SGBOX NEXT GENERATION SIEM

ALL IN ONE PLATFORM

AVAILABLE ON-PREMISE AND MULTITENANT

SGBOX

SIEM AS YOU NEED

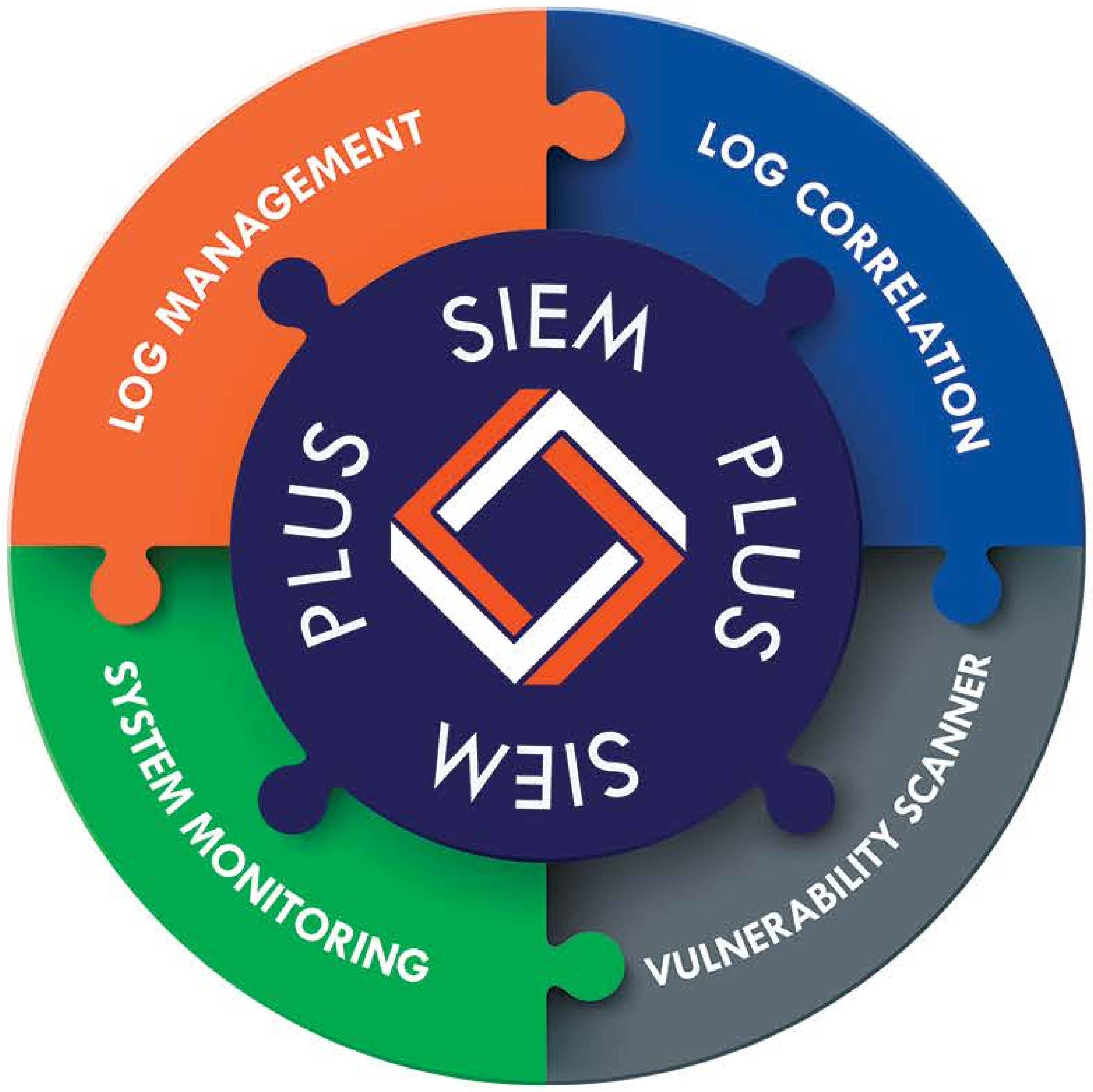
SGBox is a software platform to gain network visibility by collecting and aggregating information from any IT infrastructure component, offering real time analysis and correlation capabilities to mitigate security risk and respond to threats. SGBox provides a vulnerability scanning service to reduce the data breach risk, supporting the IT staff on making decisions, providing visibility of the network security posture. SGBox is intuitive and easy to manage to avoid complex configurations and reduce administrative cost ensuring a predictable license cost.

SECURITY CONTROL MANAGEMENT

As well as managing all SGBox capabilities and remote collectors, the control management provides important shared functions. The console can manage dashboard, devices for data collection and monitoring, both local or geographically distributed vulnerability scans. Users are authenticated on external directories such as LDAP or Active Directory, assigning them user profiles to ensure granular permissions to each single SGBox functionality.

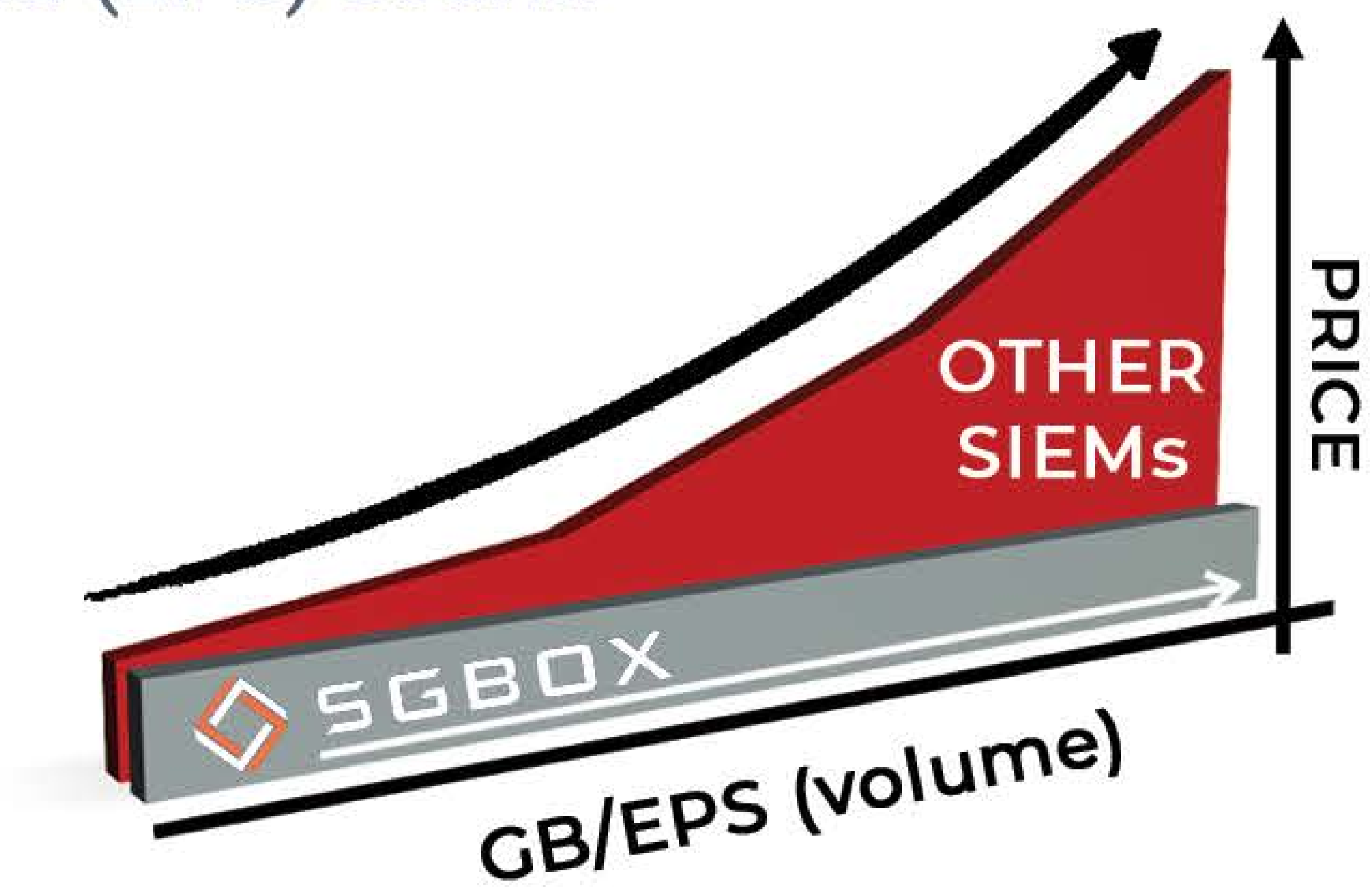
USER ACTIVITY MONITORING

Easy and fast tracking of user activities to summarize the potential anomalous behavior.



PREDICTABLE PRICE

The first SIEM at a predicable price and transparent licensing model. The license cost is based on the total number of devices sending logs, not on the obsolete volume of data or event per second (EPS) count.



MULTI-TENANCY AND PERSONALIZED VIEWS

As a fully multi-tenant solution, SGBox System Monitoring allows collection and integration of metrics from multiple customer sites and geographically dispersed locations into a single web console.

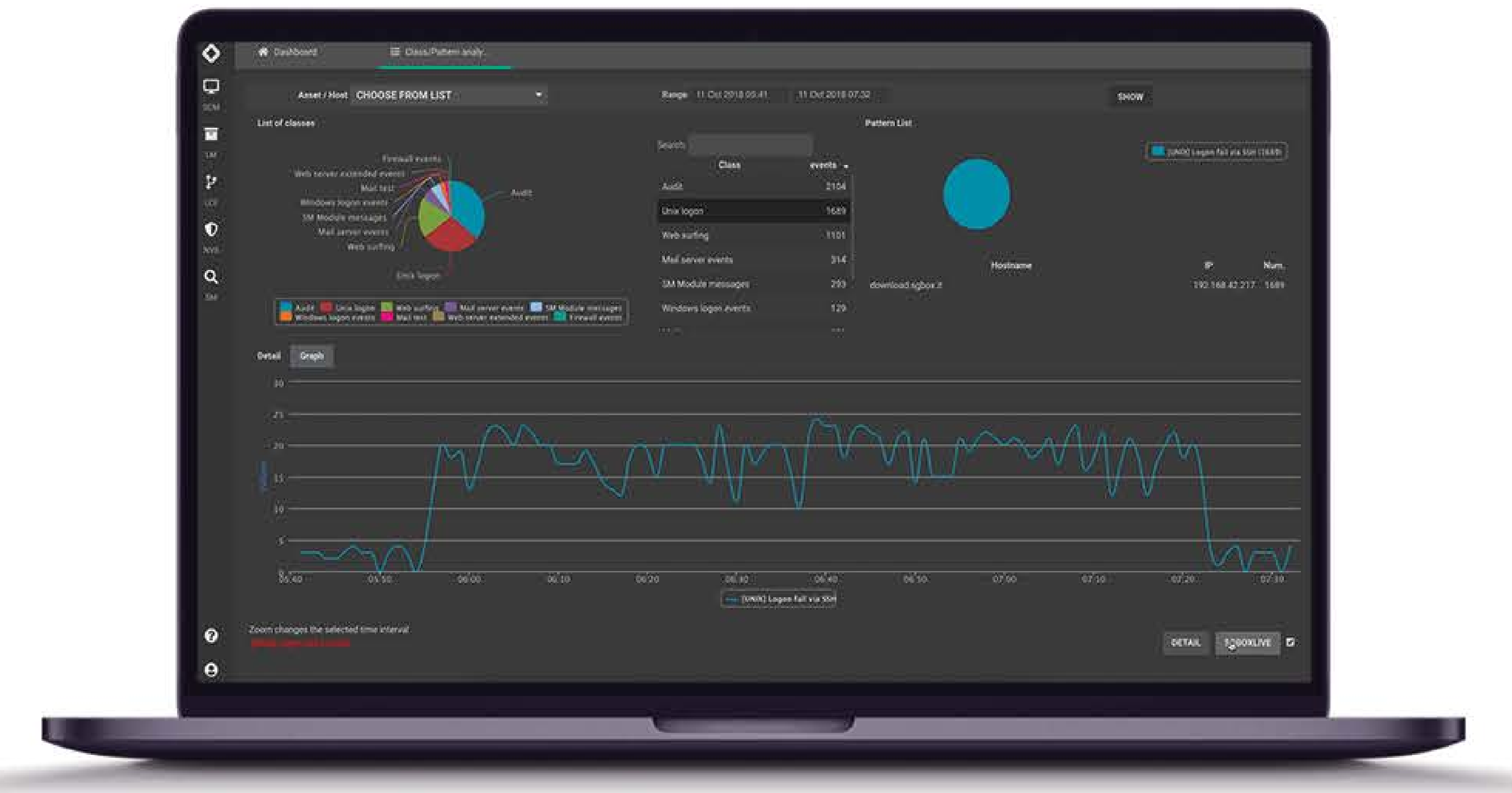
Each customer gets a personalized view to monitor, alert and report on the state of their infrastructure—network, servers, applications, etc. Administrators can also be assigned limited rights to set baselines and configure monitoring for the segments of the IT infrastructure for which they have management access.

LOG MANAGEMENT (LM)

An high log volume ingestion engine to streamline the process of log collection, centralization, monitoring and analysis. SGBox Log Management can manage events from any kind of data source such as OS's, applications, network devices, IoT sensors, security components, etc.. Users accelerate troubleshooting efforts with relevant data from across the network environment, with dynamic indexing policies that make it cost-effective to collect, inspect, and store all the logs. SGBox also empowers administrators providing detailed comprehensive reports on security events and in a turn of a key can adopt countermeasures to mitigate security threats.

DYNAMIC SEARCHES

Possibility to drill-down events, starting from an overview of historical data, zooming in detail to analyze the single event. Selecting a parameter in the event flow will change the view allowing advanced searches.



Class	events
Audit	2104
Unix logon	1689
Web surfing	1101
Mail server events	314
SM Module messages	293
Windows logon events	129

Hostname	IP	Num.
download.sgbox.it	192.168.42.217	1689

Zoom changes the selected time interval

NETWORK & HOST THREAT DETECTION

SGBox is able to detect relevant threats such as successful user privileged gains, web application attacks, network trojan, DOS attacks, potential corporate privacy violations, file integrity monitoring, rootkit and others.

COMPLIANCE

SGBox helps customers in the process of compliance to main regulations such as GDPR, ISO27001, SAMA, PCI-DSS, etc. A set of out-of-the-box reports are ready to use.

NO LIMITATIONS ON LOG TYPE

SGBox is able to collect any kind of log data format, without any limitation. In case of unknown log formats, (i.e. custom applications) the SGBox laboratories may generate the appropriate parser. SGBox also provides all the needed tools to allow the customer or partner to create a custom pattern by themselves.

SIGN AND ENCRYPTION

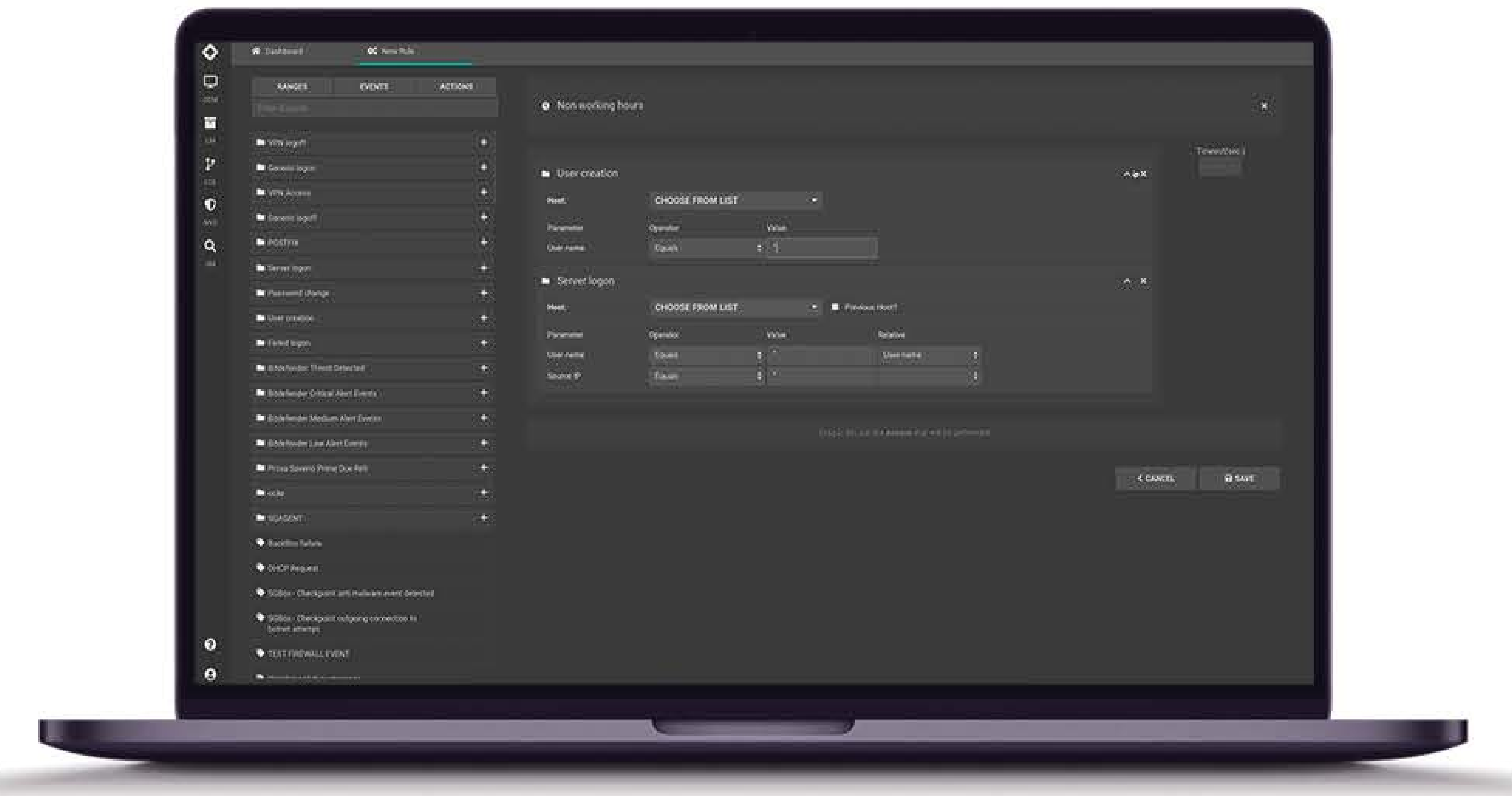
Efficient log encryption and asymmetric signing capabilities to ensure the integrity of the stored data.

EVENT CORRELATION (LCE)

Networks create lots of events. Events can be SNMP traps generated by a server rebooting, syslog messages, Microsoft event logs etc. How do you know which events are important? The ones telling you something important? That is where event correlation engine come in handy. This component is automatically fed with events originating from managed elements (applications and devices), monitoring tools and vulnerability scanners. Each event captures something special that happened in the domain of interest to the event correlator, which will vary depending upon the type of analysis the correlator is attempting to perform. SGBox provides an advanced correlation engine to describe anomalous scenarios, detect and activate automated responses to threats.

RULE-BASED EVENT CORRELATION

Correlate all events, along with contextual information such as identity, roles, vulnerabilities, device monitoring alarms and more, to detect scenarios indicative of a threat.



THREAT AUTOMATED RESPONSE

The correlation engine even hosts the capability to engage automated response in case of threats by launching scripts or interacting with external security components via API to mitigate threats. Furthermore the correlation engine can activate SGBox apps to interact with external tools.

SGBOX API

SGBox exposes API's to allow external tools to retrieve information on alarms and events from the internal of SGBox to make more analysis.

SOAR INTEGRATION

SGBox can be interoperable with SOAR solutions (Security Operations Automation Response) to feed those platforms providing meaningful information.

ONLINE AND HYSTORICAL DATA CORRELATION

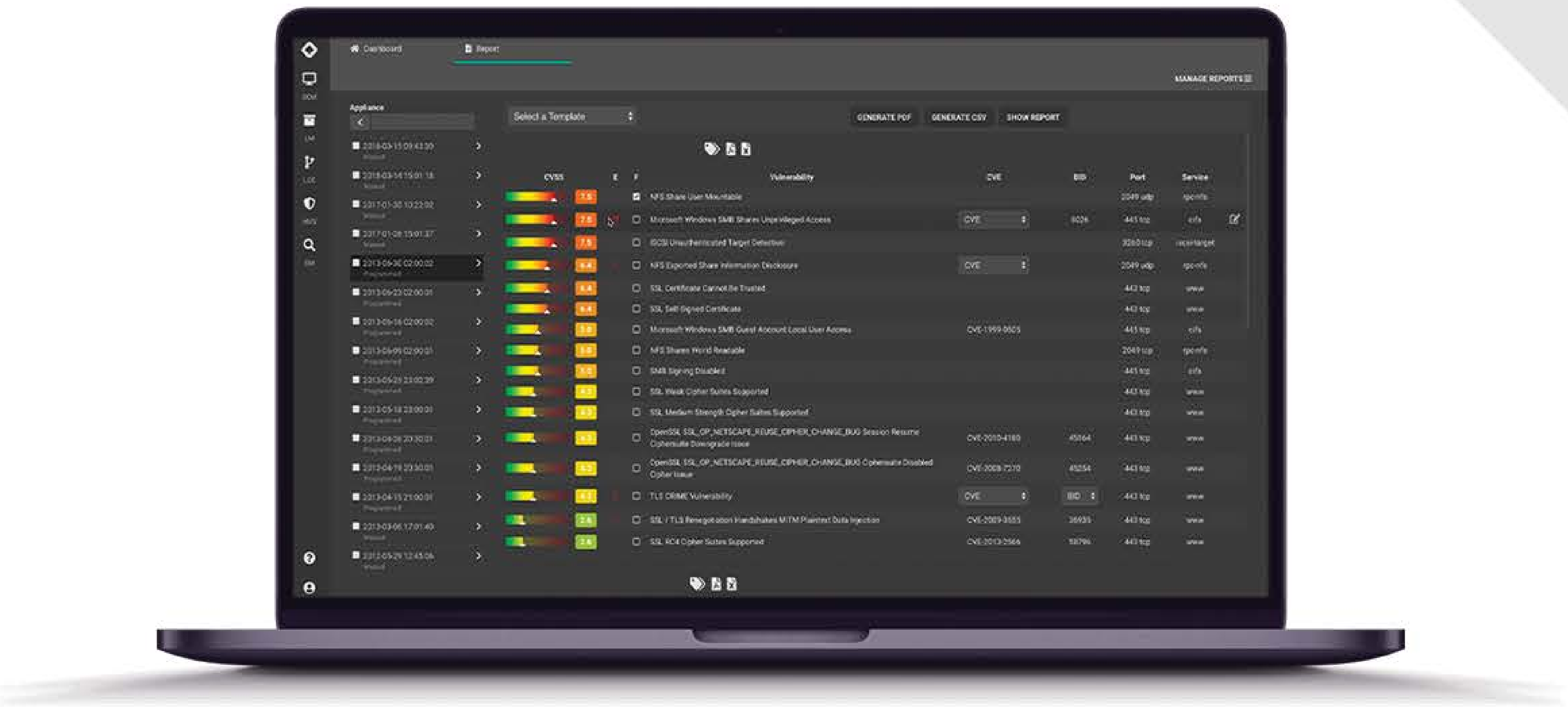
The correlation rules can be applied both real time data and historical to allow forensic analysis.

NETWORK VULNERABILITY SCANNER (NVS)

A Vulnerability Scanner is available into the SGBox Next Generation SIEM to assess computers, networks or applications for known weaknesses, simplifying the administrative efforts. SGBox identifies and detects vulnerabilities arising from mis-configurations within a network-based asset such as a firewall, router, web server, application server, etc., allowing both authenticated and unauthenticated scans. SGBox Vulnerability Scanner is also available as SaaS (Software as a Service), provided over the internet and delivered as a web application and provides the possibility to customize vulnerability reports.

CUSTOMIZABLE REPORTS

Possibility to define personalized reports based on different level of details on vulnerabilities and remediations to deliver to the different IT Staff profiles.



CVSS	E	F	Vulnerability	CVE	BID	Port	Service
7.5		☑	NFS Share User Mountable			2049 udp	rpc-nfs
7.5		☐	Microsoft Windows SMB Shares Unprivileged Access	CVE	8026	445 tcp	cifs
7.5		☐	iSCSI Unauthenticated Target Detection			3260 tcp	iscsi-target
6.4		☐	NFS Exported Share Information Disclosure	CVE		2049 udp	rpc-nfs
6.4		☐	SSL Certificate Cannot Be Trusted			443 tcp	www
6.4		☐	SSL Self Signed Certificate			443 tcp	www
5.0		☐	Microsoft Windows SMB Guest Account Local User Access	CVE-1999-0505		445 tcp	cifs
5.0		☐	NFS Shares World Readable			2049 tcp	rpc-nfs
5.0		☐	SMB Signing Disabled			445 tcp	cifs
4.3		☐	SSL Weak Cipher Suites Supported			443 tcp	www
4.3		☐	SSL Medium Strength Cipher Suites Supported			443 tcp	www
4.3		☐	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	CVE-2010-4180	45164	443 tcp	www
4.3		☐	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Ciphersuite Disabled Cipher Issue	CVE-2008-7270	45254	443 tcp	www
4.3		☐	TLS CRIME Vulnerability	CVE	BID	443 tcp	www
2.6		☐	SSL / TLS Renegotiation Handshakes MITM Plaintext Data Injection	CVE-2009-3555	36935	443 tcp	www
2.6		☐	SSL RC4 Cipher Suites Supported	CVE-2013-2566	58796	443 tcp	www

GROUPS OF ASSETS

SGBox allows the creation of group of assets to differentiate the scanning policies and scheduling, coupling each group with one or more admins that will get the reports and alerts based on predefined policies.

CVSS & REMOTE SCANS

SGBox Vulnerability Scanner uses the Common Vulnerability Scoring System (CVSS) to attribute a score to each assessed asset, group and overall.

COMPLIANCE SCANS

SGBox is ready to support the compliance requirements of major regulations such as GDPR, SAMA Cyber Security Framework, PCI-DSS, ISO27001, etc. Several compliance reports available out-of-the-box.

TREND & DIFFERENTIAL REPORTS

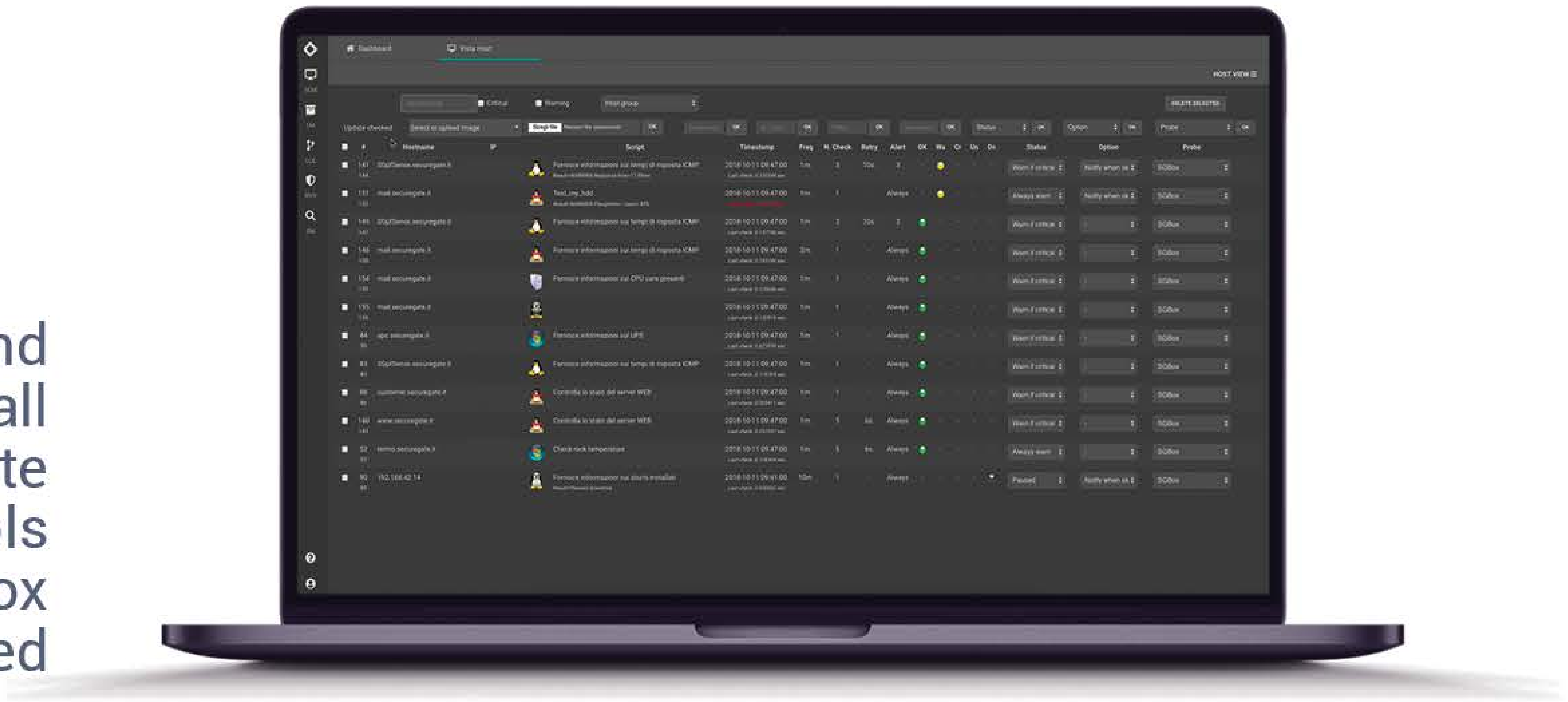
Incremental reports can be generated to highlight the vulnerability trend, the differential reports indicate the fixed problems and scoring between two or more scans.

SYSTEM MONITORING (SM)

SGBox System Monitoring performs a variety of more granular functions that fall under network and application monitoring, using the SNMP protocol and embedded proprietary controls. The System Monitoring capability also monitor a range of devices including servers, storage devices, desktop computers, printers and mobile devices. All of these monitoring activities provide notifications for technicians and control rooms when there is a network failure or system malfunction. The System Monitoring tool also includes thresholds to activate alarms and allows to take hardware and software inventory devices.

100% WEB-BASED ARCHITECTURE

SGBox System Monitoring is hassle-free and does not require extensive policy and firewall reconfigurations to collect and communicate metrics. Since it uses standard web protocols (HTTP/HTTPS) for all communications, SGBox allows monitoring of servers that are deployed within a private network or in the public cloud.



REAL TIME MONITORING

With a huge amount of built-in network performance checks, monitor health and critical metrics such as packet loss, latency, speed, errors and discards and analyze performance bottlenecks.

TRESHOLDS

Thresholds must be defined for every alarm with the corresponding parameters and levels to get instant alerts for violation.

MONITORING COLLECTORS

SGBox System Monitoring can adopt remote collectors to perform monitoring checks on complex and geographical distributed networks.

EASY SETUP AND TRASPARENT COST

The SGBox System Monitoring is fast and easy to setup and maintain, avoiding huge amounts of professional services to increase the TCO. As all the SGBox solution even the system monitor cost is based on a per-device pricing model to ensure a transparent predictable price.

USER BEHAVIOR ANALYTICS (UBA)

The SGBox UBA application is designed to define a baseline for each user and events related to the user, to create a reference and identify normal or anomalous behavior. Each event is evaluated through the related user's history, taking into account the environment, frequency, quantity, behavior of other users on the same situation and other factors. The UBA detects whether what is occurring is normal or not, if it is statistically acceptable by associating a risk factor to each action. UBA helps to survey the user's behavior also considering the meaning of that action.

PERFECT SGBOX INTEGRATION

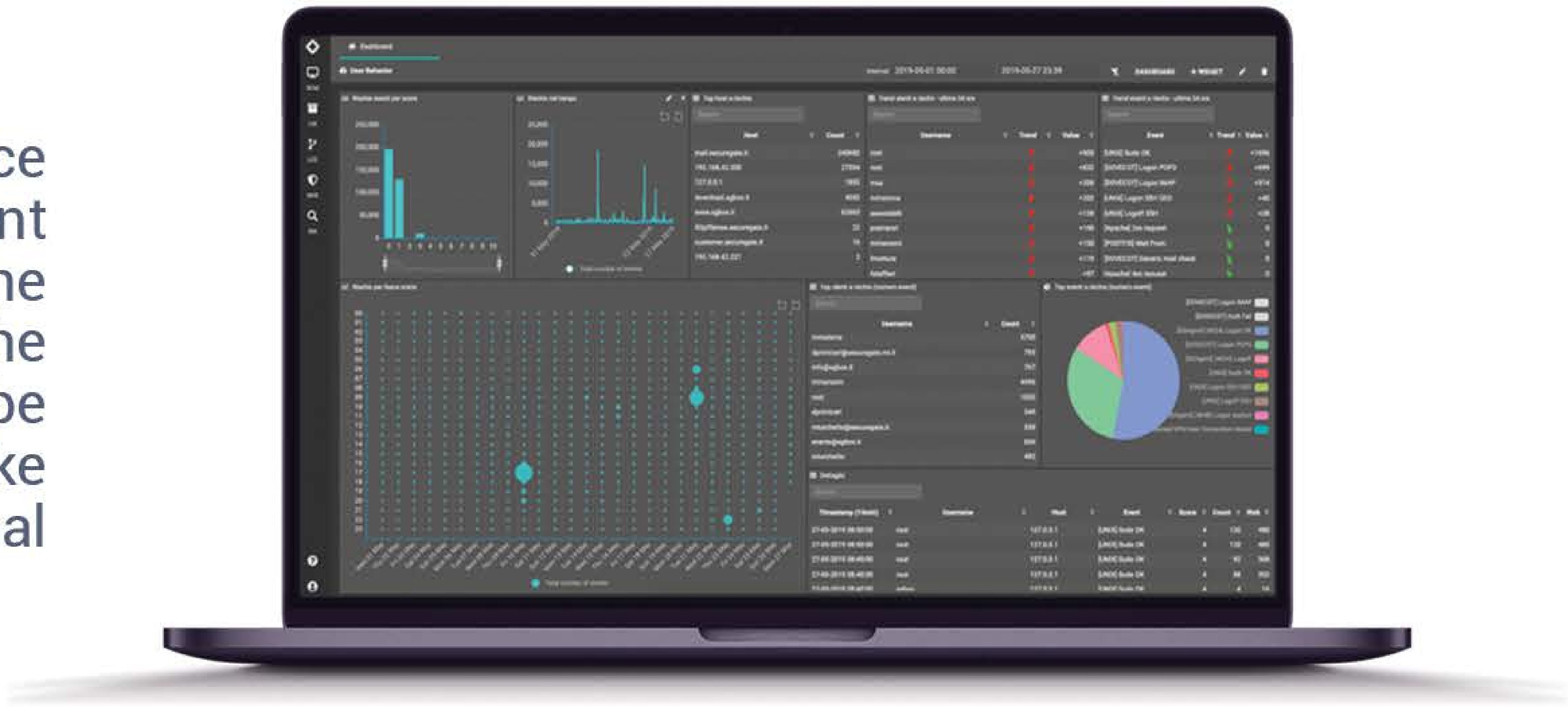
Interaction by the user is not needed, since SGBox UBA automatically checks for all different situations. All the anomalies discovered by the UBA app, become events that can be used in the LCE correlation system. Events from UBA can be part or start any complex correlation rule, to take reactions, send alarms or interact with external tools by calling their API.

TACTICAL DASHBOARD

The SGBox dashboard system is used to display the various aspects of the UBA application. By enabling the app, the user will be able to add a series of new high-level widgets that will allow him to view information about the behavior in different ways, including a timeline and trend objects.

USER RELATED RISK

User behavior is also associated to risk categories to define a priority, based on the meaning of a particular event, not only on its volume. A set of dedicated widgets show, together with trend indicators, the risk associated to users, events and hosts impacted by user's activity.



HUMAN READABLE ALARMS

Real time anomalies are also displayed in a human readable form, so you will discover that: *"User John is involved in a privilege escalation event. This is the first time we've seen John in this situation. This normally does not happen at 3AM. This leads us to think that this is a serious anomaly"*.

SIMPLE MULTI FILTER SEARCHES

User can apply filters on any object in the widget set by simply selecting the host or event or user he's looking for. Dashboard will automatically reflect user' selections and will highlight the meaningful information to allow a quick discover of the anomalies.

THE VALUE OF OUR COMPANY

At SGBox we work with passion and serve all the customers with the same attention, we believe a satisfied customer is the best way to carry our philosophy. We are committed to research and innovate to offer our customers easy and effective solutions.

SGBOX IS TCO FRIENDLY

If compared to other competitor solutions, the SGBox total cost of ownership is so suitable, not only for the convenient and predictable pricing model. The modern and intuitive user interface optimizes the learning curve, the innovative product design dramatically reduces the initial and recursive expenses for consulting services.

DISTRIBUTED ARCHITECTURE

SGBox architecture has been designed to serve both mid to large sized enterprises without any management issue. The scalable architecture allows to use remote security collectors to serve complex infrastructures and customers with geographically distributed branch offices.

REMOTE MANAGEMENT SERVICES (RMS)

Since the SIEM are not off-the-shelf products but need to be customized on the different and specific requirements of each single customer, SGBox security engineers, together with the partner technical staff, can help the customer to deploy and evolve the configurations and rules to support the customer growth.

THIRD PARTY INTEGRATION

SGBox now support external applications. Applications implement many functionalities, from custom backups to integration with third party tools. API's allow end user to create custom SGBox applications. External application can also collect SGBox data thru API's.

SGBox is a dynamic and innovative security vendor with over 10 years of experience in cyber security software development. In strong expansion in Europe and Middle Eastern markets, SGBox redefines the approach to cybersecurity and compliance (GDPR, SAMA, ISO27001, PCI-DSS,...) proposing an integrated but modular, scalable and easy-to-use solution, able to adapt to the growing market demand.

CONTACT US

Headquarter
Via Melchiorre Gioia 168, Milano, 20125 - Italy

✉ sales@sgbox.it
www.sgbox.it