



Resolve threats faster with  
orchestrated threat intelligence



## Overview

Federal government agencies face unique cybersecurity challenges such as **confidentiality within classified systems, integrating siloed operations, defending critical systems, and so much more.**

When defending against threats is mission-critical, being proactive ensures that sensitive data remains secure against espionage and unauthorized access.

Analyst1 was designed for the federal government to answer two fundamental cyber threat intelligence questions related to the identification, assessment, and mitigation of cyber threats:

**“So what?”** What do we know?

**“Who cares?”** How does it pertain to us?

Our **advanced threat intelligence platform** is unmatched for operational readiness, applying heightened automation, natural language processing, and supervised machine learning to ensure that defensive measures outpace threats in the environment.

## Introducing Analyst1

Enterprises invest heavily in threat intelligence, but many struggle to demonstrate its impact on their defense efforts. This creates what is known as the Threat Coordination Gap: while intelligence is generated, teams find it difficult to trace whether it results in improved coverage, detection, or mitigation.

Analyst1 is the Orchestrated Threat Intelligence Platform designed to close this gap. It takes raw feeds and reports and transforms them into structured intelligence, linking it to your assets and vulnerabilities. Additionally, it integrates with your SIEM, ticketing, and vulnerability management systems. National security agencies and Fortune 500 companies rely on Analyst1 to coordinate defense across teams, automate workflows, and reduce the time for mitigation from days to minutes.

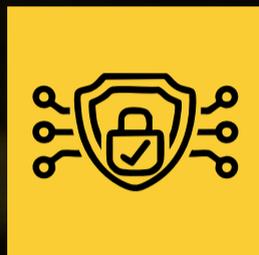


# ANALYST1

Resolve threats faster with  
orchestrated threat intelligence



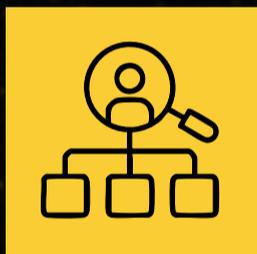
**97% customer  
retention**



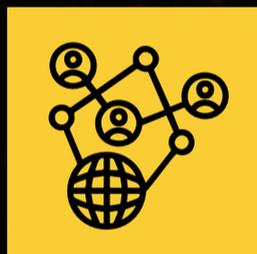
**Bidirectional SIEM  
integrations**



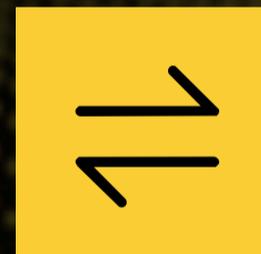
**Vulnerability and  
asset management**



**Original source  
attribution**



**Connect to  
99% of feeds**



**Bidirectional  
ticketing**



**Automatic rule  
creation**



**Sensor  
versioning**



**Indicator  
hit stats**

