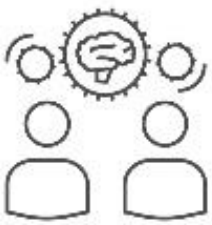
CYBOT HUNTER

Threat Hunting Platform

DATA SHEET

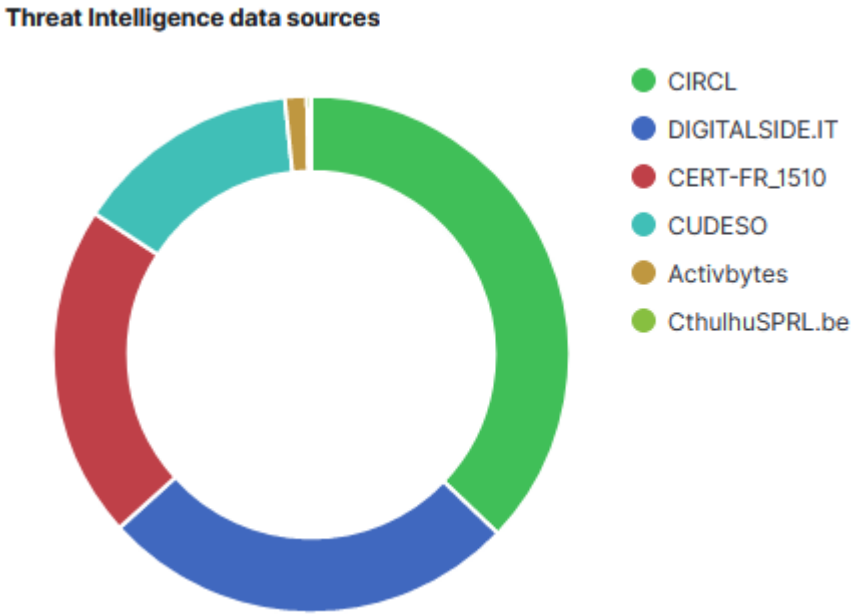


Threat Intelligence Sharing Platform

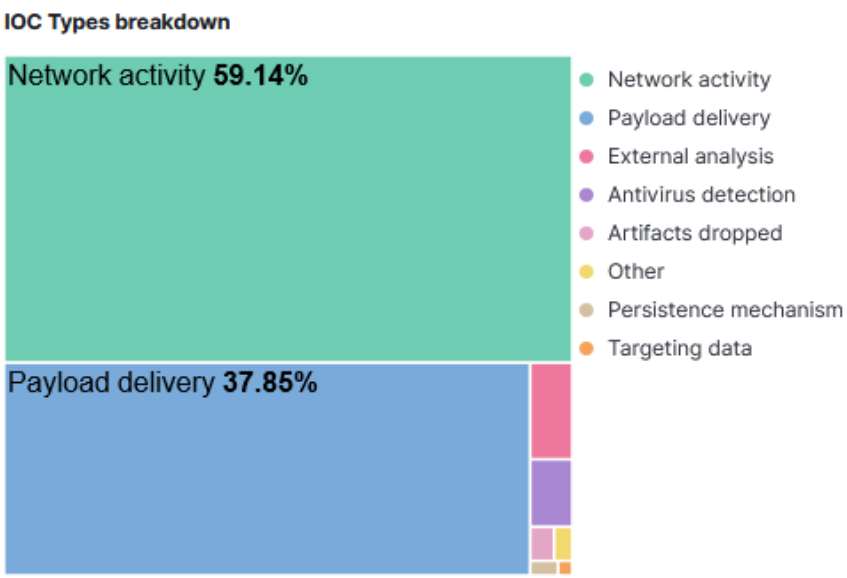
activebytes innovations

THREAT INTELLIGENCE SHARING PLATFROM FEATURES

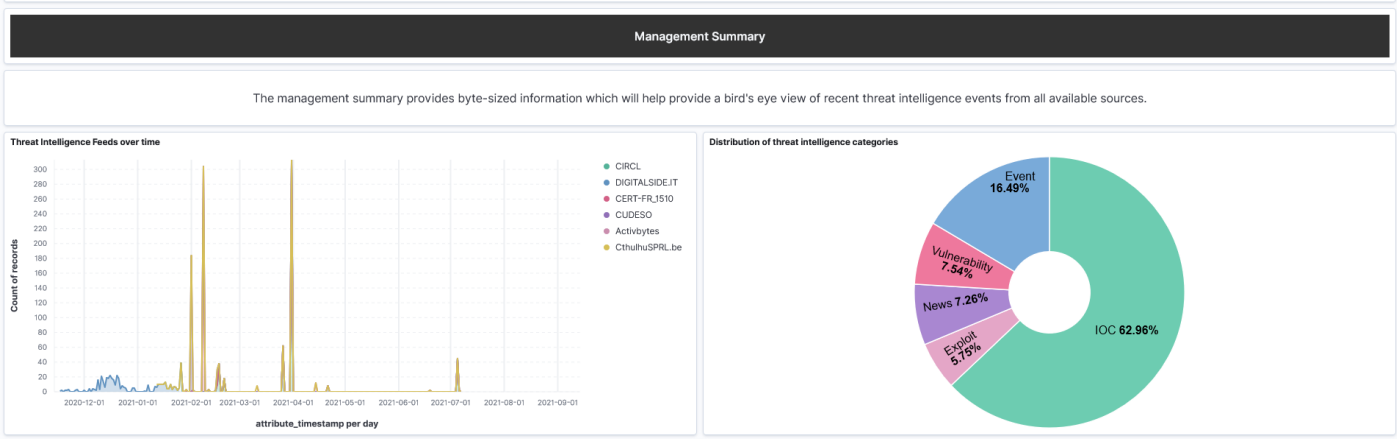
- Receiving and Sharing threat intelligence information in a controlled and structured manner
- Receiving threat intelligence information from various open source, dark web sources



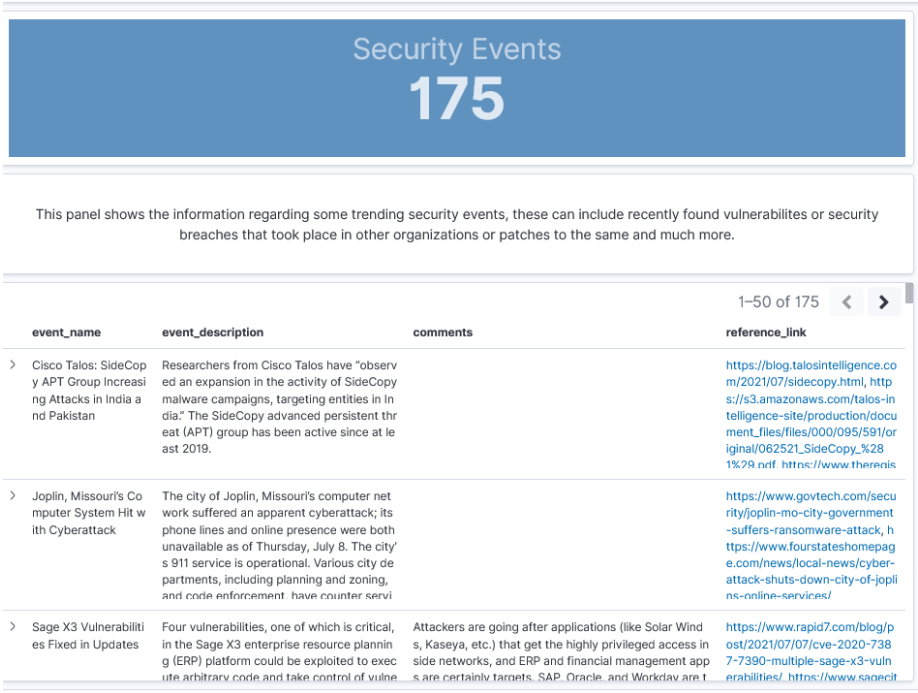
- Receive threat intelligence information from other commercial sources as well.
- Pre- configured to receive threat intelligence data from multiple sources
- Role based access control.
- Capable to securely gather, share, store and correlate IoC's of targeted attacks, vulnerability information etc
- Record all type of IOCs includes Ip, URLs, text, files, hashes, IDS signatures etc.



- Allows internal team to collaborate and discuss on intelligence events.
- Allows organization to share threat intelligence information with peers effectively
- No restrictions with number of users
- API for all major functionality allows seamless integration with other security solutions
- Automatically co-relate and mark related previous incidents for effective tracking
- Exportable as dashboards and reports with better graphical representations
- Meant for both technical and not technical resources



- Commercial threat feeds ands service from ActiveBytes dedicated threat intelligence Team for effective Threat information analysis, identification, Domain takedown etc.
- TI Feeds of Malware Information, Threat Intelligence News, Vulnerability and exploits information.



activebytes innovations

Headlines
77

This panel shows some trending news items headlines that are related to cyber security, along with reference links for further reading.

1–50 of 77

news_headline	reference_link
The operators behind the attack on Kaseya are demanding a $70 million ransom payment in the form of Bitcoin in exchange for a decryptor tool that will allegedly return victims' files to them.	https://www.cnn.com/2021/07/05/business/ransomware-group-payment-kaseya/index.html
The Fancy Bear APT, suspected of being behind the SolarWinds supply chain attack, is also reportedly orchestrating brute-force password attacks all over the internet.	https://www.wired.com/story/fancy-bear-russia-brute-force-hacking/
The Kaseya supply chain ransomware attack may affect up to 1,500 organizations. Kaseya shut down the compromised program within an hour of detecting it.	https://www.washingtonpost.com/business/2021/07/06/kaseya-ransomware-attack-victims/
Google removed nine malicious apps from its Play Store that were spotted stealing Facebook credentials, but not before being downloaded a combined 5.9 million times.	https://threatpost.com/android-apps-google-play-facebook-credentials/167563/
Microsoft is warning customers that attackers are actively exploiting the so-called "PrintNightmare" vulnerabilities in its print spooler service.	https://www.theverge.com/2021/7/2/22560435/microsoft-printnightmare-windows-print-spooler-service-vulnerability-exploit-0-day
Insurance brokerages that offer cyberinsurance policies are starting to revamp their approach to ransomware; the companies have paid out large claims and some of them have been hit with ransomware themselves	https://apnews.com/article/kaseya-ransomware-attack-0705-4c2272cdd428ddfa1f3644d513566c06

Vulnerabilities with Exploits
61

An exploit is a piece of software, data or sequence of commands that takes advantage of a vulnerability to cause unintended behavior or to gain unauthorized access to sensitive data. The following table shows the breakdown of some vulnerabilities with their exploit information including the CVE, CVSS etc. that were obtained from various sources in the given timeframe.

1–50 of 61

event_name	event_description	cve	cvss	vendor
Unauthorized Directory Traversal Vulnerability in FCKeditor	Multiple directory traversal vulnerabilities in FCKeditor before 2.6.4.1 allow remote attackers to create executable files in arbitrary directories via directory traversal sequences in the input to unspecified connector modules, as exploited in the wild for remote code execution in July 2009, related to the file browser and the editor/filemanager/connectors/ directory	2009-2265	No CVSS found	FCKEditor
XSS Vulnerability in Cisco Adaptive Security Appliance Software	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow	2020-3580	CVSS v3.1 Base Score: 6.1 (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)	Cisco
XSS Vulnerability in Jira	The number range searcher component in Jira Server and Jira Data Center before version 8.5.14, from version 8.6.0 before version 8.13.6, and from version 8.14.0 before version 8.16.1 allows remote attackers inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability.	2021-26078	CVSS v3.0 Base Score: 6.1 (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)	Atlassian