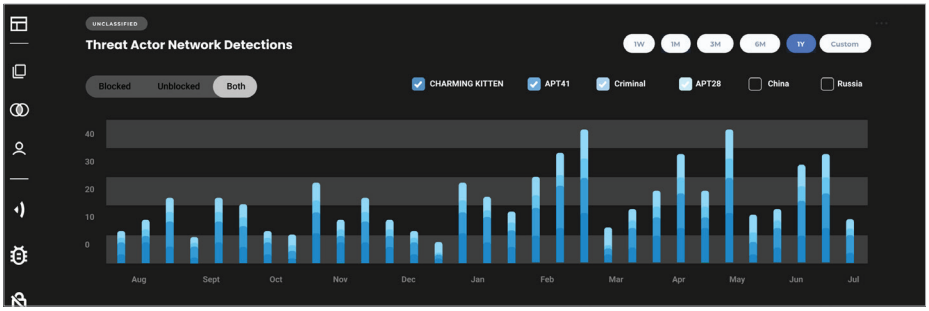

Analyst1

Analyst1 v1.9

Analyst1 operates as an authoritative repository of threat intelligence that uses native feeds and APIs for automated, bi-directional data sharing with SIEM systems. This product highlights indicators of compromise enriched with contextual information that saves analysts time and lets them make targeted response decisions instead of searching at random.

Analyst1 uncovers key information regarding various geographic regions and the threat actors that originate from them. This data becomes particularly valuable when conducting threat hunting. A summary report identifies every threat actor tied to a particular country and displays all group activity levels, targets, and MITRE ATT&CK patterns. It also offers details of individual threat actors, including aliases, recent hits, unique signature IDs, and more. Analysts can discover the existence of any indicators of compromise associated with particular threat actor groups within their own network, and ticketing system integration lets them see which team members, if any, have begun addressing these issues. Security teams may automate the process of creating and assigning tickets if they wish to streamline response.

The malware page resembles the threat actor page and shows the same contextual enrichments, like recent hits and indicators of compromise. The page also links each malware back to its associated actor group and gives an exposure score to indicate how vulnerable a network may be to this same actor group. It then offers net defense actions that analysts may take and rules they may deploy to protect against further attacks.

This platform also offers very strong reporting features. The A1 Bot automatically extracts all actionable information and highlights the most relevant details. Because it performs functions that analysts would otherwise have to do, A1 Bot frees security teams to focus on more complex investigations and responses. If necessary, analysts may override A1 Bot information with their own insights.

The interface has many configuration options, integrations, and rules, making Analyst1 a highly flexible solution. However, these options come with a steep learning curve and lack intuitive operability. We had difficulty figuring out which options to adopt and how to adopt them. Still, Analyst1 has many rich features to offer, and many security teams may find developing more familiarity with the platform well worth the time and effort.

Overall, security pros will find Analyst1 a comprehensive threat intelligence platform. It offers effective visibility into assets and devices so that analysts may quickly gain an understanding of the systems to which assets are tied and the vulnerabilities that exist on them. We really like that it reveals associations between assets and threat actors or CVEs because these associations prevent security teams from developing tunnel vision and addressing only high CVE criticalities while leaving less critical vulnerabilities unpatched. Government organizations may especially appreciate that Analyst1 can run on top-secret networks and portion mark everything according to classification and dissemination controls.

Pricing starts at $15,000 per named user license and includes 24/7 phone, email, and website support. Organizations also have access to a user guide which contains support documentation and a handful of how-to video tutorials. We recommend migrating the documentation from one large, flat file into a searchable knowledgebase to make finding relevant manuals easier and more intuitive.

— Katelyn Dunn
Tested by Tom Weil

DETAILS

Vendor Analyst1

Price $15,000 per named user license

Contact analyst1.com

Features	★★★★★
Documentation	★★★★¾
Value for money	★★★★★
Performance	★★★★★
Support	★★★★★
Ease of use	★★★★¾
OVERALL RATING	★★★★¾

Strengths The A1 Bot automatically extracts all actionable information and highlights the most relevant details and frees security teams to focus on more complex investigations and responses.

Weaknesses The many configuration options come with a steep learning curve and lack intuitive operability. We had difficulty figuring out which options to adopt and how to adopt them

Verdict Overall, Analyst1 is a comprehensive threat intelligence platform that Government organizations may especially appreciate because it can run on top-secret networks and portion mark everything according to classification and dissemination controls.