Kaspersky®
Anti Targeted
Attack Platform

KATA 2.0 What's New

Top 5

Prevention: Integration with Kaspersky Secure Mail Gateway
Great Web Interface
Sandbox Clustering
VMware ESXi support
Rescan of previously captured objects and network communications

Prevention

Integration with KSMG – helps to prevent targeted attacks from happening

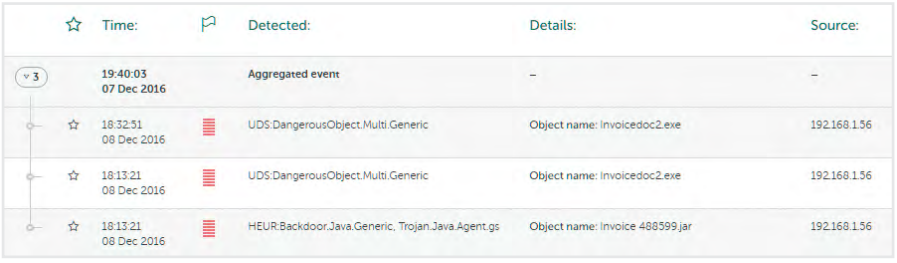
KATA 2.0 gets integration with Kaspersky Secure Mail Gateway appliance, email system & mail security solution by Kaspersky Lab.

Now KSMG provides not only innovative cloud-assisted Anti-Spam, Anti-Phishing and advanced multi-layered Anti-Malware protection with Zero-day and anti-exploit capabilities, but also allows leveraging KATA 2.0 Clustered Sandbox environment to detonate samples from email traffic.

Interface and workflow

Great web interface – for effortless workflow and clear visibility

KATA 2.0 introduces completely redesigned interface and greatly improved incidents workflow. Related events, which are part of one incident, are now collapsed in one Aggregated event to give visibility without overloading sight with irrelevant information.



A number of customizable **Dashboards** provide insight into system work and analysis results:

- system and components health and activity, queues lengths and performance
- on events registered, status and technologies used to provide verdict, incidents assignment
- top lists of IPs, domains, emails related to incidents

Notifications on incidents* – to instantly inform Security Team of important discovery

KATA 2.0 introduces email notifications for Security Officers about events discovered in various systems inside corporate network.

Flexible customized rules (according to technology responsible for verdict, severity level, etc.) allow providing only relevant information to each given email account.

Downloadable reports* – to demonstrate results for senior management

All valuable information from dashboards of KATA 2.0 can be provided as downloadable report to give overview of the system health and overall results.

Statistics on registered events and technologies responsible for verdicts, top lists of systems attacked – ready for demonstration to C-level staff.

Marking most critical system and personnel – for extra careful examination

With KATA 2.0 Security Team gets possibility to explicitly mark the most critical and important (VIP) resources, including systems, servers, staff members, etc.

Events with these resources involved can be managed and tracked with extra caution, responsible personnel to be notified according to different rules.

Role-based access control – enterprise-level scenarios to safeguard sensitive data

Multiple KATA 2.0 users can be assigned with different roles and privileges sets.

This allows separating duties according to access level and preserving sensitive corporate data, such as personally identifiable information (PII), sensitive personal information (SPI), and contents of communications.

Integration

Full support of VMware ESXi* – to be flexible and allocate resources for poc with ease

From now on KATA Platform fully supports virtualized environments and can be deployed in VMware vSphere infrastructure, in parallel with Kaspersky Private Security Network.

Sandbox Clustering – to ensure prompt objects detonation

Allocating multiple Sandbox servers allows KATA 2.0 to process large amounts of network objects and to efficiently serve in heavy loaded networks.

KES 10 SP2 as Endpoint Sensor – to ease integration for existing KL customers

Kaspersky Endpoint Security 10 SP2 can be employed as Endpoint Agent to provide KATA 2.0 with valuable information about files, processes and communications running on monitored machines. Centralized management of Kaspersky Endpoint Security 10 SP2 Endpoint Sensors settings via Kaspersky Security Center 10 SP2 MR1 is available.

Improved email integration – to monitor effortlessly most important communications

SMTP email integration allows KATA 2.0 to support seamless pairing into customer email infrastructure without hustle for email systems administrators.

Important additional integration scenario supported in KATA 2.0 – extracting SMTP flow directly from mirrored SPAN traffic from perimeter network devices. In this situation, involvement of email system administrator is not required at all.

Integration with LIghtweight KPSN 2.0 * – to run poc in restricted environments

New lowered KPSN 2.0 requirements allow to conduct Proof of Concept and deploy KATA system for Production in a number of corporate environments with extremely restrictive data policies.

Detection

Rescan of previously captured objects and network communications*

Network communications data and objects are stored in KATA 2.0 and rescanned periodically. If the incident escaped detection the day before yesterday, it will be discovered today with updated information from KL.

This provides better visibility into recent events and allows detecting traces of malicious activity retrospectively (backwards in time) using current latest Threat Intelligence data.

Enhanced events correlation – connecting the dots to see a bigger picture

KATA 2.0 introduces new possibilities to correlate events generated by multiple components by means of Targeted Attack Analyzer.

For example, if particular executable behavior raises concern (while being detonated in Sandbox environment), its process communicates to dangerous Internet resources, if the traces of very similar communications were discovered in network traffic (in future or in the past), Security Team will be notified of this discovery and provided with a list of machines generated this communications.

Another scenario – if file was considered as suspicious after Sandbox detonation, and the same object was later executed or opened on one of the machines, Security Team will be notified on this incident and provided with the list of computers, which have this object stored.

Scanning password-protected attachments in email messages – to discover everything

Attackers often use the trick of encrypting malicious files and documents inside password-protected archives to pass through security systems.

Password-protected and encrypted archives in network traffic are extracted in KATA 2.0 and their contents are detonated in Sandbox.

URLs In email messages scanning – to discover hidden targeted threats

Links in email messages may look innocuous, but often they lead to custom-build malware or tailored sinkhole or phishing websites.

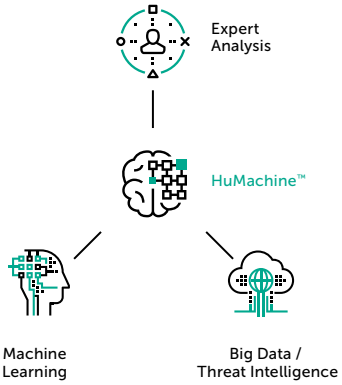
In KATA 2.0 dangerous web links in email messages are thoroughly investigated. Objects downloaded via this addresses are detonated and examined with scrutiny in KATA 2.0 Sandbox environment. Additionally, URLs are checked using URL reputation service in Kaspersky (Private) Security Network.

Whitelisting – to hide irrelevant data from analysis and remove unnecessary load

With KATA 2.0 administrators can easily exclude from scanning certain files types and resources, such as legitimate network vulnerability scanners, IT security systems and so forth.

* Marked features will be available **only with the Technical Release** of KATA 2.0 (planned for 1st of March 2017). Pilot-ready Release Candidate (December 2016) does not include these:

- Notifications on incidents
- Downloadable reports
- Full support of VMware ESXi
- Integration with Lightweight KPSN 2.0
- KES 10 SP2 as Endpoint Sensor
- Rescan of previously captured objects and network communications



All about Internet security: **www.securelist.com**
Find a partner near you: **www.kaspersky.com/buyoffline**

www.kaspersky.com
#truecybersecurity