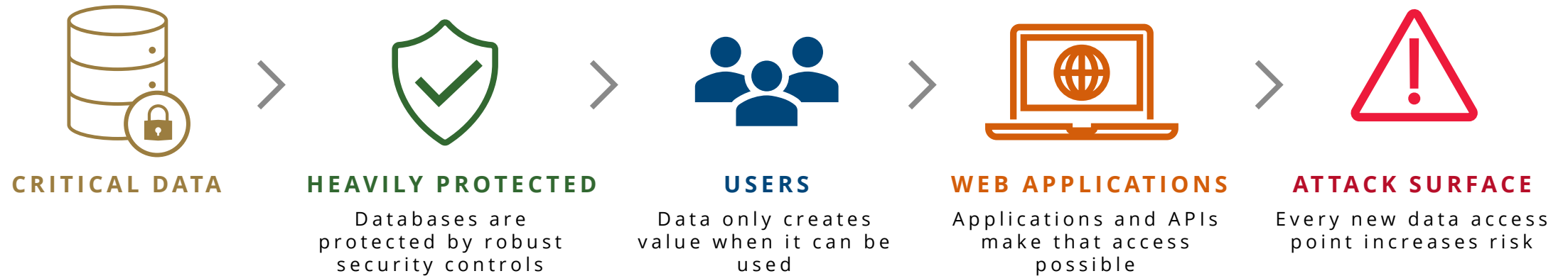
PROTECTING OUR MOST VALUABLE ASSET

Banco de Portugal is no exception — and the data it holds is among the most critical in the country.





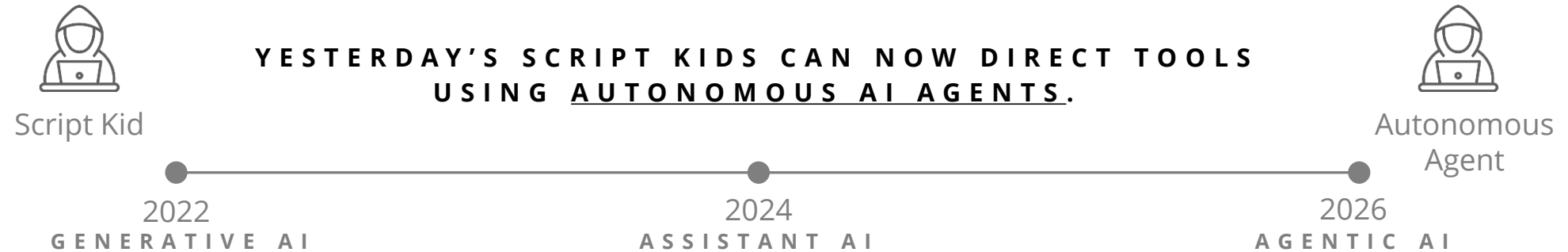
PROTECTING OUR MOST VALUABLE ASSET



The challenge is not only protecting data
It's ensuring every exposed application is secure



AI ACCELERATES THE CYBERTHREAT



BEFORE AI

-  Skilled, specialized attackers required
-  Manual reconnaissance and exploitation
-  Human-paced
-  Limited number of simultaneous targets

WITH AGENTIC AI

-  Any actor can launch sophisticated attacks
-  Automated scanning and exploitation without fatigue
-  24 / 7 / 365 continuous operation
-  Thousands of targets tested in parallel



AI CHANGES THE CYBER-RISK EQUATION

The threat landscape has evolved — but our defences haven't scaled to match.



Attack Surface

70 / 180

180 total enterprise applications, with 70 directly exposed to the internet.



Financial Cost

€130,000

Traditional testing models become increasingly expensive at scale.



Human Limits

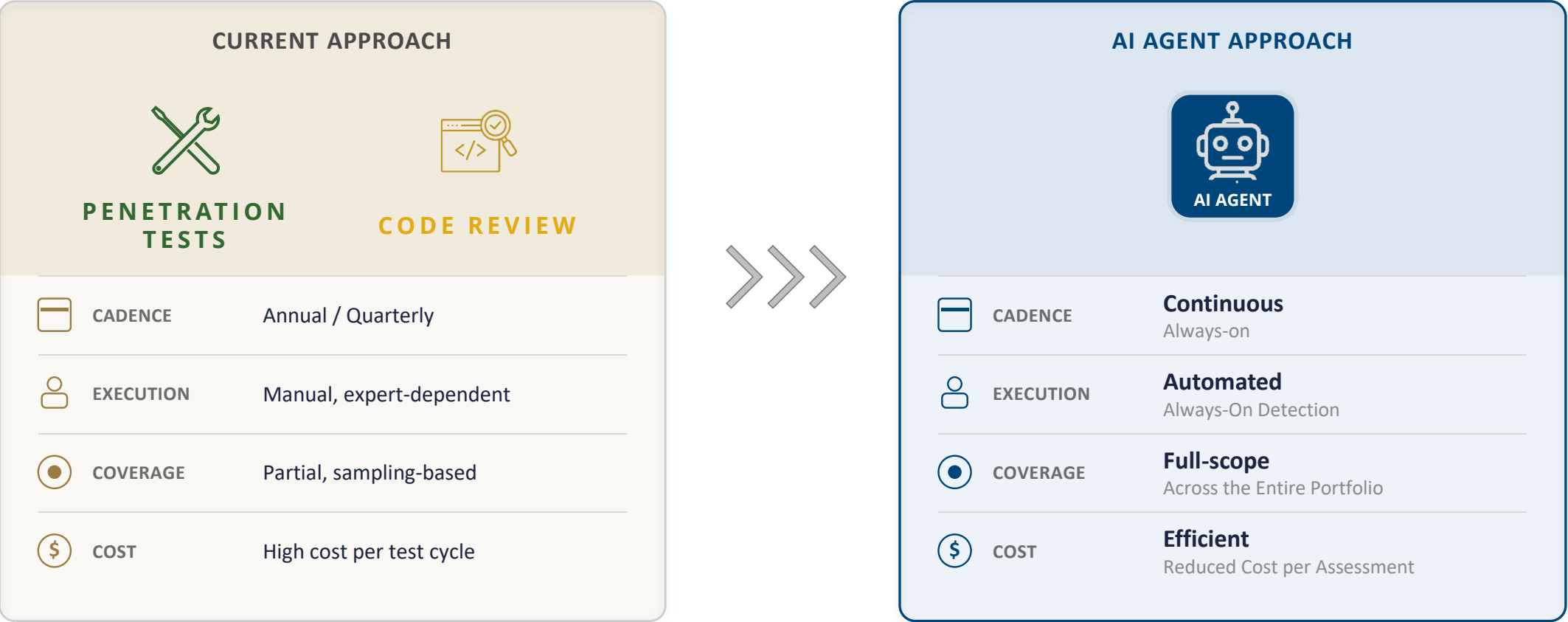
8 FTE

Limited internal capacity and reliance on external specialists constrain testing coverage and frequency.

Our exposure grows faster than our capacity to test



PATH FORWARD





AGENTS

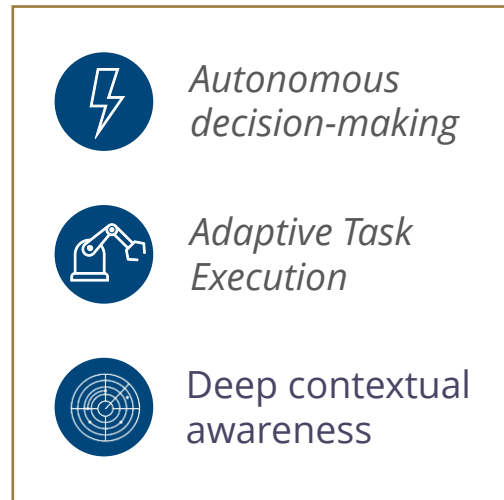


007



WHAT IS AN AI AGENT?

An AI Agent is an autonomous system that perceives its context, reasons and takes actions to achieve user goals





USE CASE

SIRES

Platform supporting critical regulatory processes, including entity licensing, board changes, and supervisory filings.



High Criticality
Critical regulatory processes and highly sensitive data.



Known Vulnerabilities
Certified environment with previously identified vulnerabilities



Security Reports
Recent reports available for comparative analysis



GOAL

Assess the effectiveness of **autonomous AI agents** in identifying **OWASP Top 10 vulnerabilities**.

~60%
COVERAGE



A01 Broken Access Control
Agent: IDOR

A02 Security Misconfiguration
Agent: Infra + Crypto

A03 Software Supply Chain
Agent: CVE Validator

A04 Cryptographic Failures
Agent: TLS + Crypto

A05 Injection
Agent: SQLi + XSS

A06 Insecure Design

A07 Authentication Failures
Agent: Auth Failures

A08 Software or Data Integrity Failures

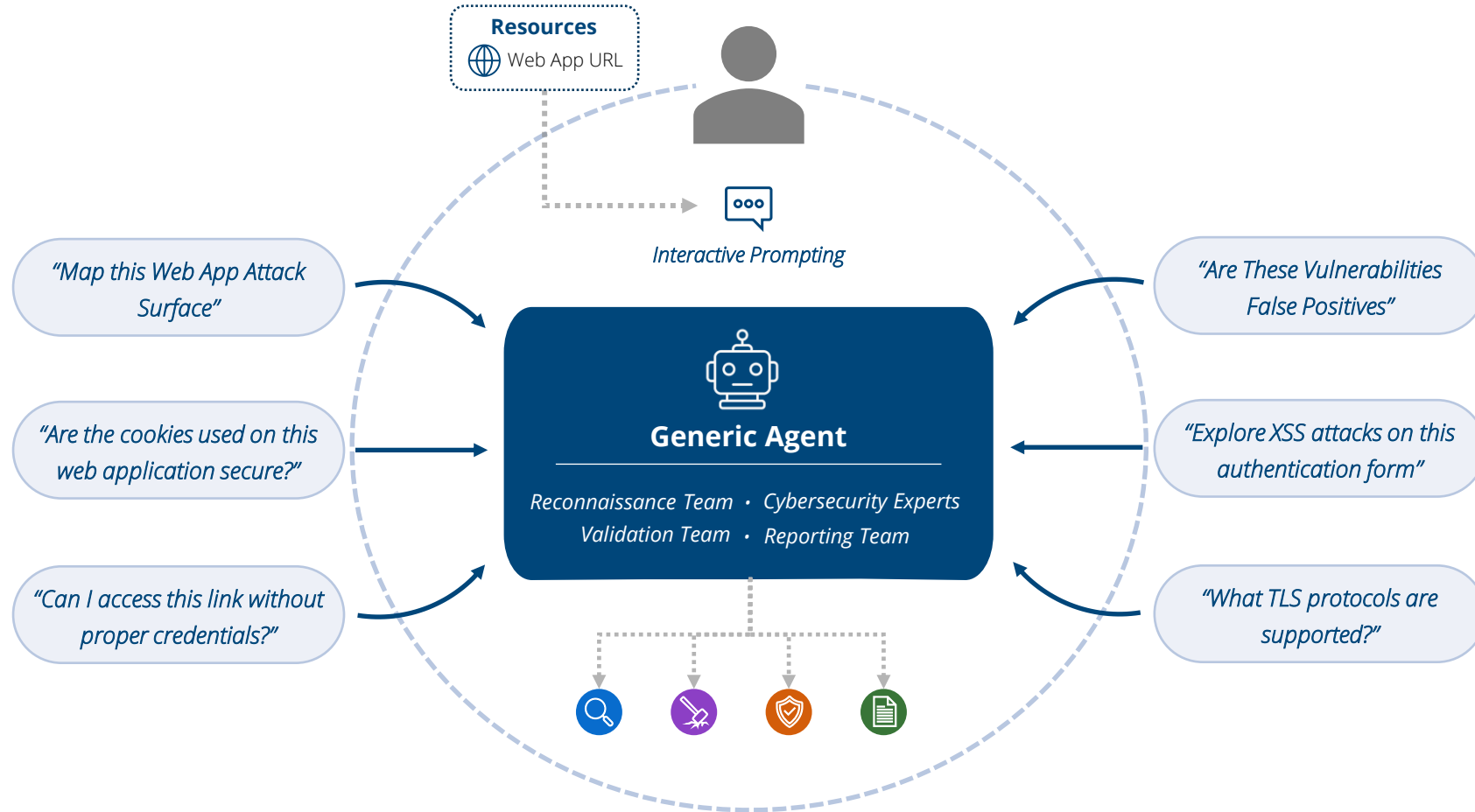
A09 Security Logging and Alerting Failures

A10 Mishandling of Exceptional Conditions

4 Complete 2 Partial 4 Not Covered



AI AGENT: INTERACTIVE





AI AGENT: INTERACTIVE



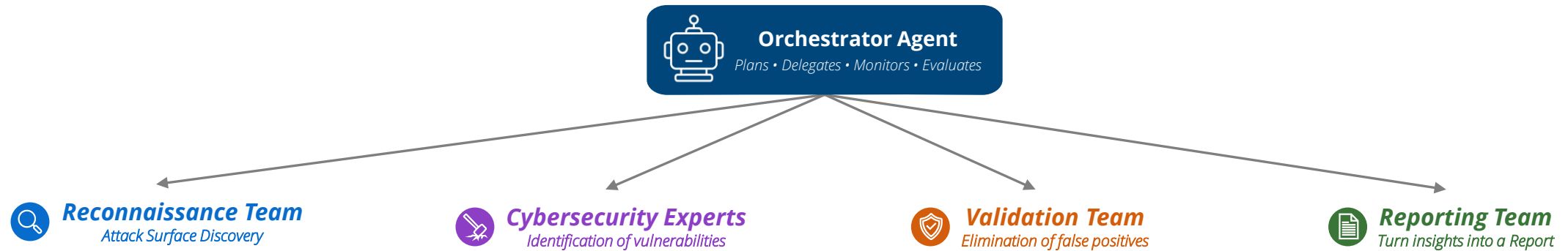
Generic Agent

*Reconnaissance Team • Cybersecurity Experts
Validation Team • Reporting Team*



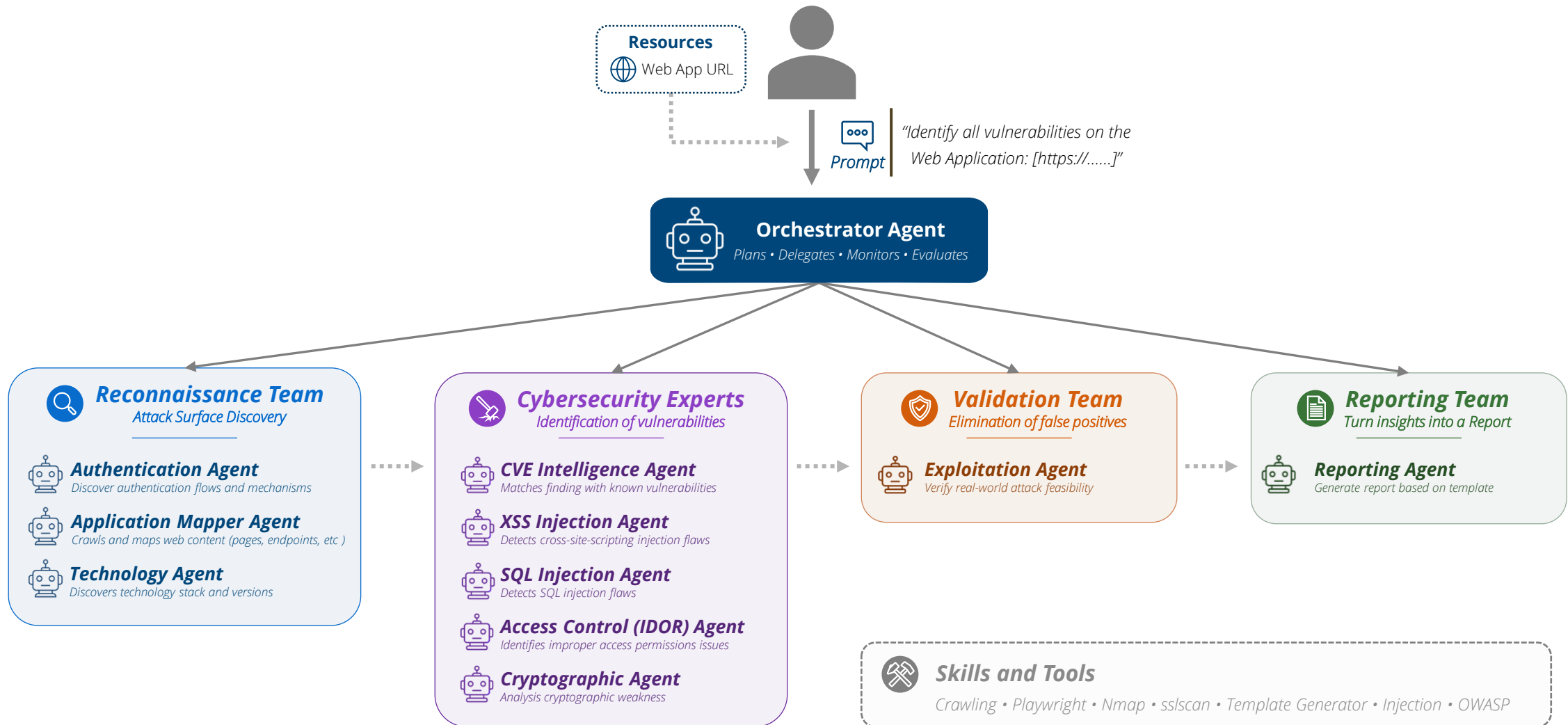


AI AGENT: AUTONOMOUS



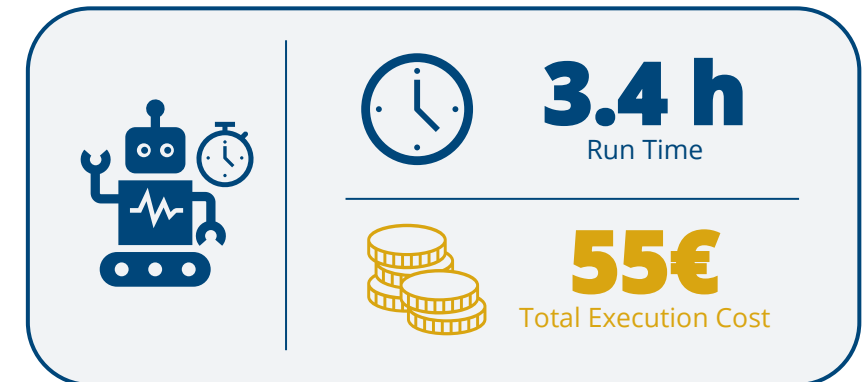
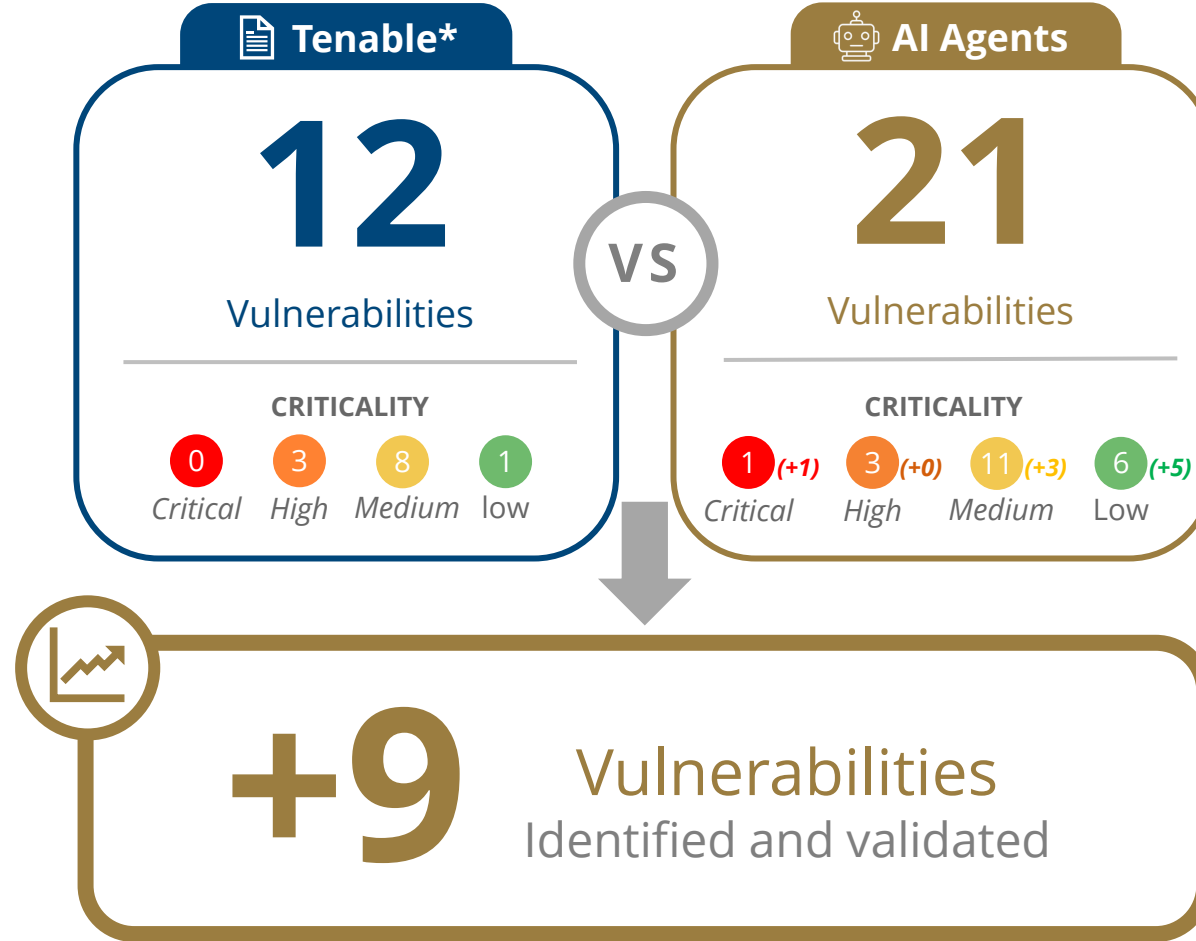


AI AGENT: AUTONOMOUS





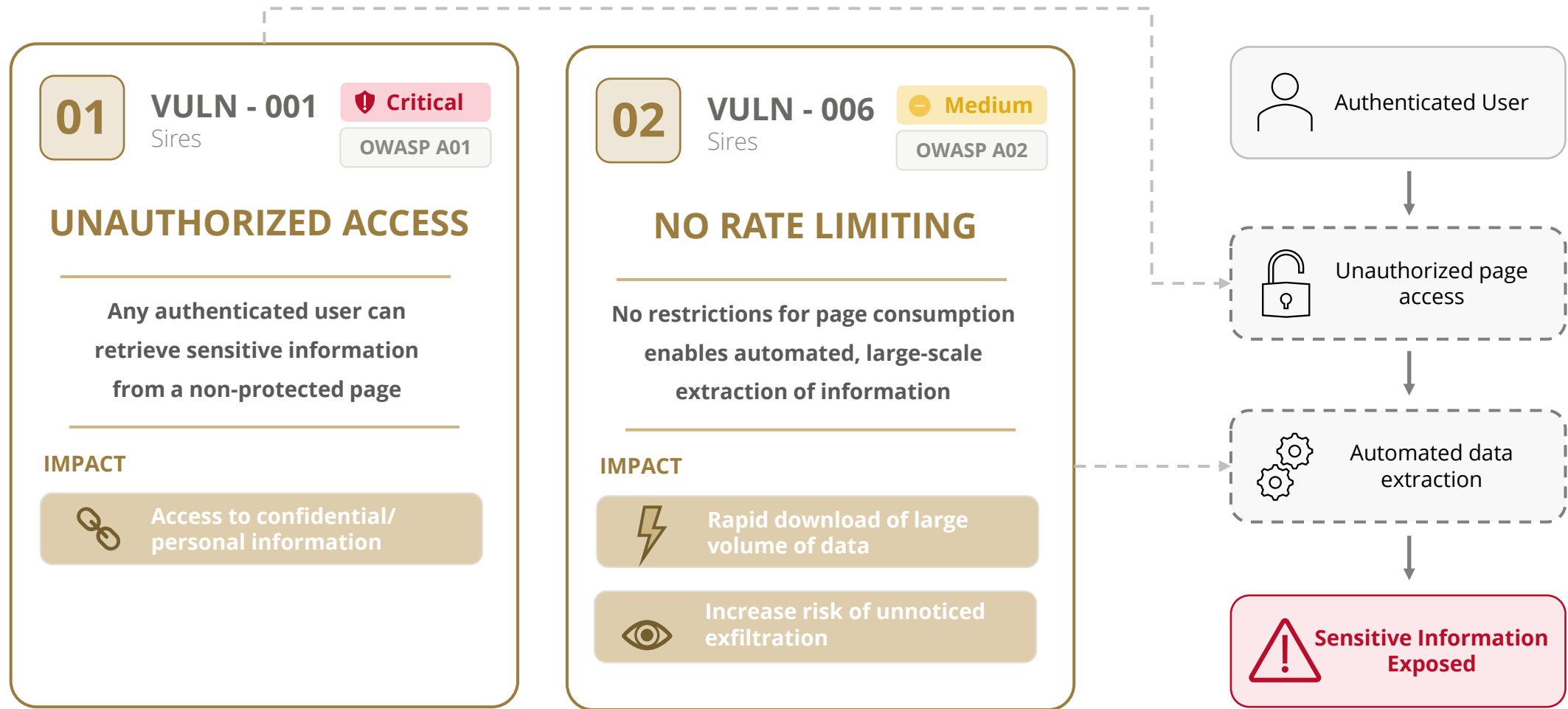
RESULTS: SIRES



*Only 12 of the 17 vulnerabilities recorded were addressed by agents

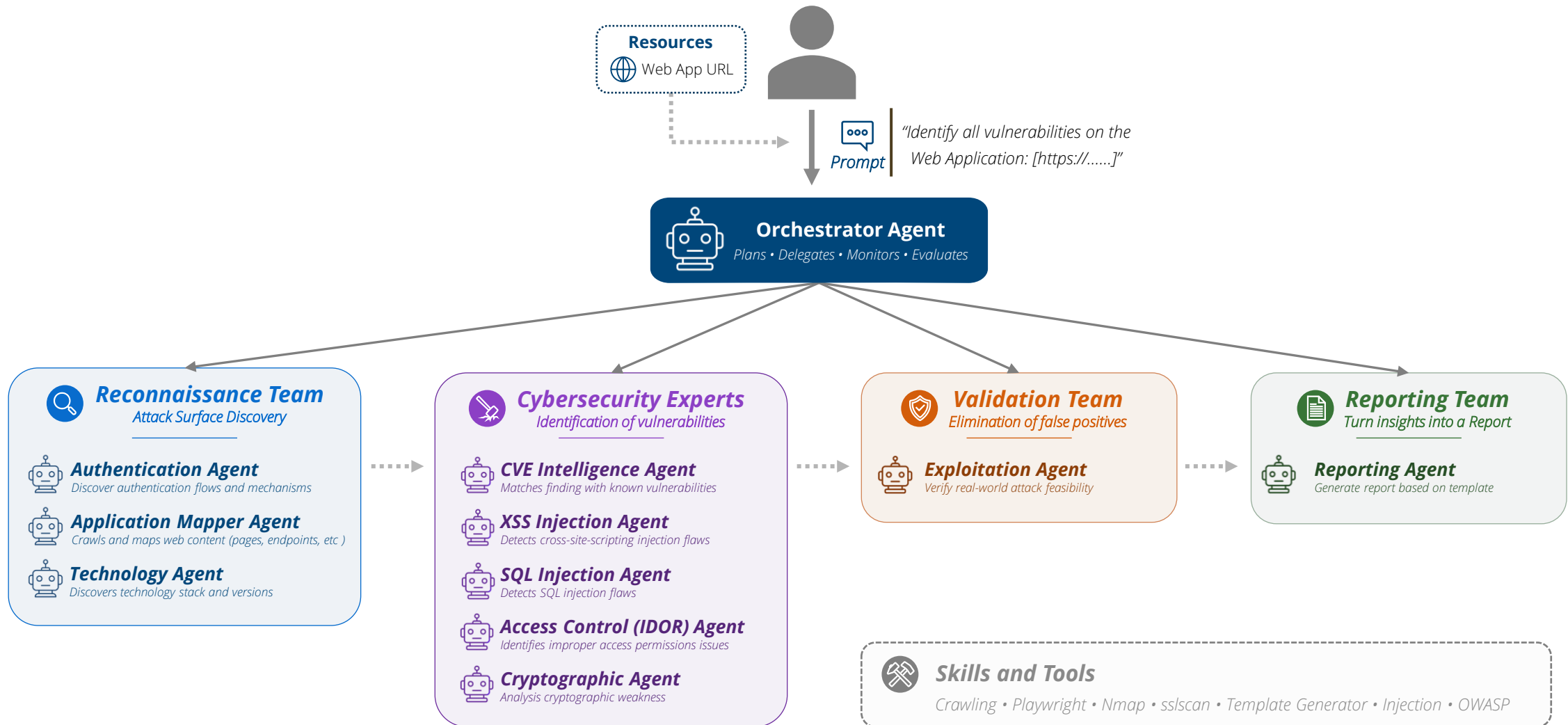


SUCCESS STORIES



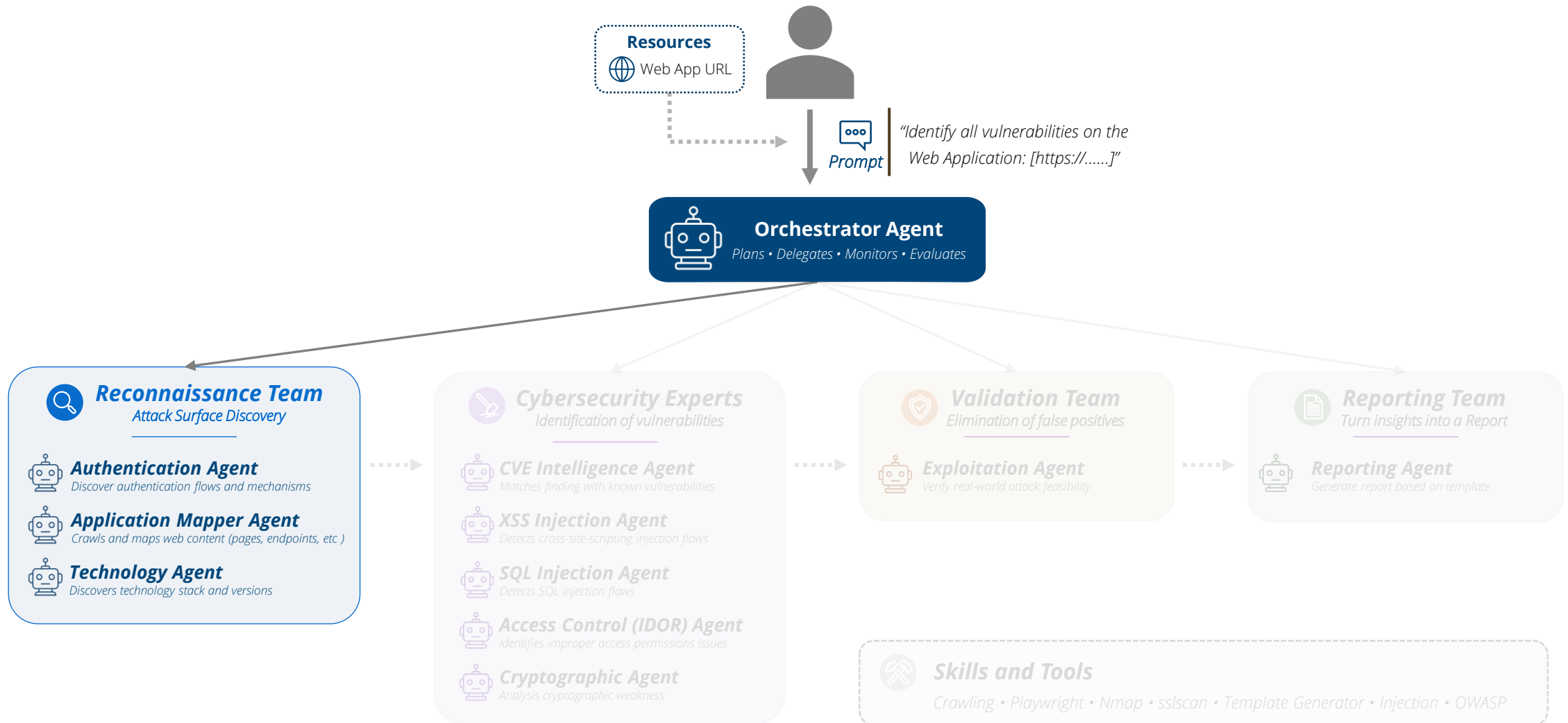


AI AGENT: AUTONOMOUS



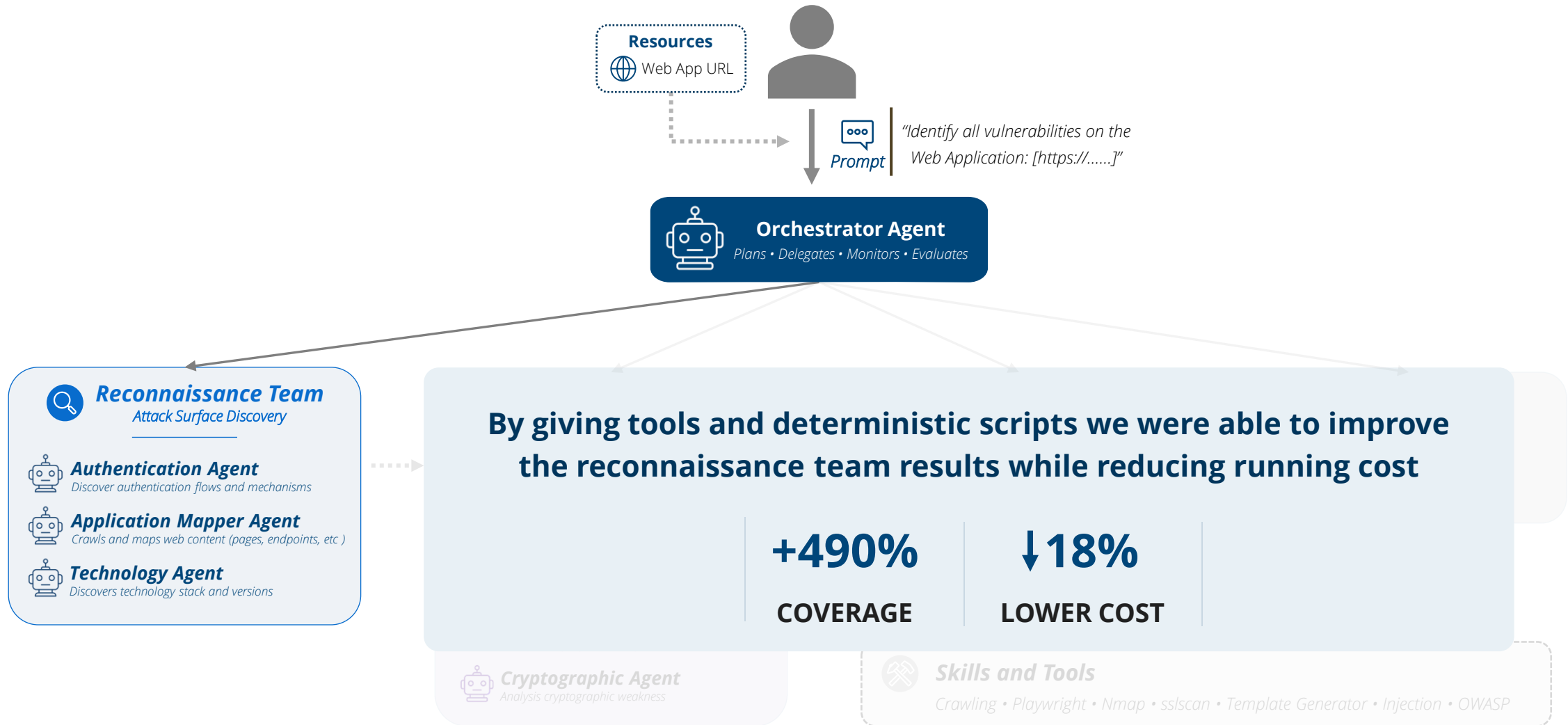


AI AGENT: AUTONOMOUS & HYBRID





AI AGENT: AUTONOMOUS & HYBRID





CURRENT RESULTS

SIRES & FLOW



✓ **Full coverage** of known vulnerabilities with identification of **additional critical vulnerabilities**, showing high potential for **process automation**



“

*“IF WE DON'T HARNESS AI FOR DEFENSE, WE
ARE BRINGING A KNIFE TO A GUNFIGHT.”*

— JEN EASTERLY, CISA DIRECTOR (CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY)

”



THANK YOU