Overview
Cyber threats are one of the most serious economic and national security challenges the nation faces today. Cyber threats are constantly evolving, and federal agencies must operate under the assumption that adversaries can and will infiltrate their networks. IT complexity, insider threats, and a plethora of privileged users plague public sector cyber readiness. Cybersecurity maturity needs attention.

What is the problem?
From malware, to ransomware, to phishing attacks, security breaches are happening daily in not only the federal government but at the state and local levels as well. Government organizations don’t just have to combat the standard hackers and cyber thugs – they also have to defend against spying attempts from nation-states. The dynamic nature, frequency, complexity, and magnitude of cyber intrusions present challenges to even the best secured networks.

Obstacles for public sector:
- Budget constraints
- Complexity of internal environment
- Competing priorities and initiatives
- Lack of manpower
- Skills gap

The Solution
With the public sector facing an increase in vulnerabilities, acquiring more robust cybersecurity solutions will help aid in securing its IP, private data, and nation-state secrets. Applying intelligence to detect and mitigate these threats, will enable analysts to better research malicious activity, and help accelerate the time to response and mitigation.

Results with Analyst1
Analyst1 establishes an evolving knowledge base of correlated insights about threats, attack patterns, malware families, vulnerabilities, internal assets, mission-critical systems at risk, and the defensive posture of a network over time.

Analyst1 reduces tool fatigue by providing a “single pane of glass” that facilitates seamless integration of multiple sources of information and eliminates labor-intensive tasks of assembling all information needed to prioritize mitigation actions.

2019 Verizon Data Breach Investigations report shows 168% increase year-over-year in number of government network breaches linked directly to state-sponsored actors

Analyst1 for Public Sector

“67% of all public-sector incidents and breaches came from external bad actors”
Verizon Data Breach Report

Analyst1 is a powerful solution for training threat teams on the critical skills needed to identify malicious activity. By determining the severity of threats to an organization, analysts can better defend against sophisticated attacks.
Analyst1 Capabilities

- Automate identification, collection, and correlation of diverse information
- Provide context and insights required to take action
- Author, text, and deploy effective countermeasures across multiple intrusion detection and prevention systems
- Detect and mitigate threat activity codifying cyber threat workflows
- Maintain traceability between evidence, indicators, rules and sensors to identify why a rule was created, the type of activity it detects, and what sensors are tasked.
- Obtain visibility into intrusion detection and prevention systems to maintain awareness of sensor types, enforced rules, POCs, physical locations, and logical locations.