JUCY sandbox

The Next Generation of Sandbox combining Unkown Cyber's Genomic Static Analysis, Dyanamic Analysis and AI.

	CORE FEATURES	
√	**Windows 10 64bit**	**JUCY Sandbox 3.0** has over 30 customized analysis packages. These packages guide the analysis process for each sample, specifying which actions to take and what data to collect during the analysis. This sets the conditions necessary for comprehensive examination by defeating anti-analysis techniques. After triggering malware to launch, JUCY Sandbox analyzes behavior through the multiple stages of the attack. If desired users may direct the use of specific analysis packages. However, when no package is specified JUCY Sandbox will automatically select packages based on the target file type to fully automate the investigation.
Coming in JUCY 3.1 (weeks)	**Windows 7 32bit**	
Coming in JUCY 3.1 (weeks)	**Windows 11 64 bit**	
√	**Genomic Analysis** **Windows** **Mac** **Linux**	That's not all! JUCY Sandbox capabilities go beyond the limitations of traditional sandboxes by providing the genomic static analysis capabilities of Unknown Cyber. This additional analysis consists of deep inspection of binaries regardless of environment. Users receive a statistical comparison of the code in the files submitted to the code of known malware. This allows environment agnostic analysis of Windows, Linux, and Mac executable formats in almost every architecture to include: Intel 32 and 64-bit, .Net, Apple, MIPS, Motorola, and more.
√	**Video Record**	JUCY Sandbox Large Enterprise allows customers to record complete investigations on video. Investigations which are recorded can be played back to show all actions conducted during each analysis runtime. Videos may be downloaded for dissemination or used in the presentation of findings.

√	**User Interaction**	User Interaction JUCY Sandbox's user interaction lets you operate the machine while it's under attack. These features allow users to run additional programs or conduct any actions desired within the JUCY Sandbox environment. Beyond our simulated interaction capabilities user interaction allows the analyst to fully control the actions performed in the investigation.
√	**Screen Shots/ Capture**	Throughout the entire analysis, screenshots are captured when notable actions are sensed. Screenshot/ Capture is available for both human interactive sessions or those conducted using simulated user interaction. All screenshots are provided in the automated report of findings at the conclusion of analysis.
√	**MITRE ATT&CK Mapping**	MITRE ATT&CK Mapping A comprehensive understanding of the Tactics and Techniques used in attacks is very important for threat analytics. JUCY Sandbox returns the observed Tactics and Techniques mapped to the MITRE ATT&CK Matrix. If you wish to further map code to these techniques our Genomic BO Query uses AI to track and interpret specific malicious functions and explain where they are and what they do. You can also use this information to create bytecode YARA rules for use with compatible IDS, and SIEM.
√	**Unlimited Analysis**	Unlimited Analysis JUCY Sandbox Large Enterprise has no limits on the number of manual submissions or resubmissions for analysis.

√	**Malware Configuration**	Malware Configuration The malware configuration is the information extracted from the memory of a malicious object. Benefits: • Complete information about malware • Combined IOCs collection • Data from broken or sleeping samples
√	**Timeout**	Timeout Not all malicious programs are active right after launch. Some of them require additional actions from a user. With JUCY Sandbox you can select the time needed to perform the planned steps for interaction and analysis.
√	**File Size**	File Size We support 30 megabyte files by default. Users will have the option to upload larger files by selection.
√	**Export Samples and PCAP (manual only)**	Export Samples and PCAP Supports: • RAW • PCAP • PCAP NG with TLS • Upload or download of samples • Full network activity record (PCAP)
√	**Text reports**	Text Reports Receive comprehensive information from JUCY Sandbox's analysis with all indicators of compromises, a process tree, and screenshots. These results are available to download for dissemination.

√	**Script Tracer**	Script Tracer JUCY Sandbox's script tracer makes it easy to trace and de-obfuscate the execution flow of scripting languages. Supported: - JScript - VB Script - VBA - PowerShell - Python - Macro 4.0.
√	**URL Analysis of Different Browsers**	Receive URL Analysis of Different Browsers Supports: - Internet Explorer - Edge - Chrome - Firefox Checking suspicious URLs in only one browser may miss certain attack vectors.
	ADVANCED FEATURES	
√	**Privacy**	Privacy JUCY Sandbox Large Enterprise customers have their own private stand-alone server for all sandboxing operations. No information is shared outside of the organization without the consent of the customer.
Feature Request	**MITM Proxy for HTTPS**	MITM Proxy for HTTPS Requests Many malicious applications use secure connections to conduct C2. MITM allows analysis inside the TLS protocol to get domains, links, and request headers, as well as the content of connections to the command and control server.

	GENOMIC FEATURES & THREAT INTELLIGENCE	
√	**Genomic Matching**	Genomic Matching Match malware by statistical similarity in code to identify malware which have repurposed the same malicious code. Receive Match Score to immediately know the number of malware that match the suspect file. Set rules to automatically send the hashes of malware with 100% statistical similarity to IDS or SIEM. Automatically create bytecode YARA signatures to block or hunt other malware variants. Pivot from the matched malware with automated threat intelligence to harden defenses by passing other IOCs captured from matching malware to IDS or SIEM. TI Features discussed in Search and Association include: • Thousands of Malicious Matching File Hashes • Malicious Matching IP Addresses • Malicious Matching URLs
√	**Code Watchlist**	Code Watchlist Know when a file submitted for analysis uses code that matches a particular malware of interest. • User tip: The adversary repurposes malware. We routinely see new malware that is 100% similar to malware created many years ago but is not yet detected by leading AV and Sandboxes. Get notified when it appears in your watchlist!
√	**Automated Hunt Signatures**	Automated Hunt Signatures From the code of any malware, automatically create bytecode YARA signatures to harden or hunt.

		Our signatures can be passed to IDS or SIEM to protect from the next malware variant. They can also be used to accelerate the proactive hunt activities of your organization. There is no faster way to create highly accurate YARA to stop the next threat. Our signatures can also be used post incident to eradicate other variants the adversary may have planted in your infrastructure. Our signatures can also be used to find malware in memory. Our imbedded Command Line Tool allows easy deployment of YARA Signatures for hunting.
√	**Hash Match**	Hash Match From any malicious file collect and deliver by API all other matched malicious file hashes of known malware.
√	**Malicious Function ID**	Malicious Function ID Our genomic analysis goes deep! Identify amongst billions of functions an individual function that has been added to change an otherwise safe program into one that is malicious. You can see this in our example where we matched a file and identified the one additional function that had trojanized the program. This capability helps assure software is not counterfeit and does not contain malicious functionality.
√	**Malicious Function Search**	Malicious Function Search Any function can be searched across our community database or any of a customer's private files to see all files that contain the same function or functions.
√	**Function YARA**	Function YARA From any function a YARA rule can be automatically created to pass to IDS or SIEM. These rules may also be used to hunt captured memory snapshots for the function of interest.

√	**Function Tagging - IDA/ Ghidra Plugins**	Function Tagging - IDA/ Ghidra Plugins Functions can be tagged by users and interacted with through our IDA and Ghidra Plugins.
√	**Threat Intel Search**	Threat Intel Search Threat Intel Search lets you link intelligence from other files through search queries and code similarity. This is a unique capability because similarity intelligence allows the creation of new intelligence. With Threat Intel Search you gain insights into malware activities through association. Our search allows the identification of suspicious connections and generation of new IOCs which are not available without genomics. With traditional search methods when you search on URL or IP, the information returned is limited to files that have the same URL or IP. Adding matched statistical similarity of code is extremely useful because threat actors change URL and IP addresses causing intelligence derived from these alone to become stale. Pivoting on similarity of code allows you to search and find new malware even if they have updated C2. Matches on similarity are not fragile. Similarity is immutable reliable intelligence for formulating pivots, and early identification. Similarity can likewise be used to find new URL and IP used in new variants of malware along with corresponding hashes of code-matched files and other IOCs. Similarity allows users to generate threat intelligence about their own organization. From a file which carries a malicious URL, users immediately see the number of matched files in the last 30, 60, or 90 days which are malware created from the same code. This campaign information allows automatic creation of YARA rules to proactively protect from the next attack. This situational understanding, only available through the comparison of code, gives users actionable information regarding the exposure their organization is experiencing from a specific persistent malware. Quickly connect isolated indicators and code matched through similarity to known real-world attacks and malware families.

√	**Threat Intel Association**	Threat Intel Association Link isolated TTPs to known threats with contextual data such as related malware family names, and other recorded interactive sandbox sessions where these threats were identified.
√	**Ask BO**	Ask BO Why ask BO? Because BO knows code. A BO query can be requested for any function or group of functions to produce an LLM generated human readable report of the code’s functionality.
	EXTENDED ANALYSIS	
√	**Memory Capture**	Memory Capture Capture full memory dumps of the target system.
√	**Memory Hunt Signatures**	Memory Hunt Signatures Genomic comparison of binary code allows the automatic creation of bytecode YARA signatures to hunt memory.
√	**Monitoring of System Processes**	Monitoring of System Processes. JUCY Sandbox monitors every process that interacts with a system function to provide complete monitoring of all system actions and capture which processes are created, accessed, or modified during execution.
√	**File Capture**	File Capture Capture files that are created, modified and deleted during execution.

√	**Network Traffic Capture**	Network Traffic Capture Network traffic is captured and exportable in PCAP format.
√	**Always Priority in Queue**	Always Priority in Queue Always First! Because JUCY Sandbox Large Enterprise customers have their own private stand-alone server they are always first in line for sandbox analysis.
√	**Automated or User Selected Analysis Packs**	Automated or User Selected Analysis Packs JUCY Sandbox runs over 30 different analysis packages which are combined with the software needed to support their dependencies. Users can have these packages automatically selected and run by default. Users also have the option to specifically select the packages they wish to use in analysis.
√	**Automated Interactivity**	Automated Interactivity In both analysis sessions launched via the API and in the interface, JUCY Sandbox can automatically click through interactive elements, links in documents visible to the user, or buttons in an installer.
	API/ EXPORTS	
√	**REST API**	REST API Our API enables you to integrate JUCY Sandbox into your malware analysis framework. API allows DFIR specialists to automatically submit files and URLs for analysis and then automatically pivot to collect associated IOCs of other malware that may use a different URL or other matched IOC but are linked through code. This minimizes the required time for research and delivers new information on which you can act.

√	**JSON Reports**	JSON Reports The JUCY JSON report contains all available information of sandbox analysis as well as links to the content. The report also contains the main indicators of compromise (IOCs) detected for easy export and sharing.
Feature Request	**Export to MISP Format**	Export to MISP Format If you conduct a high volume of analysis sessions JUCY Sandbox allows you to download all significant events in MISP for further analysis for export to IDS or SIEM systems and easy dissemination.
√	**HTML Document**	HTML Document JUCY reports are available for download in HTML format.
Feature Request	**Common Analysis History via API**	Common Analysis History via API Gain transparent visibility into your team's analysis activity and retrieve the analysis, history, and IOCs for all users via API.
	ADDITIONAL SERVICES	
√	**Premium Support**	Premium Support • Extended technical assistance and support resources to optimize performance, and solve problems faster. • 24-hour response time (working hours) • Dedicated account manager • Highly qualified technical experts