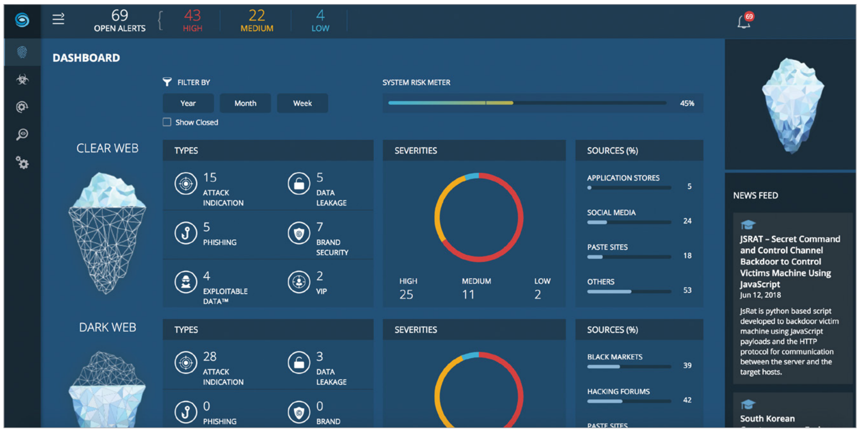
SC MEDIA ★★★★½



JSRAT – Secret Command and Control Channel Backdoor to Control Victims Machine Using JavaScript
Jun 12, 2018

JsRat is python based script developed to backdoor victim machine using JavaScript payloads and the HTTP protocol for communication between the server and the target hosts.

South Korean

IntSights Cyber Intelligence

Threat Intelligence Platform

The Threat Intelligence Platform from IntSights Cyber Intelligence allows users to correlate traffic data against threat feeds and send out alerts for immediate action. The platform is based on a virtual appliance located on-premises that can integrate into existing security infrastructures such as SIEM and firewalls. Moreover, this offering can integrate with Office 365 Exchange as well as other cloud-based service providers.

IntSights has divided the solution's interface into several different modules, including a customer-facing dashboard, assets listing and an alerts page. For this evaluation, we focused on two specific modules: IOC Management and Alerts tabs.

The IOC management tab shows the various intelligence feeds available through the solution. In addition to those provided by IntSights and its membership through the Cyber Threat Alliance, there are three available premium feeds and three public feeds. Users also can create manual intelligence feeds for customized data coming into the platform. An efficient feature allows for the creation of exceptions, which can be set so that IOCs in the manually created list will be excluded from all integrated IOC lists. Shield icons appear next to each feed in the interface and display the confidence level that IntSights has in the data channel. Accordingly, IntSights is continually working to add more feeds right out of the box.

A final function we noted in this tab is the investigation screen. We appreciate that analysts can email the details of the results directly to a recipient who isn't required to have an account to interact with them.

For analysts in the middle of an investigation, though, an automated feed may not be the most appropriate tool. Instead, the research tab proves a better resource because it shows the trends of different threat actors – giving analysts the ability to dive into their backgrounds – and any file signatures or domains associated with them. Using the search function in this tab, analysts can run very simple queries against the solution's database for real-time results. IntSights is still working on updates to this feature which will be rolled out over the next couple of months, but in the meantime, the company recommends customers rely more on IOC management if the search results are not deep enough.

Once the solution identifies an IOC, the alerts tab provides screenshots of the danger and indicates severity (low, medium, high, critical). An alert category, such as "Data Leak," also confirms which security personnel are assigned the alert and provides report date and time information.

Pricing for the platform begins at $100,000 for enterprise customers who want the automation/integration module, which includes a virtual appliance. Its minimum requirements are 2 CPUs, 8GB RAM and 40GB disk space and it will rely on a preconfigured OVA package to integrate with the other components in your stack. Support is available in windows of either 8/5 or 24/7.

– Dan Cure,
reviewed by: Matthew Hreben & Michael Diehl

DETAILS

Vendor: IntSights Cyber Intelligence

Solution: Threat Intelligence Platform

Price: Starting at $100,000 for enterprise customers.

Contact: intsights.com

Features	★★★★¾
Documentation	★★★★★
Value for money	★★★★
Performance	★★★★★
Support	★★★★½
Ease of use	★★★★★

OVERALL RATING ★★★★½

Strengths: Lots of integrations with traditional infrastructure as well as cloud solutions.

Weaknesses: A little cost prohibitive for the market space.

Verdict: Beautiful dashboard with an amazing product behind it; a quality company and solution that you should keep an eye on.

INTSIGHTS
Threat Intelligence Realized.

info@intsights.com
1-800-532-4617
110 W 40th Street, Suite 1901
New-York, NY 10018
www.intsights.com