VELOX

WHITE PAPER

ScanPlus Security Information and Event Management

2021// VSPL

VELOX®
Develops Opportunities For Enterprises...

INTRODUCTION

In the early days of cybersecurity, technological innovation centered around the development of preventive tools that could stop cyber-attacks as they happened. Tools such as host-based or network-based intrusion detection systems, firewalls, and anti-virus software are built to secure the network against attacks.

Today's cyber-attacks are often so sophisticated that without the proper tools, IT organizations may not even realize that an attack has taken place. This reality is why an increasing number of IT organizations are relying on their log files as a means of monitoring activity on the IT infrastructure and maintaining awareness of possible security threats. IT organizations must understand the features and capabilities of SIEM

ScanPlus SIEM is a real-time event data collection and correlation tool, which helps the organization with updated security and application-level information. It correlates, responds, and alerts the threat analyzed in the source of events. ScanPlus SIEM is effective in security orchestration, automation, and response (SOAR) solution, it is possible to achieve more, in less time, while still allowing for human decision-making when it's most critical.

SIEM

ScanPlus SIEM collects and aggregates log data generated throughout the organization's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters.

ScanPlus then identifies and categorizes incidents and events, as well as analyzes them. The software delivers on two main objectives, which are as follows:

1. To provide reports on security-related incidents and events, such as successful and failed logins, malware activity, and other possibly malicious activities.
2. To send alerts if analysis shows that an activity runs against predetermined rule sets and thus indicates a potential security issue.

FEATURES

·**Events Storing:** ScanPlus SIEM Stores the data for a longer period so that decisions can be made off of more complete data sets. Large networks produce massive volumes of data. ScanPlus SIEM incorporates features that support efficient retention of high data volumes for required lengths of time. A historical report can be exported from the summarized analysis of the particular period.

·**Customizable Dashboards:** Used to analyze (and visualize) data to recognize patterns or target activity or data that does not fit into a normal pattern. ScanPlus SIEM includes dashboarding features that enable real-time monitoring, ScanPlus SIEM Dashboards can often be customized to feature the most important or relevant data, increasing the overall visibility of the network and enabling live monitoring in real-time by a human operator.

·**Accurate Correlation:** Sorts data into packets that are meaningful, similar, and share common traits. The goal is to turn data into useful information. ScanPlus SIEM can use machine learning or rules-based algorithms to draw connections between events in different systems.

·**Escalating via Alerts:** When data is gathered or identified that trigger certain responses - such as alerts or potential security problems - ScanPlus SIEM can activate certain protocols to alert users, like notifications sent to the dashboard, an automated email or text message. ScanPlus SIEM can identify suspicious event log activity, such as repeated failed login attempts, excessive CPU usage, large data transfers, and immediate alert IT security analysts when a possible IoC is detected.

·**Integration Feasibility:** Data can be gathered from any number of sites once ScanPlus SIEM is introduced, including servers, networks, databases, software, and email systems. The aggregator also serves as a consolidating resource before data is sent to be correlated or retained. ScanPlus SIEM aggregates event logs from all operating systems and applications within a given network.

SIEM: AGENT

For securing your IT Infrastructure in a feasible way, ScanPlus SIEM provides agent-based and agent-less solutions. Single setup file of the ScanPlus integrated with both solutions.

Agentless Setup:

Agentless Setup is the default mode of monitoring the network devices for event management. In addition to network devices, ScanPlus can be configured for the Windows Server, Linux Servers, and Linux devices. All nodes which are to be monitored and secured with ScanPlus SIEM, need to be configured for one or more of the following event targets:

- ·Syslog Server
- ·Windows Event Collector
- ·SNMP trap Receiver

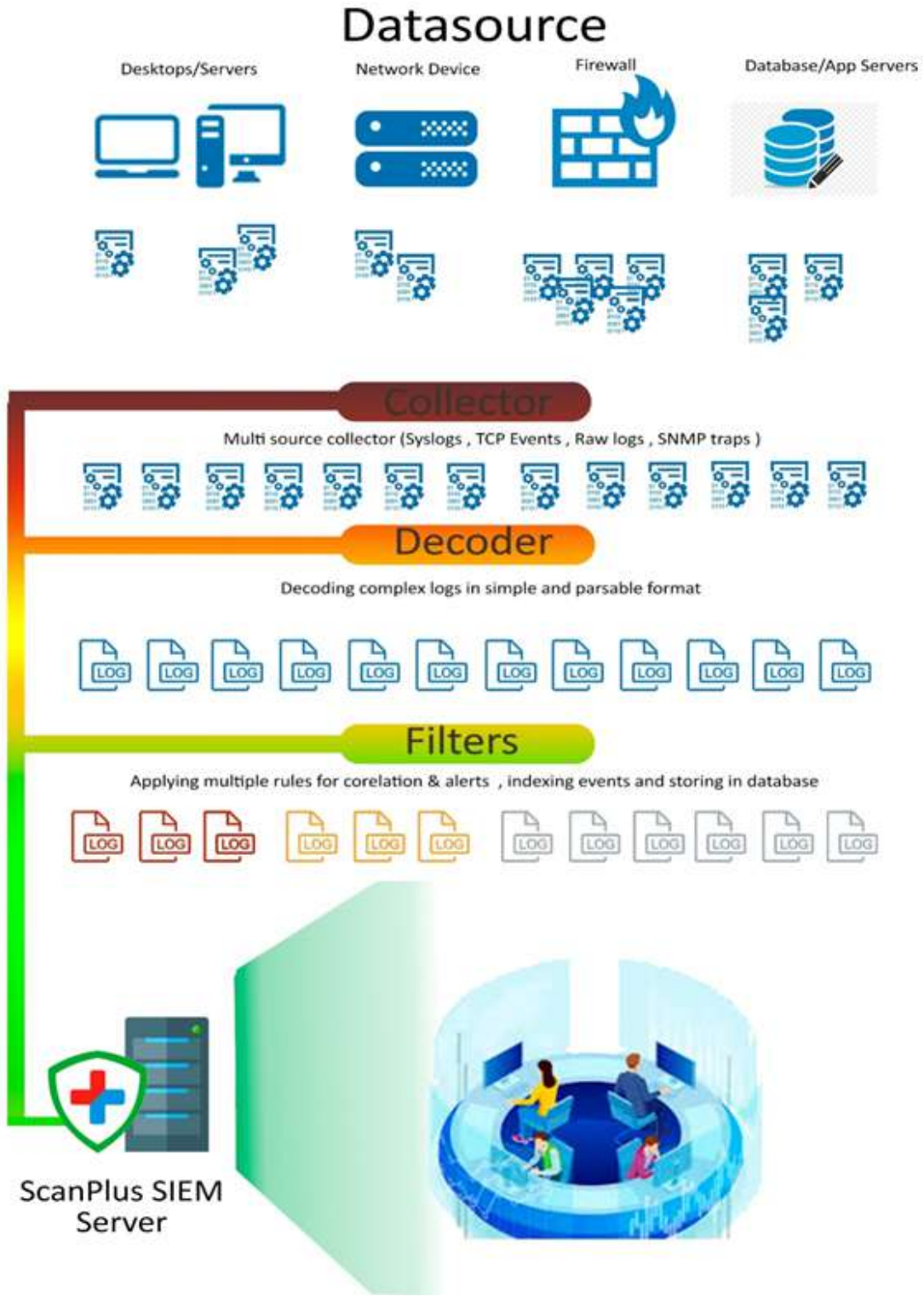
ScanPlus SIEM collector after receiving the individual event starts its instant decoding and co-relation with all updated rules. Filtration of the event for SIEM rules is based on the raw event and its current security score in the ScanPlus console. If it gets filtered with ScanPlus single or multiple rules, the indication is sent on the console. For high-priority events, an alert via email and SMS is sent. Every raw event is stored in a database for report and aggregation.

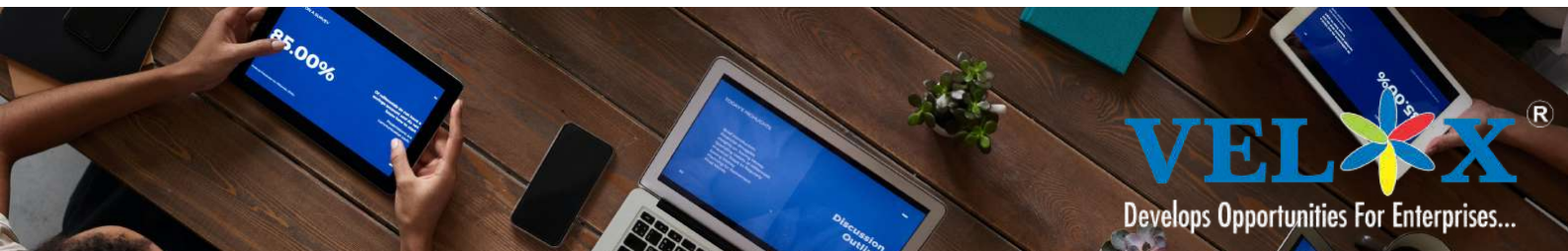
Agent-Based Setup:

ScanPlus setup can be installed in the Windows and Linux operating system for agent-based setup. This setup will monitor the system with additional hooks which collect in-depth events apart from default event source as for Windows Event collector, firewall logs, etc.

After installation of SIEM agent, it starts node Scanner utility to collect the initial node identification to install ScanPlus hook driver to monitor events generated in the system. ScanPlus then send these events to the configured SIEM server in raw format. Depend on the current security score of the event appropriate action is taken in response to the event.

SIEM: FLOW


Datasource
Desktops/Servers
Network Device
Firewall
Database/App Servers
Collector
Multi source collector (Syslogs , TCP Events , Raw logs , SNMP traps)
Decoder
Decoding complex logs in simple and parsable format
Filters
Applying multiple rules for corelation & alerts , indexing events and storing in database
LOG
ScanPlus SIEM Server


VELOX®
Develops Opportunities For Enterprises...

COLLECTORS:

Using multiple collector sources for collecting events, ScanPlus SIEM can be integrated with multiple data sources for multiple collectors. This increases the depth of events and co-relation capabilities of the tool. Following are the collectors used by ScanPlus SIEM

·**Syslog Events:** Network devices can be configured to send Syslog msg to ScanPlus SIEM Server on default of configured ports

·**SNMP traps:** Endpoints with SNMP services can be configured for SNMP traps. Using generic informational and security mibs to collect the information from endpoints.

·**Raw Log files:** Various logs such as firewall logs, crash dump, database logs are periodically read by SIEM agent.

·**Windows Events:** Windows Events can be forwarded or read locally by ScanPlus SIEM agent to collect and send or store the events

·**Filter Drivers:** In agent-based setup, ScanPlus installed filter driver for application and network events and information passed through.

NORMALIZATION:

After the collector collects the events from multiple sources, it sends the events in the ScanPlus filter to convert raw data into the readable and categorized format. Every event is marked with a ScanPlus Security score which helps to co-relate these events with upcoming and existing events. Every event is passed through multiple rules which effectively alerts the Administrators event with low severity is co-related by rules with existing events with their respective ScanPlus Security scores.

·**Decoders:** Irrespective of data source events are decoded in the main category with severity assigned to it. ScanPlus uses 84 different types of decoders to convert the raw data massages in a simple format. Extracting all possible essential information and converting complex logs into a simple yet informative format is done by the various deciders in real-time.

·**Security Score:** Parsed events are indexed for the correlation queue with its events security score. Security scores are assigned by the content of the event, the volume of the event in the event pool, and the current security score of the endpoint Datasource or event source or destination.

DEFAULT RULES:

ScanPlus SIEM security team is constantly testing and analyzing events with their correlation factor with the latest security measure taken around the IT organization. After testing and developing new set of correlation rules or decoder, new patch is released on the central SIEM Application server. Every ScanPlus SIEM Server client connected to these SIEM Application Server over the internet automatically downloads the latest patch and install them silently.

·**Default Rules:** Every parsed raw log by decoders are sent to correlation and security assessment. This process uses current security score of the device/end points, security score of the event and rules to alert the administrator if any threat is detected. Every event by default have been categories in 7 default severity levels. After passing through multiple rules filters, each event is stored for the reporting and further correlation purpose.

·**User Rules:** After event is filtered through default ScanPlus filters, event is passed thorough user-based rules for further action such as Alert, Discarding, Changing properties (Like severity or msg). User based rules are created in console by administrator with simple create rules form or selecting individual event for reference. Administrator can create number of rules as per its industrial practices.

DEFAULT RULES

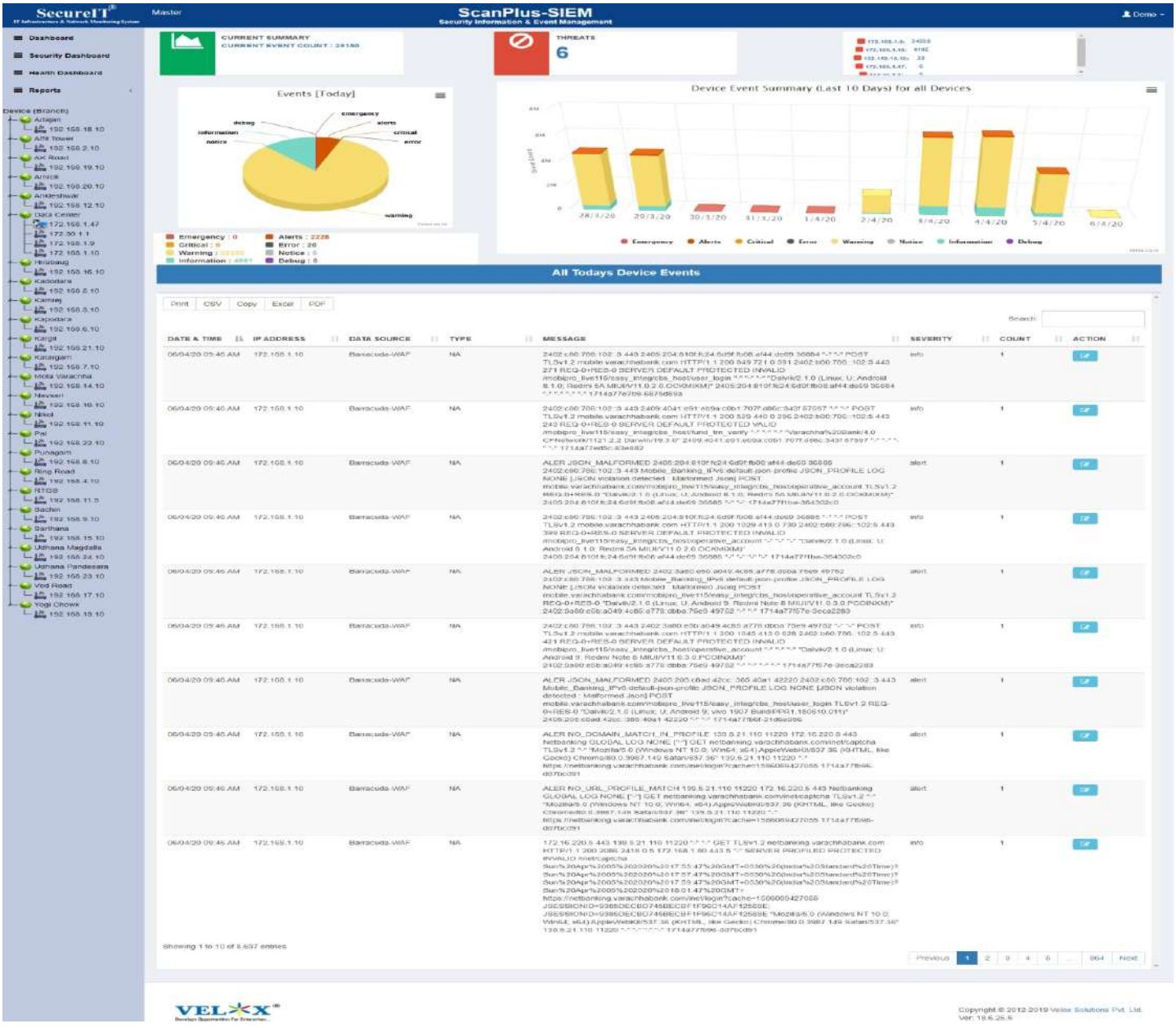
- amazon_rules.xml
- apache_rules.xml
- apparmor_rules.xml
- arpwatch_rules.xml
- asterisk_rules.xml
- attack_rules.xml
- auditd_rules.xml
- azure_rules.xml
- checkpoint-smart1.xml
- cimserver_rules.xml
- ciscat_rules.xml
- cisco-asa_rules.xml
- cisco-estreamer_rules.xml
- cisco-ios_rules.xml
- clam_av_rules.xml
- config.xml
- courier_rules.xml
- cylance_rules.xml
- docker_integration_rules.xml
- docker_rules.xml
- dovecot_rules.xml
- dropbear_rules.xml
- exim_rules.xml
- firewall_rules.xml
- firewalld_rules.xml
- fortigate_rules.xml
- freeipa_rules.xml
- ftpd_rules.xml
- generic_rules.xml
- hordeimp_rules.xml
- hp_rules.xml
- identity_guard_rules.xml
- ids_rules.xml
- imperva_rules.xml
- jenkins_rules.xml
- junos_rules.xml
- kaspersky_rules.xml
- mailscanner_rules.xml
- mariadb_rules.xml
- mcafee_av_rules.xml
- mcafee_epo_rules.xml
- mongodb_rules.xml
- ms_dhcp_rules.xml
- ms_ftpd_rules.xml
- ms_ipsec_rules.xml
- ms_logs_rules.xml
- ms_sqlserver_rules.xml
- ms_wdefender_rules.xml
- msauth_rules.xml
- ms-exchange_rules.xml
- msse_rules.xml
- mysql_audit_rules.xml
- mysql_rules.xml
- named_rules.xml
- netscaler_rules.xml
- netscreenfw_rules.xml
- nextcloud_rules.xml
- nginx_rules.xml
- openbsd_rules.xml
- opensmtpd_rules.xml
- openvas_rules.xml
- openvpn_rules.xml
- oscap_rules.xml
- osquery_rules.xml
- owlh-zeek_rules.xml
- owncloud_rules.xml
- panda-paps_rules.xml
- pfsense_rules.xml
- php_rules.xml
- pix_rules.xml
- policy_rules.xml
- postfix_rules.xml
- postgresql_rules.xml
- proftpd_rules.xml
- proxmox-ve_rules.xml
- puppet_rules.xml
- pureftpd_rules.xml
- qualysguard_rules.xml
- racoon_rules.xml
- redis_rules.xml
- roundcube_rules.xml
- rsaauthmanager_rules.xml
- sca_rules.xml
- sendmail_rules.xml
- servu_rules.xml
- smbd_rules.xml
- solaris_bsm_rules.xml
- sonicwall_rules.xml
- sophos_rules.xml
- spamd_rules.xml
- squid_rules.xml
- sshd_rules.xml
- suricata_rules.xml
- symantecav_rules.xml
- symantecws_rules.xml
- syslog_rules.xml
- sysmon_rules.xml
- systemd_rules.xml
- telnetd_rules.xml
- unbound_rules.xml
- usb_rules.xml
- virustotal_rules.xml
- vmpop3d_rules.xml
- vmware_rules.xml
- vpn_concentrator_rules.xml
- vpopmail_rules.xml
- vsftpd_rules.xml
- vshell_rules.xml
- vulnerability-detector_rules.xml
- vuls_rules.xml
- web_appsec_rules.xml
- web_rules.xml
- win-application_rules.xml
- win-base_rules.xml
- win-mcafee_rules.xml
- win-ms_logs_rules.xml
- win-ms-se_rules.xml
- win-security_rules.xml
- win-sysmon_rules.xml
- win-system_rules.xml
- win-vipre_rules.xml
- win-wdefender_rules.xml
- win-wfirewall_rules.xml
- wordpress_rules.xml
- zeus_rules.xml

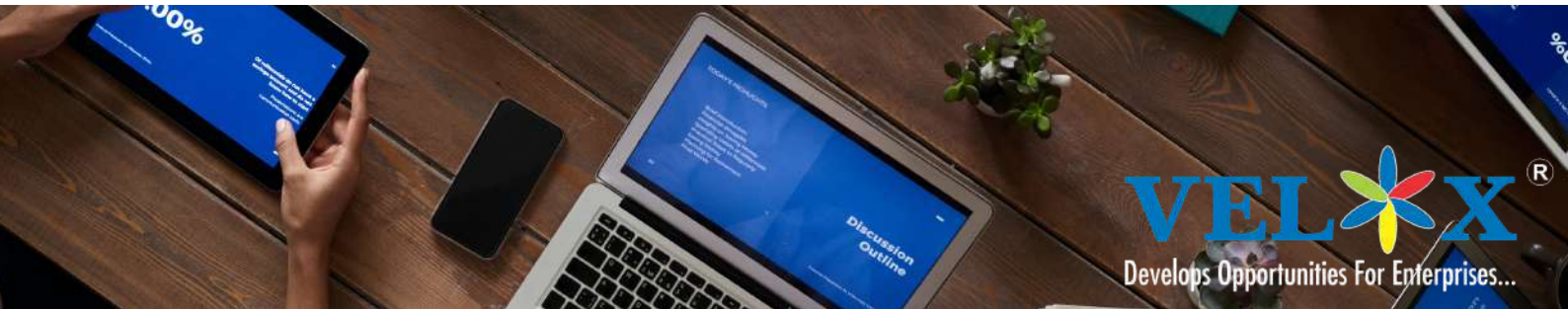
DEFAULT DECODERS

- activeresponse_decoders.xml
- aixipsec_decoders.xml
- apache_decoders.xml
- arpwatch_decoders.xml
- asterisk_decoders.xml
- auditd_decoders.xml
- azure_decoders.xml
- barracuda_decoders.xml
- checkpoint_decoders (2).xml
- checkpoint_decoders.xml
- cimserver_decoders.xml
- ciscoasa_decoders.xml
- ciscoestreamer_decoders.xml
- ciscoios_decoders.xml
- ciscovpn_decoders.xml
- clamav_decoders.xml
- courier_decoders.xml
- cylance_decoders.xml
- docker_decoders.xml
- dovecot_decoders.xml
- dpkg_decoders.xml
- dragonnids_decoders.xml
- dropbear_decoders.xml
- exim_decoders.xml
- fortigate_decoders.xml
- freeipa_decoders.xml
- ftpd_decoders.xml
- grandstream_decoders.xml
- horde_decoders.xml
- hp_decoders.xml
- identity_guard_decoders.xml
- imapd_decoders.xml
- imperva_decoders.xml
- jenkins_decoders.xml
- json_decoders.xml
- junos_decoders.xml
- kaspersky_decoders.xml
- kernel_decoders.xml
- mailscanner_decoders.xml
- mariadb_decoders.xml
- mcafee_decoders.xml
- mongodb_decoders.xml
- mysql_decoders.xml
- named_decoders.xml
- netscaler_decoders.xml
- netscreen_decoders.xml
- nextcloud_decoders.xml
- nginx_decoders.xml
- ntpd_decoders.xml
- openbsd_decoders.xml
- openldap_decoders.xml
- openvas_decoders.xml
- openvpn_decoders.xml
- oscap_decoders.xml
- ossec_decoders.xml
- owncloud_decoders.xml
- pam_decoders.xml
- pandapaps_decoders.xml
- perdition_decoders.xml
- pfsense_decoders.xml
- pix_decoders.xml
- portsentry_decoders.xml
- postfix_decoders.xml
- postgresql_decoders.xml
- proftpd_decoders.xml
- proxmoxve_decoders.xml
- puppet_decoders.xml
- pureftpd_decoders.xml
- qualysguard_decoders.xml
- racoon_decoders.xml
- redis_decoders.xml
- roundcube_decoders.xml
- rsaauthmanager_decoders.xml
- rshd_decoders.xml
- samba_decoders.xml
- sendmail_decoders.xml
- servu_decoders.xml
- snort_decoders.xml
- solaris_decoders.xml
- sonicwall_decoders.xml
- sophos_decoders.xml
- sqlserver_decoders.xml
- squid_decoders.xml
- ssh_decoders.xml
- su_decoders.xml
- sudo_decoders.xml
- suhosin_decoders.xml
- symantec_decoders.xml
- telnet_decoders.xml
- trendosce_decoders.xml
- unbound_decoders.xml
- unix_decoders.xml
- vmpop3_decoders.xml
- vmware_decoders.xml
- vpopmail_decoders.xml
- vsftpd_decoders.xml
- vshell_decoders.xml
- wazuh_decoders.xml
- webaccesslog_decoders.xml
- windows_decoders.xml
- wordpress_decoders.xml
- zeus_decoders.xml

MAIN DASHBOARD:

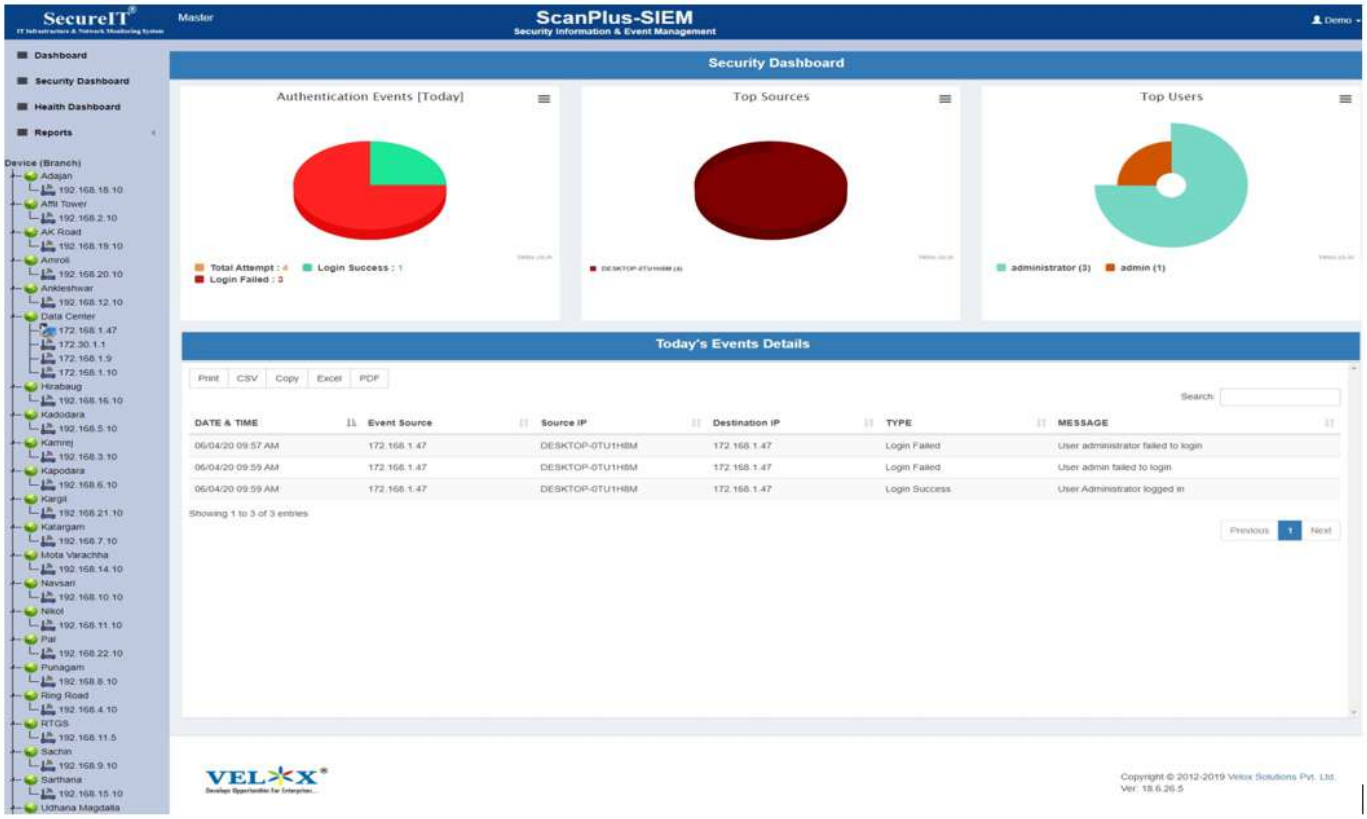
ScanPlus SIEM dashboard is a summary of the all events that occurred in the SIEM monitoring environment on the current day. On a single dashboard, the user is shown a summary, threats, and aggregated events.





SECURITY DASHBOARD:

All events which are marked as security category are shown in this dashboard. Security events include Authentication related events (failed attempt login, successful after failed login attempt), Application Access related events. These events are shown on real-time basis. User-based rules which are marked for such category are also shown in this dashboard.



NOTABLE RESULT AREAS:

Collection and analysis of events, incidents

Conducting a thorough incident analysis helps you uncover the reasons it happened, remove the root causes and take precautions against repeat incidents. Our solutions incorporate the following steps to guide you through the process.

- ·Conduct a Root Cause Analysis
- ·Identify Patterns
- ·Correct and Prevent Issues

Threat detection

Our solution analyses the entirety of a security ecosystem to identify any malicious activity that could compromise the network. If a threat is detected, then mitigation efforts must be enacted to properly neutralize the threat before it can exploit any present vulnerabilities.

Threat Hunting

ScanPlus SIEM proactively searches for cyber threats that are lurking undetected in a network. Cyber threat hunting digs deep to find malicious actors in your environment that have slipped past your initial endpoint security defenses.

Forensics, Root cause analysis

Forensic analysis or Root cause analysis refers to a detailed investigation for detecting and documenting the course, reasons, and consequences of a security incident or violation of rules of the organization, such tasks are performed by ScanPlus SIEM, to keep your environment secure.

Orchestration of remediation

ScanPlus SIEM's orchestration chains tasks together to create larger processes and workflows that span toolsets, which allows organizations to move beyond automation. It opens new possibilities to work at scale, saving security teams valuable resources and speeding up responses to more routine issues.

Threat Intelligence and security analytics

Cyber Security Analytics evolved from Security Incident and Event Management (SIEM) to meet the need for greater security across the business; more context and more insights. There are three key components: Security Incident and Event Management (SIEM), Behaviour Anomaly Detection (BAD or UEBA), and Threat Intelligence. Identified as a 'strong performer' our solution is recognized for its capabilities in large environments.

USE CASE 1:

GS MAHANAGAR BANK

Background:

This Bank was established by the people from the Ahmednagar Dist. in the name of "The Ahmednagar Sahakari Bank Ltd." on 6th October 1973. Late. Solicitor Shri. G.S. Shelke and his colleagues were the motivating force behind the establishment of this bank. Late. Solicitor Shri G.S. Shelke became the first Chairman, Lt. Shri. G.A. Thube, the first Vice-Chairman, Shri. S. S. Bhagat, the first Secretary.

The Bank has a humble but very inspiring beginning. The minimum amount of Rs.10/- per share was required from prospective members and as such practically, from all over Mumbai, they collected the initial share capital of Rs.1.36 Lakhs. With this small amount, they started this co-operative activity in Greater Mumbai. The Bank was initially set up to help Mill workers from the Kalachowki and Lalbaug area and Dockworkers from Carnac Bunder, Fruit, Vegetable and Flower vendors from Crawford market, Byculla and Dadar market, Fish vendors from Colaba, and a small number of shop keepers and self-employed persons.

In the later stages, the Bank has changed its object and decided to cater to the needs of common people from all sectors of the society. To obtain this, the bank has decided to change the name from "The Ahmednagar Sahakari Bank Ltd." to "The Mahanagar Co-operative Bank Ltd." The new name came into force with effect from 21st January 1998.

Thanks to the sustained and assiduous efforts over 43 years after its inception, the bank had gained a strong foundation in terms of its membership, resources, assets, and profits. During this period the bank grew from strength to strength. The Bank has grown in stature, progressed in its social and economic objectives, and produced an image of what an ideal bank should be. It is secured 'A' grade classification for all the years from the beginning. Resultantly the Reserve Bank of India awarded scheduled status to the Bank on 30th January 1998. This also boosted the confidence of our members, account holders, and depositors of the Bank.

GS MAHANAGAR BANK

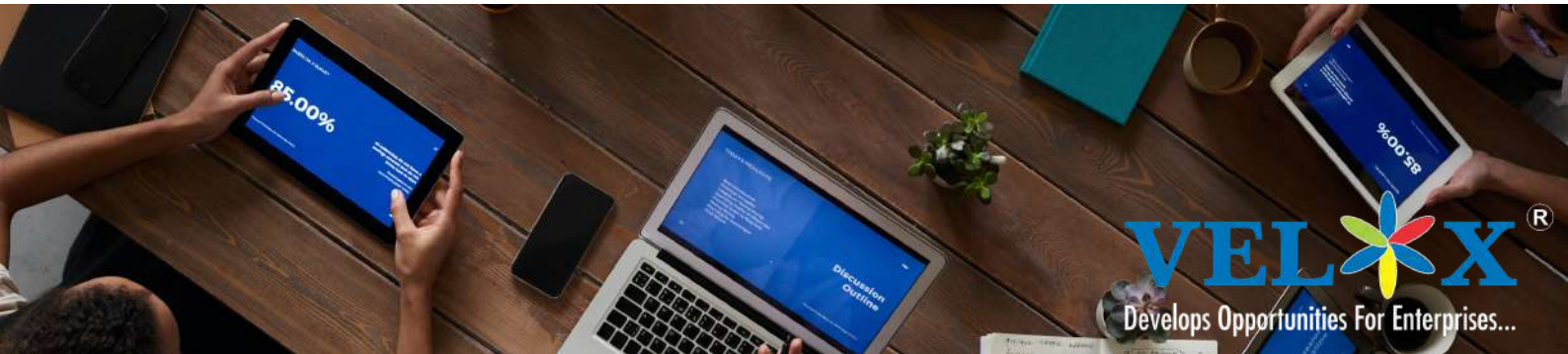
Men with excellent academic qualifications on the Board of Directors of the Bank have given the Bank the benefit of wisdom, expertise, and experience with its rich heritage and the solid support that the Bank receives on all fronts from all its constituents. The Bank is confident to make future wisely and consistently. The Bank has been paying dividends to its shareholders at the rate of 15% which is the maximum permissible dividend as per the MCS Act. Bank has a total of 61 Branches and nonstop 12 hours service in 5 Branches. The area of operation covers all over Maharashtra. The Bank is perhaps the fastest-growing Bank in the Cooperative sector.

Besides this, the Board of Directors has visualized the future increasing competition in this industry and also the expectations of the Reserve Bank of India. For this purpose, the Board of Directors is considering the introduction of Modern Banking Services such as ATM Centers, Debit Card, Home Banking, RTGS, NEFT, Demat, IMPS, Net Banking, etc. With this, we are fully geared to face the cutthroat competition in the Banking Industry in the near future.

Innovative Banking is another area of operation that Mahanagar Bank is currently focusing on for sustainable long-term growth. The Bank has always endeavored for providing satisfactory customer service with the help of the latest technology. With a view to meet the challenges of a technologically advanced banking system and to upgrade its existing technology, the bank has introduced "Total Bank Automation" to provide the facility of inter-branch connectivity for any time and any branch banking transactions.

Branches: 68
Turnover: 4500 Cr
CBS: Omni Soft (Infrasoft Technologies)

Solutions Provided:
1.SIEM
2.Cyber Security Framework
3.IT Helpdesk
4.Network Monitoring Solutions
5.IT Asset Management
6.ScanPlus Terminal Security Solutions



GS MAHANAGAR BANK

Key observations during the implementation.

1.Implementing Cyber Security and SIEM at different geographies of Maharashtra during Covid Time was challenging.

2.Integration of SIEM for monitoring Core banking server was done. The current setup is in the captive model.

- Collection of Windows event logs
  - § Remote access for abnormal behavior like Unknown Source, beyond official time.
  - § Unauthorized configuration changes
  - § Services and application execution monitoring
  - § Critical directory access.
- Collection of Antivirus logs.
  - § Malware detection
  - § Unexpected traffic detection
- Status of availability of Server hosting CBS.
- Health Logs related to CPU, RAM, and HDD of the concerned server.
- Server Activity information of the said server for both application and DB.
- Alerts to specified Emails and text alerts to specified mobile numbers.

3.SIEM hosting through SOC had few challenges as the enabled logs were not reaching SIEM initially due to the log-related issues. This was rectified subsequently with the joint effort of the Bank's IT team and support team of Velox Solutions.

Key benefits to customers.

1.All RBI-guided frameworks are implemented, and compliance reports are shared from time to time.

2.The bank has saved a massive investment cum expense for setting up the SOC and hiring resources of its own for this kind of requirement.

3.Through the hosted CBS application is monitored by the host, to a certain level of monitoring the CBS server is also done by SOC which is complementing the same. Also, the Bank has visibility to it.

4.Seamless monitoring from a SOC with dedicated resources for the purpose of cyberspace security monitoring for the Bank.

USE CASE 2:

GAYATRI BANK

Background:

The Gayatri Co-Operative Urban Bank Ltd., Jagtial, Dist: Jagtial (TS) established in the year 2000, as a Unit Bank at Jagtial in undivided Andhra Pradesh at that time, presently in Telangana State. The Bank has started functioning from 11-09-2000 with RBI License No.UBD/HYD/AP/26P/24-05-2000.

- Initially Bank was started with Rs. 25,11,000/- share capital from 1008 members as a Unit Bank.
- The main objective of the Bank is to cater to the Banking needs of the poor, middle, rural, Semi-Urban, and Urban people and also take care of the banking needs of the business establishments through Quick, Prompt &Transparent services.
- The situation, when the Bank was started, the general Co-operative Banking scenario was witnessing the failure of many Cooperative banks and loss of faith in the system by the public, who were not willing to patronage Co-operative Banks because of their past performance. Though the Bank witnessed such a situation in their initial period of establishment, with our sustained efforts and backed by good customer service, could still create a name for themselves in their Area of Operation.
- For the first 8 years, Bank had worked as only a unit Bank. However with the liberalization of Branch Licensing policy of the RBI in the 2008 Year, for Branch expansion in the Co-Operative sector, which encouraged branch expansion for the performing Co-Operative Banks, the Bank could get 2 Licenses for Opening of new branches during the Financial Year 2008-09, thereby increasing our strength to 3 Branches and so on.
- An established last Co-Operative Urban Bank in undivided Andhra Pradesh State, within the span of 18 Years. The Bank could reach to 2nd position based on Business, among 52 Cooperative Urban Banks in Telangana, with their rich integrity, adherence to prudent banking practices, technology advancement, customized products, and services.

Branches: 23

Turnover: 1400 Cr

CBS: BSG curing

Solutions Provided:

1.SIEM

2.Cyber Security Framework

3.IT Helpdesk

GAYATRI BANK

4.Network Monitoring Solutions
5.IT Asset Management
6.ScanPlus Terminal Security Solutions

Key observations during the implementation.

1.Implementing Cyber Security and SIEM at different geographies of Telangana during Covid Time was challenging.

2.Integration of SIEM for monitoring the Core banking server was challenging as the same is in the hosted module. Since the access to CBS is limited.

- Collection of Windows event logs
  - § Remote access for abnormal behavior like Unknown Source, beyond the official time
  - § Unauthorized configuration changes
  - § Services and application execution monitoring
  - § Critical directory access.
- Collection of Antivirus logs.
  - § Malware detection
  - § Unexpected traffic detection
- Status of availability of VM Server hosting CBS.
- Health Logs related to CPU, RAM, and HDD of the respective VM.
- Server Activity information of the said VM for both application and DB.
- Alerts to specified Emails and text alerts to specified mobile numbers.

3.SIEM hosting through SOC had few challenges as the enabled logs were not reaching SIEM initially due to the log-related issues. This was rectified subsequently with the joint effort of the Bank's IT team and support team of Velox Solutions.

Key benefits to customers.

1.All RBI-guided frameworks are implemented, and reports are shared from time to time.

2.The bank has saved a massive investment cum expense for setting up the SOC and hiring resources of its own for this kind of requirement.

3.Through the hosted CBS application is monitored by the host, to a certain level of monitoring the CBS server is also done by SOC which is complementing the same and also the Bank has visibility to it.

4.Seamless monitoring from a SOC with dedicated resources for the purpose of cyberspace security monitoring for the Bank.

Mumbai, India | Chicago, USA

email: sales@velox.co.in

VELOX®

Develops Opportunities For Enterprises...

INDIA | USA | DUBAI | NEPAL | ZIMBABWE | MEXICO | SRI LANKA

visit us at www.velox.co.in

***