CYBOT™

Automated Investigation & Hunting Platform

Datasheet

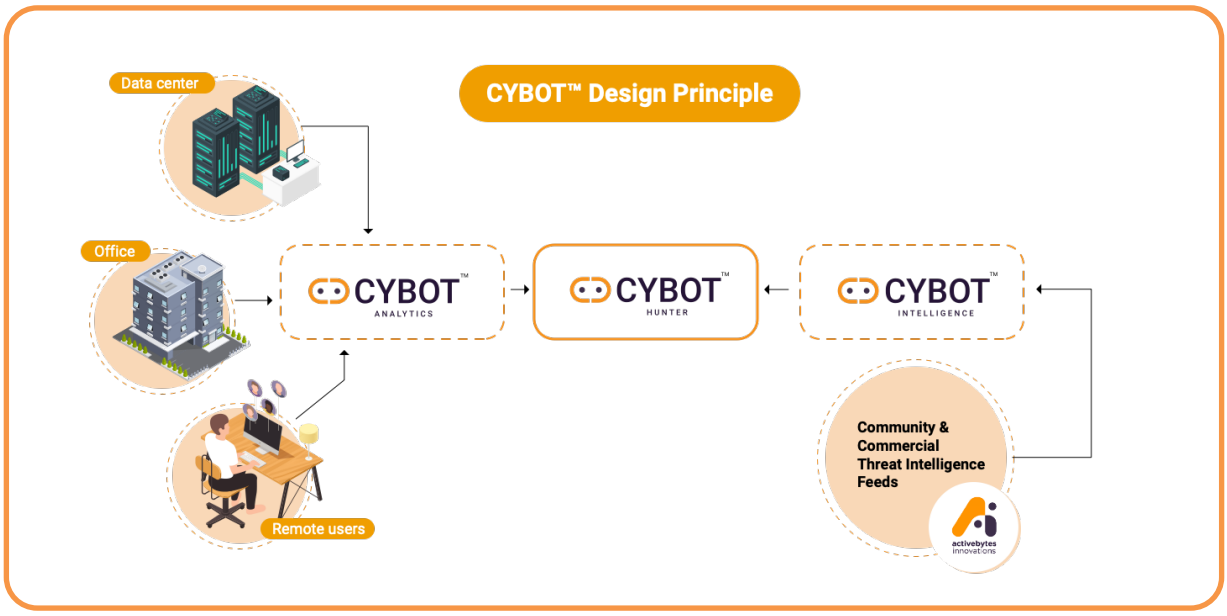
CYBOT™ Intelligence

activebytes innovations

www.active-bytes.com

About CYBOT™

- CYBOT™ collects raw logs from enterprise network, remote users, servers and stores to its analytical engine in a contextualized and secured way. The logs then undergo intelligent automatic analysis, thereby going the extra mile in threat hunting which, a human cannot do.
- CYBOT™ is designed to be adaptive to the latest adversary techniques and tactics by keeping in track with the Threat Intelligence events that it is programmed to receive from our trusted community sources and Activebytes Innovation's dedicated threat intelligence team.
- CYBOT™ intelligently and automatically hunts and investigates the threat leveraging Realtime Logs by performing correlation with TI IOCs received from even the dark sources, thereby detecting adversary attack patterns that a human can never pickup.
- Around the clock monitoring of logs and every unusual, suspected event is subjected to drill down the level of investigation and CYBOT™ is designed to provide automated options to respond along with suggestions and alerts to the security team. This will help analysts to deal with the adversaries that already intruded on the network.



Click here to get an overview of the working of CYBOT™

Why CYBOT™ is Your Automated Adaptive Threat Hunting Solution ?

CYBOT™ Threat Intelligence

CYBOT™ has a Threat Intelligence Platform which continuously gets updated with knowledge of the latest cyber security threats in the industry worldwide. The inputted Information from both commercial and community threat intelligence events, news and vulnerabilities is accessible in the CYBOT™ platform to both technical and non-technical teams in the form of user-friendly dashboards, printouts and emails. This provides analysts and incident responders with effective intelligence. CYBOT™ is designed to avoid repeated investigation on identical observables including IOCs and patterns, thereby reducing false-positives and noise to the analysts. We extend our security specialist's hands for threat intelligence services like domain takedown.

CYBOT™ Intelligence

CYBOT™ transforms raw feeds from various commercial and community sources into useful intelligence. The value-added analyzed and contextualized intelligence feeds from Activebytes innovations is also inputted to the platform. This effective intelligence gives and an extra edge to the security team about the latest adversary techniques and tactics, sector targeted, threat landscape, etc. that take place in the world. The huge pool of relevant intelligence feeds helps CYBOT™ in early detection of hidden, unknown, and emerging threats and this helps the analysts to quickly defend and secure their environment.

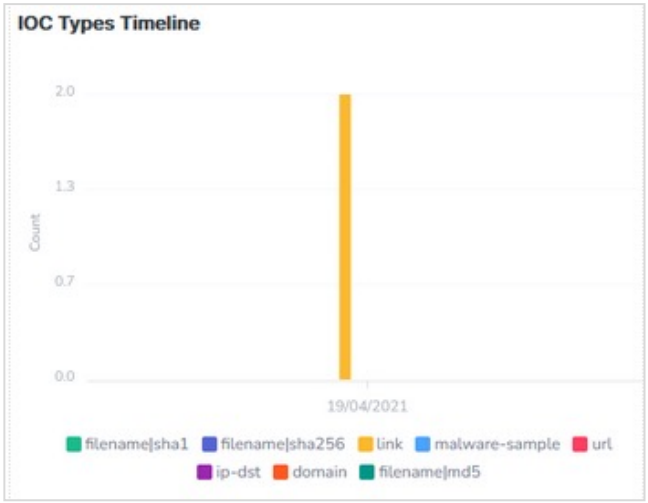
CYBOT™ protects your infrastructure from even the darkest corners

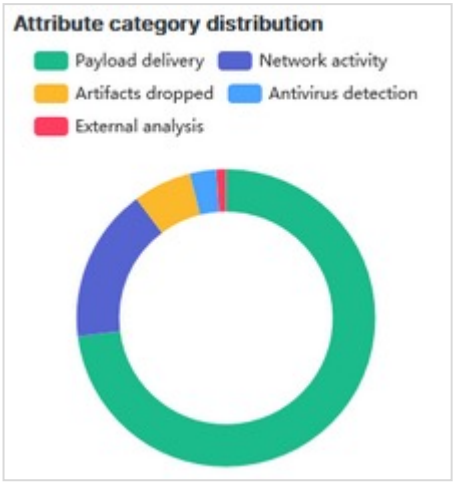
Threat intelligence feeds from various open sources and dark web sources make the CYBOT™ platform adaptive and efficient in detecting threats that escaped your defence system.

No malicious executions go undetected with TIP

With intelligence sharing, the latest technique adversary executions are fed to CYBOT™ and hence can perform faster malicious IP detection, Domain, Hash detection, etc.

User friendly technical and non-technical management summary reports generated with option to download and set notifications



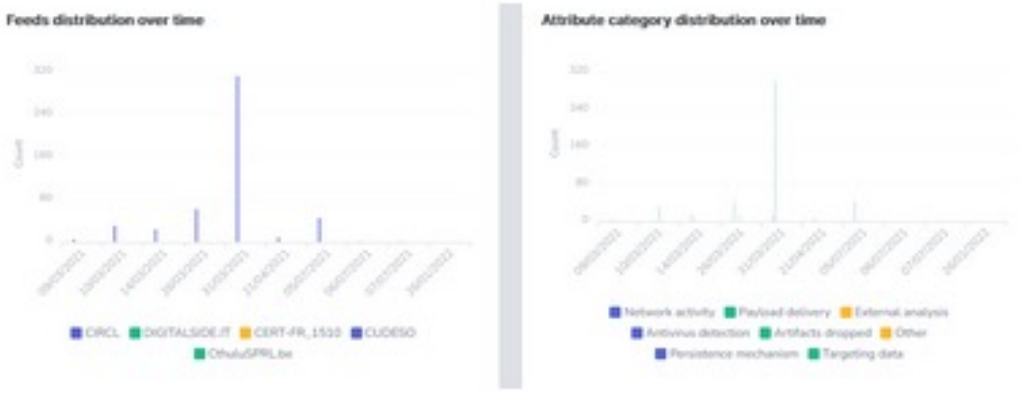


Some other features include

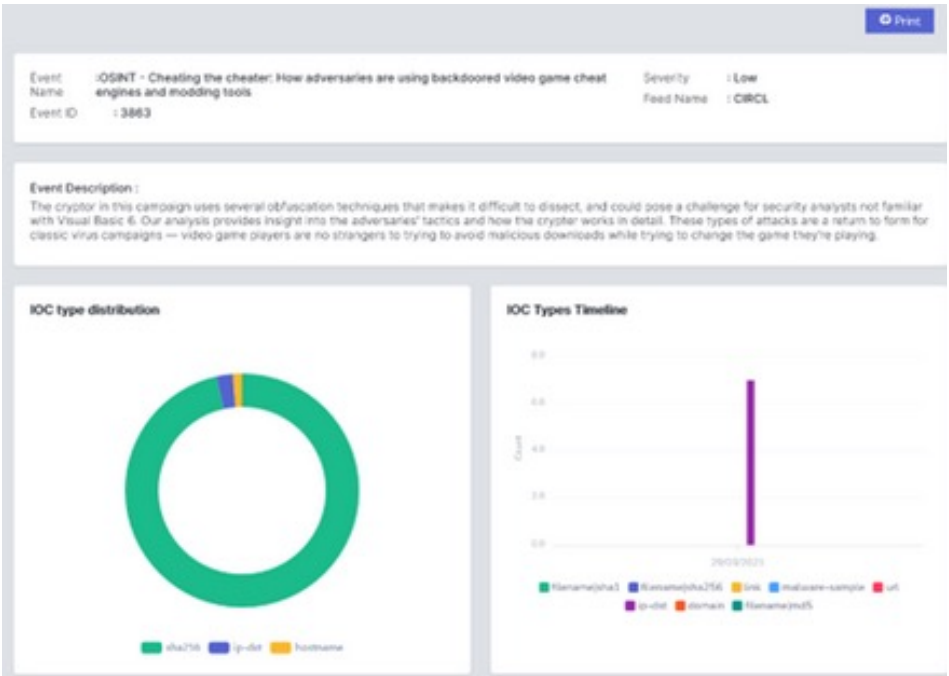
- Receiving and sharing threat intelligence information in a controlled, contextualized and structured manner benefiting the enterprise.
- Receiving threat intelligence information from various open source, dark web sources and this makes CYBOT™ intelligent and adaptive to the latest attack trends.
- Receives the latest emerging threat intelligence information from commercial sources as well.
- CYBOT™ is Pre-configured to receive threat intelligence data from multiple sources and contextualize the data for effective correlation with observables in the enterprise environment.
- Role-based access control and can be managed in the Settings option in the platform.
- Records all types of IOCs including IP, URLs, text, files, hashes, IDS signatures, etc. and hence even manually undetectable threats don't escape the investigation.
- Allows internal team to collaborate and discuss security and vulnerability intelligence events and this benefits the whole team with knowledge of the latest attacks and the ways to defend from the same.
- Allows the organization to share threat intelligence information with peers effectively.
- No restrictions with the number of users and new users can be easily added by the admin.
- API for all major functionality allows seamless integration with other security solutions.
- Automatically co-relates and marks related to 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 and services from ActiveBytes Innovations' dedicated threat intelligence team for effective threat information analysis, identification, domain takedown, etc.
- TI Feeds on Malware Information, Threat Intelligence News, Vulnerability and exploits information makes CYBOT™'s resource pool rich with the latest adversary factors.

Sample Community Threat Intelligence Events

Capable to securely gather, share, store and correlate IoCs of targeted attacks, vulnerability information etc. This makes the automated hunt faster and efficient.



Detailed information on each intelligence event, thereby providing the analysts and the management an insight on emerging threats. This will also help to decide the changes to be made in your present security defence framework. The print button can be used to get the details printed.

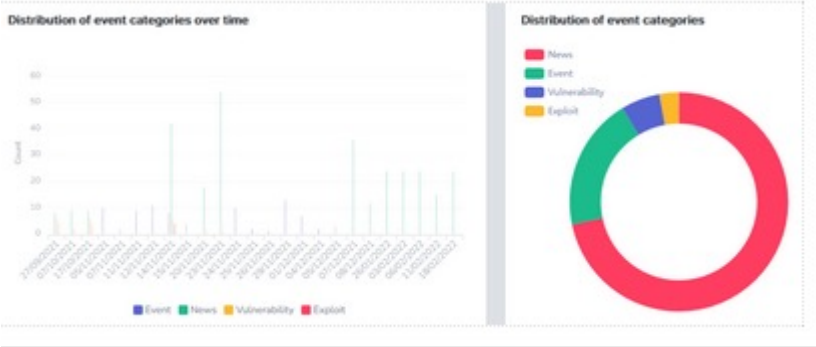


Every IOC is listed in indicators table with in-depth information, making the latest events resourceful for analysts

IOC Value	IOC Type	IOC Category	IOC Comment	IOC id	Timestamp
dracula4000.duckdns.org	hostname	Network activity	dracula4000.duckdns.org: enriched via the farsight_passivedns module.	318166	Jan 19, 1970, 10:43:24 PM
draculax.myq-see.com	hostname	Network activity	draculax.myq-see.com: enriched via the farsight_passivedns module.	318167	Jan 19, 1970, 10:43:24 PM
macross.ddns.net	hostname	Network activity		318168	Jan 19, 1970, 10:43:24 PM
win08.zapto.org	hostname	Network activity	win08.zapto.org: enriched via the farsight_passivedns module.	318169	Jan 19, 1970, 10:43:24 PM
45.163.152.127	ip-dst	Network activity		318170	Jan 19, 1970, 10:43:24 PM

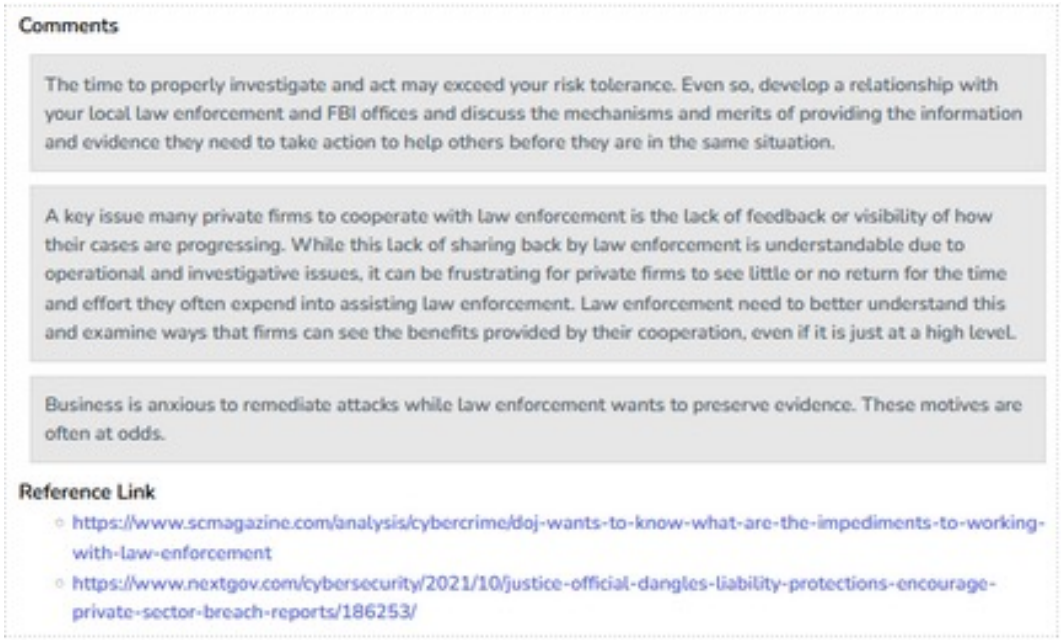
Sample Activebytes Innovations Threat Intelligence Events

The time distribution gives insight into the adversary attacks, vulnerabilities that trend during a particular time in the world, thereby providing an idea for changes required in the defence system

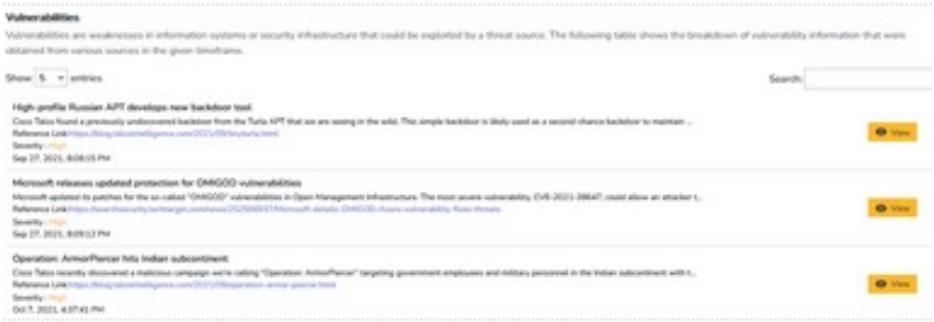


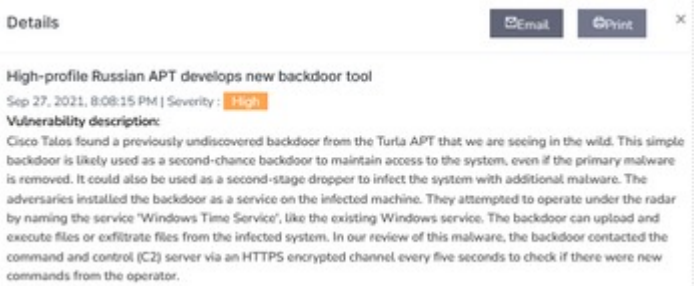
The Impact region helps you to understand the threat landscape and the degree of impact, a particular attack has caused.

Expert analysis and comments on security intelligence and vulnerability intelligence are very important for any security team to update their own IT infrastructure security accordingly.

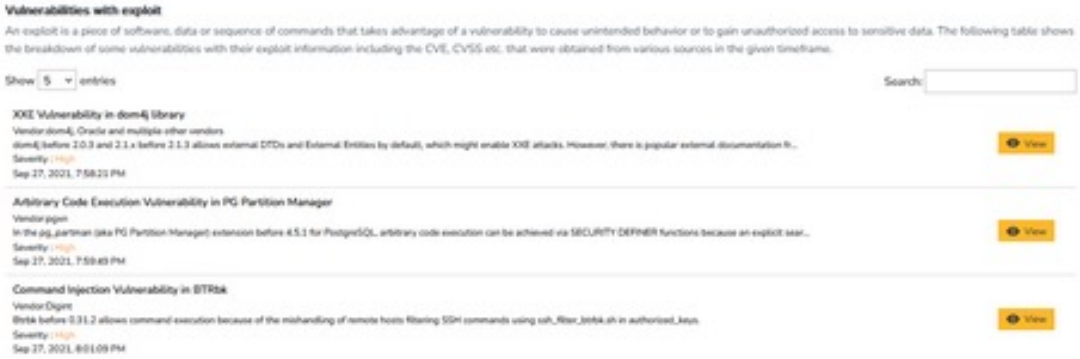


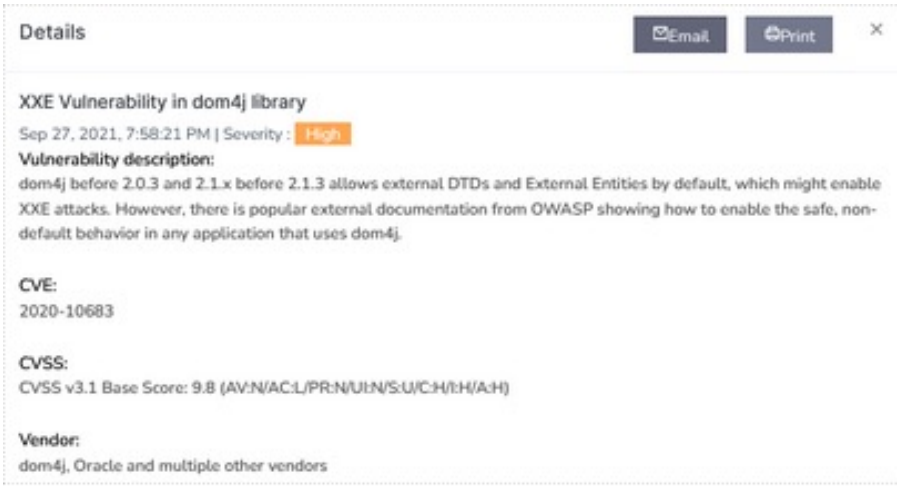
Any vulnerabilities in your environment can lead to a security breach and getting updates about the same for enterprise benefit is an added advantage

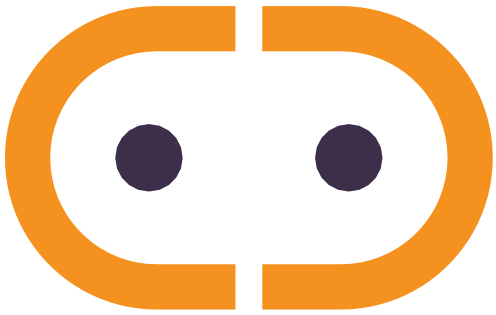




Vulnerabilities and exploits are crucial information to security teams since these need to be given extra focus during patch management







activebytes innovations

www.active-bytes.com / contact@active-bytes.com
+971 50 513 3973