Analyst1: Threat Intelligence and Network Defense Platform

Overview

Cyber threats are one of the most serious economic and national security challenges businesses of all sizes and verticals face. The dynamic nature, frequency, complexity, and magnitude of cyber intrusions present challenges to the best solutions available.

What is the problem?

Most organizations have internal security systems producing data about the activity on their networks. They also have access to external sources of data containing observations from third parties. The primary purpose of this type of security is to inform organizations the risks of advanced persistent threats, zero-day threats and exploits.

Cybersecurity experts lack an effective way to obtain actionable insight from these multiple sources of information, leaving their networks unsecured. Security experts spend precious intellectual capital using text editors and spreadsheets to manually extract, sort, and correlate disparate information before a moment is spent on analysis or response.

Organizations struggle to:

- Correlate multiple sources of data
- Identify actionable information
- Prescribe effective countermeasures

Introducing Analyst1

Analyst1, engineered by analysts for the enterprise, provides a threat intelligence and network defense platform to clarify malicious activities threatening an enterprise. Analyst1 offers organizations a more efficient method of gathering and enriching threat intelligence. Inundated with various security tools, analysts rarely have time to investigate and remediate all threats.

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.

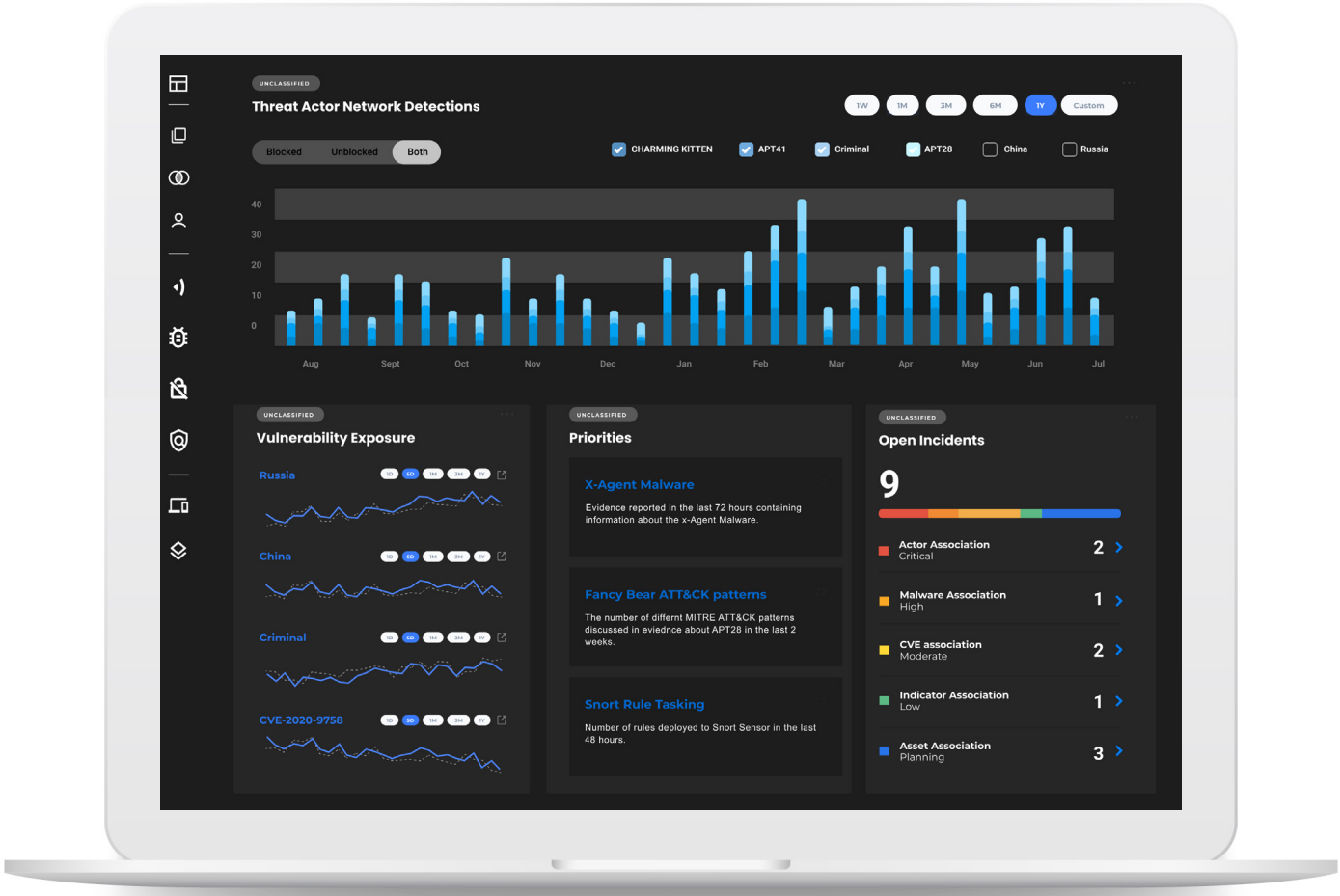
Analyst1: Threat Intelligence and Network Defense Platform

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.

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.



(888) 4-ANLYST | info@analyst1.com
11921 Freedom Dr #550, Reston, VA 20190