



Automated Investigation & Hunting Platform



Datasheet

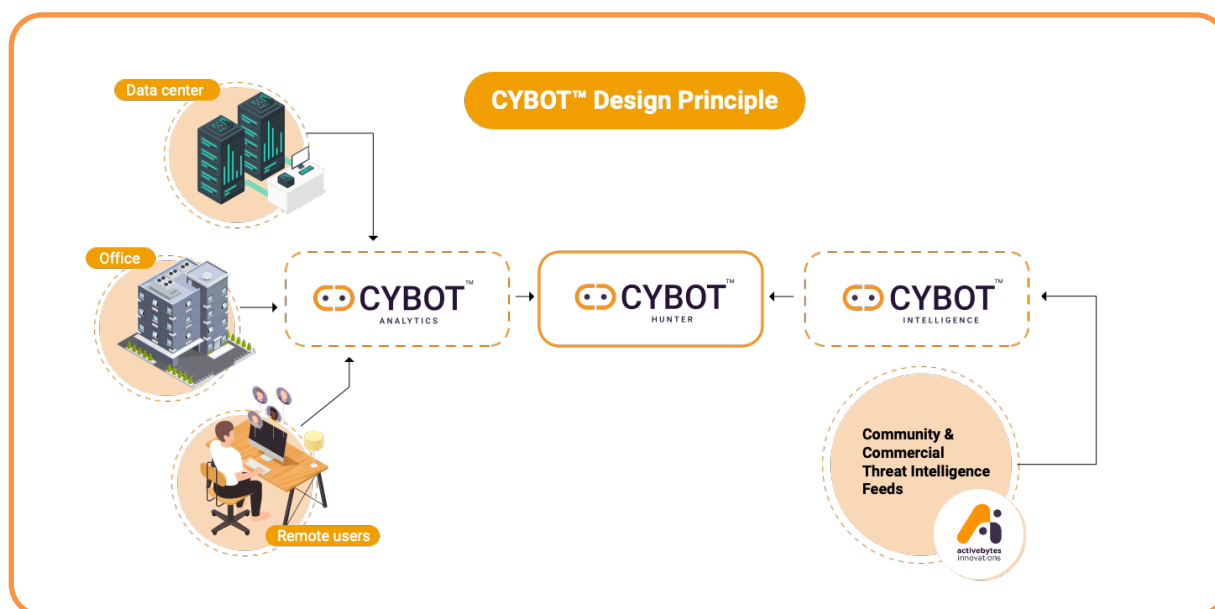
**CYBOT™ Intelligence**



[www.active-bytes.com](http://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.



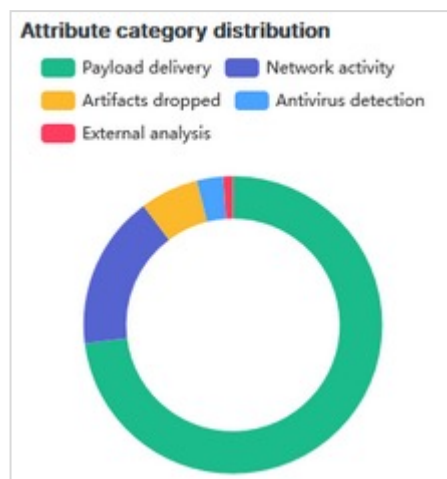
## ✓ CYBOT™ protects your infrastructure from even the darkest corners

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

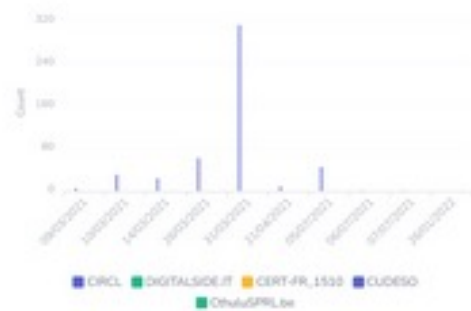
- Receiving and sharing threat intelligence information in a controlled, contextualized and structured manner benefiting the enterprise.
- Receiving threat intelligence information from various open source, dark web sources and this makes CYBOT™ intelligent and adaptive to the latest attack trends.
- 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.

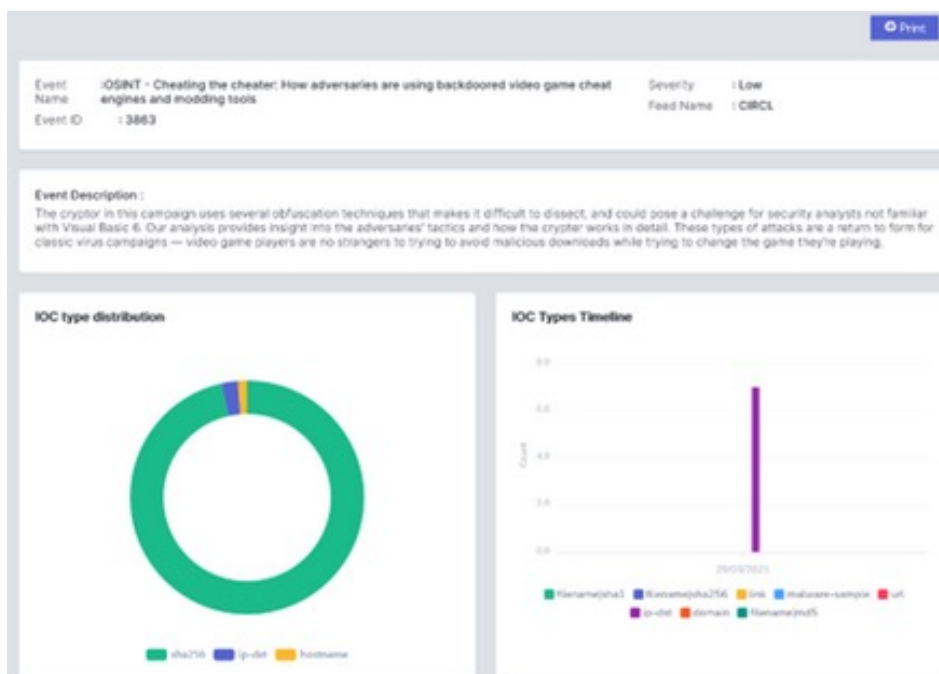
Feeds distribution over time



Attribute category distribution over time



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 foresight_passivedns module.	318066	Jan 19, 1970, 00:43:24 PM
draculax.myip-see.com	hostname	Network activity	draculax.myip-see.com: enriched via the foresight_passivedns module.	318067	Jan 19, 1970, 00:43:24 PM
macross.ddns.net	hostname	Network activity		318068	Jan 19, 1970, 00:43:24 PM
win08.zapto.org	hostname	Network activity	win08.zapto.org: enriched via the foresight_passivedns module.	318069	Jan 19, 1970, 00:43:24 PM
45.163.152.127	ip-dst	Network activity		318070	Jan 19, 1970, 00:43:24 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.

#### Comments

The time to properly investigate and act may exceed your risk tolerance. Even so, develop a relationship with your local law enforcement and FBI offices and discuss the mechanisms and merits of providing the information and evidence they need to take action to help others before they are in the same situation.

A key issue many private firms to cooperate with law enforcement is the lack of feedback or visibility of how their cases are progressing. While this lack of sharing back by law enforcement is understandable due to operational and investigative issues, it can be frustrating for private firms to see little or no return for the time and effort they often expend into assisting law enforcement. Law enforcement need to better understand this and examine ways that firms can see the benefits provided by their cooperation, even if it is just at a high level.

Business is anxious to remediate attacks while law enforcement wants to preserve evidence. These motives are often at odds.

#### Reference Link

- <https://www.scmagazine.com/analysis/cybercrime/doj-wants-to-know-what-are-the-impediments-to-working-with-law-enforcement>
- <https://www.nextgov.com/cybersecurity/2021/10/justice-official-dangles-liability-protections-encourage-private-sector-breach-reports/186253/>



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	
Vulnerabilities and weaknesses in information systems or security infrastructure that could be exploited by a threat source. The following table shows the breakdown of vulnerability information that were obtained from various sources in the given timeframe.	
Show: 5 entries	Search: <input type="text"/>
<b>High-profile Russian APT develops new backdoor tool</b>	
Cisco Talos found a previously undiscovered backdoor from the Turla APT that we are seeing in the wild. This simple backdoor is likely used as a second-chance backdoor to maintain access to the system, even if the primary malware is removed. It could also be used as a second-stage dropper to infect the system with additional malware. The adversaries installed the backdoor as a service on the infected machine. They attempted to operate under the radar by naming the service "Windows Time Service", like the existing Windows service. The backdoor can upload and execute files or exfiltrate files from the infected system. In our review of this malware, the backdoor contacted the command and control (C2) server via an HTTPS encrypted channel every five seconds to check if there were new commands from the operator.	
Reference Link: <a href="https://talosintelligence.com/research/2021/09/27/talos-apt-backdoor">https://talosintelligence.com/research/2021/09/27/talos-apt-backdoor</a>	
Severity: High	
Sep 27, 2021, 8:08:15 PM	
<b>Microsoft releases updated protection for (OMG00) vulnerabilities</b>	
Microsoft updated its patches for the so-called "OMG00" vulnerabilities in Open Management Infrastructure. The most severe vulnerability, CVE-2021-38447, could allow an attacker to execute arbitrary code with SYSTEM privileges.	
Reference Link: <a href="https://www.microsoft.com/security/advisories/Microsoft-security-bulletin-2021-09">https://www.microsoft.com/security/advisories/Microsoft-security-bulletin-2021-09</a>	
Severity: High	
Sep 27, 2021, 8:08:12 PM	
<b>Operation: AmmaPhenox hits Indian subcontinent</b>	
Cisco Talos recently discovered a malicious campaign we're calling "Operation: AmmaPhenox" targeting government employees and military personnel in the Indian subcontinent with its.	
Reference Link: <a href="https://talosintelligence.com/research/2021/09/27/operation-amma-phenox.html">https://talosintelligence.com/research/2021/09/27/operation-amma-phenox.html</a>	
Severity: High	
Oct 7, 2021, 4:37:41 PM	

#### Details

Email Print X

#### High-profile Russian APT develops new backdoor tool

Sep 27, 2021, 8:08:15 PM | Severity: High

#### Vulnerability description:

Cisco Talos found a previously undiscovered backdoor from the Turla APT that we are seeing in the wild. This simple backdoor is likely used as a second-chance backdoor to maintain access to the system, even if the primary malware is removed. It could also be used as a second-stage dropper to infect the system with additional malware. The adversaries installed the backdoor as a service on the infected machine. They attempted to operate under the radar by naming the service "Windows Time Service", like the existing Windows service. The backdoor can upload and execute files or exfiltrate files from the infected system. In our review of this malware, the backdoor contacted the command and control (C2) server via an HTTPS encrypted channel every five seconds to check if there were new commands from the operator.



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

#### Vulnerabilities with exploit

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.

Show 5 entries

Search:

##### XXE Vulnerability in dom4j library

Vendor: dom4j, Oracle and multiple other vendors

dom4j before 2.0.3 and 2.1.x before 2.1.3 allows external DTDs and External Entities by default, which might enable XXE attacks. However, there is popular external documentation R...

Severity: High

Sep 27, 2021, 7:58:21 PM

[View](#)

##### Arbitrary Code Execution Vulnerability in PG Partition Manager

Vendor: pgpm

In the pg\_partition (aka PG Partition Manager) extension before 4.5.1 for PostgreSQL, arbitrary code execution can be achieved via SECURITY DEFINER functions because an explicit stat...

Severity: High

Sep 27, 2021, 7:59:49 PM

[View](#)

##### Command Injection Vulnerability in BTRisk

Vendor: Digen

Btrisk before 0.31.2 allows command execution because of the mishandling of remote hosts filtering SSH commands using ssh\_Restrict.sh in authorized\_keys.

Severity: High

Sep 27, 2021, 8:01:09 PM

[View](#)

#### Details

[Email](#)

[Print](#)

[X](#)

##### XXE Vulnerability in dom4j library

Sep 27, 2021, 7:58:21 PM | Severity: High

##### Vulnerability description:

dom4j before 2.0.3 and 2.1.x before 2.1.3 allows external DTDs and External Entities by default, which might enable XXE attacks. However, there is popular external documentation from OWASP showing how to enable the safe, non-default behavior in any application that uses dom4j.

##### CVE:

2020-10683

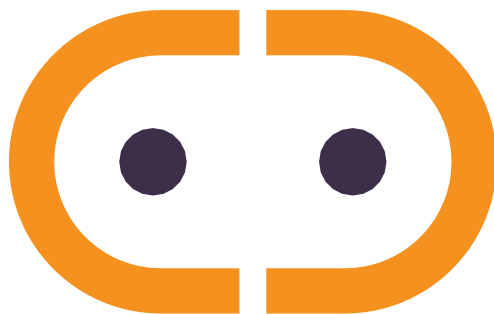
##### CVSS:

CVSS v3.1 Base Score: 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

##### Vendor:

dom4j, Oracle and multiple other vendors





[www.active-bytes.com](http://www.active-bytes.com) / [contact@active-bytes.com](mailto:contact@active-bytes.com)

+971 50 513 3973

---