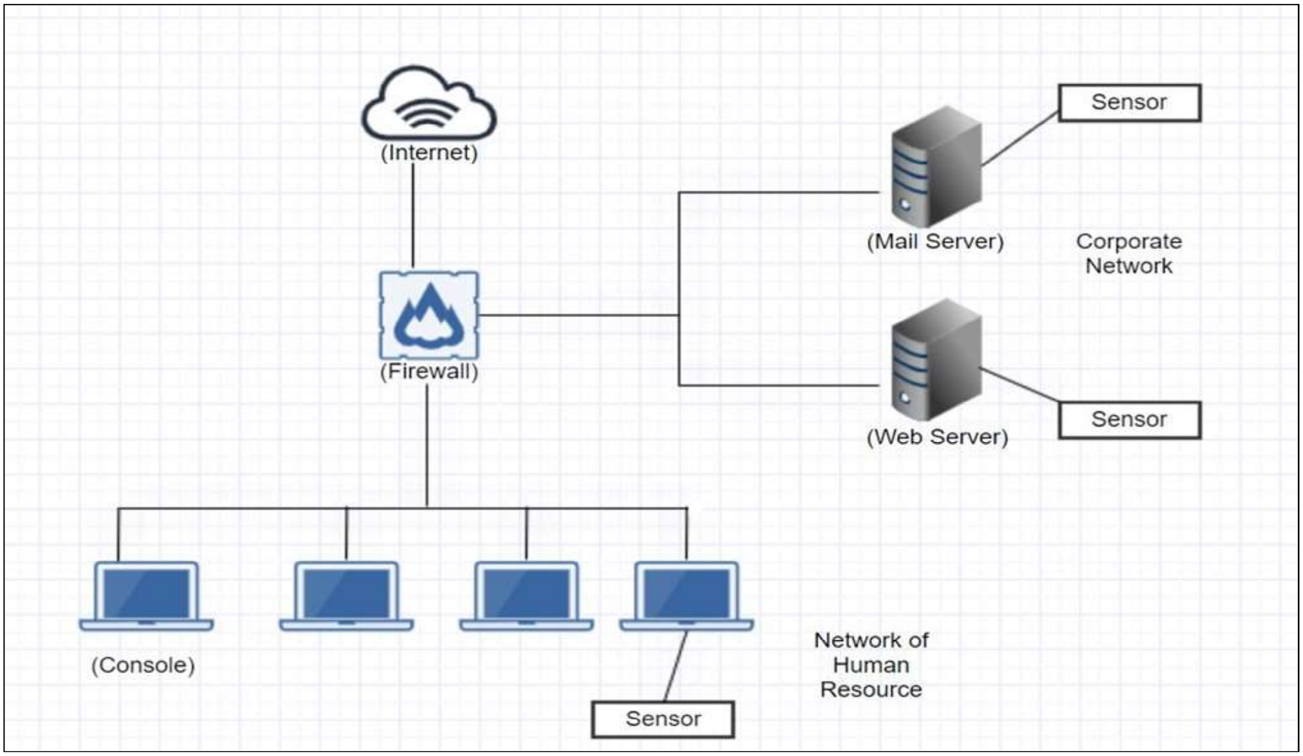
TECHNICAL DATASHEET

SecureIT- HOST INTRUSION PREVENTION SYSTEM

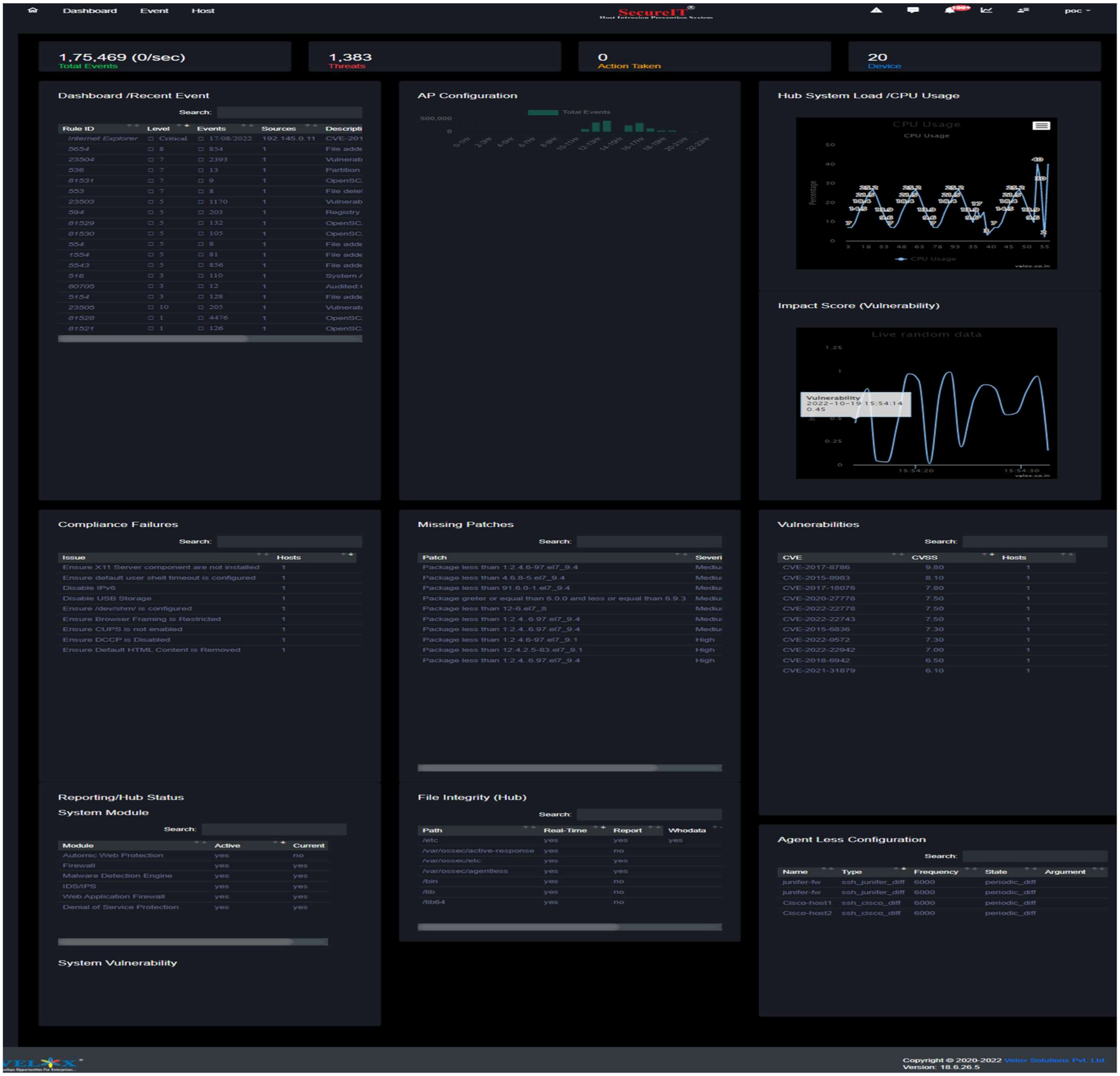
Why SecureIT- Host Intrusion Prevention System?

The SecureIT Host Intrusion Prevention System is an installed software package that monitors a single host for suspicious activity by analyzing events occurring within that host. It aims to stop malware by monitoring the behavior of code. This makes it possible to help keep your system secure without depending on a specific threat to be added to a detection update.

How SecureIT- Host Intrusion Prevention System works?



Host Intrusion Prevention System Dashboard:



1,75,469 (0/sec)
Total Events

1,383
Threats

0
Action Taken

20
Device

Dashboard /Recent Event

Search:

Rule ID	Level	Events	Sources	Descripti
Internet Explorer	□ Critical	□ 17/08/2022	192.145.0.11	CVE-201
5654	□ 8	□ 854	1	File adde
23504	□ 7	□ 2393	1	Vulnerab
536	□ 7	□ 13	1	Partition
81531	□ 7	□ 9	1	OpenSC.
553	□ 7	□ 8	1	File delet
23503	□ 5	□ 1170	1	Vulnerab
594	□ 5	□ 203	1	Registry
81529	□ 5	□ 132	1	OpenSC.
81530	□ 5	□ 105	1	OpenSC.
554	□ 5	□ 8	1	File adde
1554	□ 5	□ 81	1	File adde
5543	□ 5	□ 856	1	File adde
516	□ 3	□ 110	1	System /
80705	□ 3	□ 12	1	Audited:(
5154	□ 3	□ 128	1	File adde
23505	□ 10	□ 205	1	Vulnerab
81528	□ 1	□ 4476	1	OpenSC.
81521	□ 1	□ 126	1	OpenSC.

AP Configuration

Hub System Load /CPU Usage

Impact Score (Vulnerability)

Compliance Failures

Search:

Issue	Hosts
Ensure X11 Server component are not installed	1
Ensure default user shell timeout is configured	1
Disable IPv6	1
Disable USB Storage	1
Ensure /dev/shm/ is configured	1
Ensure Browser Framing is Restricted	1
Ensure CUPS is not enabled	1
Ensure DCCP is Disabled	1
Ensure Default HTML Content is Removed	1

Missing Patches

Search:

Patch	Severi
Package less than 1:2.4.6-97.el7_9.4	Mediu
Package less than 4.6.8-5.el7_9.4	Mediu
Package less than 91.6.0-1.el7_9.4	Mediu
Package greter or equal than 6.0.0 and less or equal than 6.9.3	Mediu
Package less than 12-6.el7_8	Mediu
Package less than 1:2.4..6.97.el7_9.4	Mediu
Package less than 1:2.4..6.97.el7_9.4	Mediu
Package less than 1:2.4.6-97.el7_9.1	High
Package less than 12:4.2.5-83.el7_9.1	High
Package less than 1:2.4..6.97.el7_9.4	High

Vulnerabilities

Search:

CVE	CVSS	Hosts
CVE-2017-8786	9.80	1
CVE-2015-8983	8.10	1
CVE-2017-18076	7.80	1
CVE-2020-27778	7.50	1
CVE-2022-22778	7.50	1
CVE-2022-22743	7.50	1
CVE-2015-6836	7.30	1
CVE-2022-0572	7.30	1
CVE-2022-22942	7.00	1
CVE-2018-6942	6.50	1
CVE-2021-31879	6.10	1

Reporting/Hub Status

System Module

Search:

Module	Active	Current
Automic Web Protection	yes	no
Firewall	yes	yes
Malware Detection Engine	yes	yes
IDS/IPS	yes	yes
Web Application Firewall	yes	yes
Denial of Service Protection	yes	yes

System Vulnerability

File Integrity (Hub)

Search:

Path	Real-Time	Report	Whodata
/etc	yes	yes	yes
/var/ossec/active-response	yes	no	
/var/ossec/etc	yes	yes	
/var/ossec/agentless	yes	yes	
/bin	yes	no	
/lib	yes	no	
/lib64	yes	no	

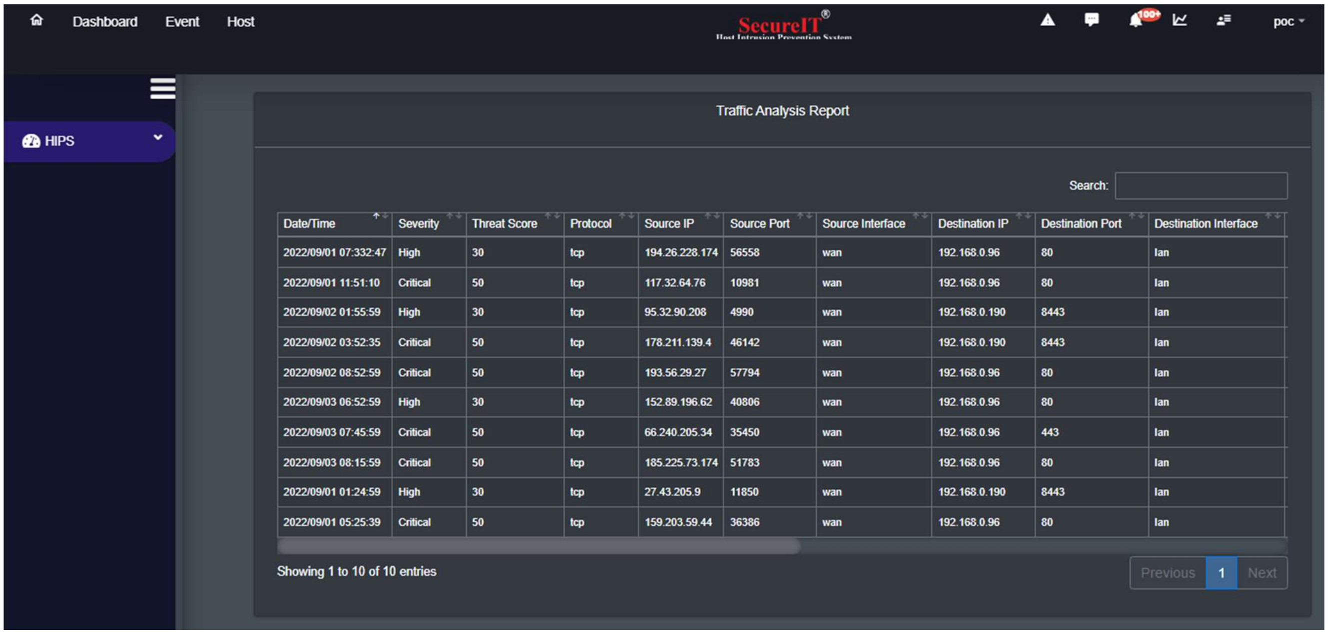
Agent Less Configuration

Search:

Name	Type	Frequency	State	Argument
junifer-fw	ssh_junifer_diff	6000	periodic_diff	
junifer-fw	ssh_junifer_diff	6000	periodic_diff	
Cisco-host1	ssh_cisco_diff	6000	periodic_diff	
Cisco-host2	ssh_cisco_diff	6000	periodic_diff	

Copyright © 2020-2022 Velox Solutions Pvt. Ltd.
Version: 18.6.26.5

DEEP PACKET INSPECTION:



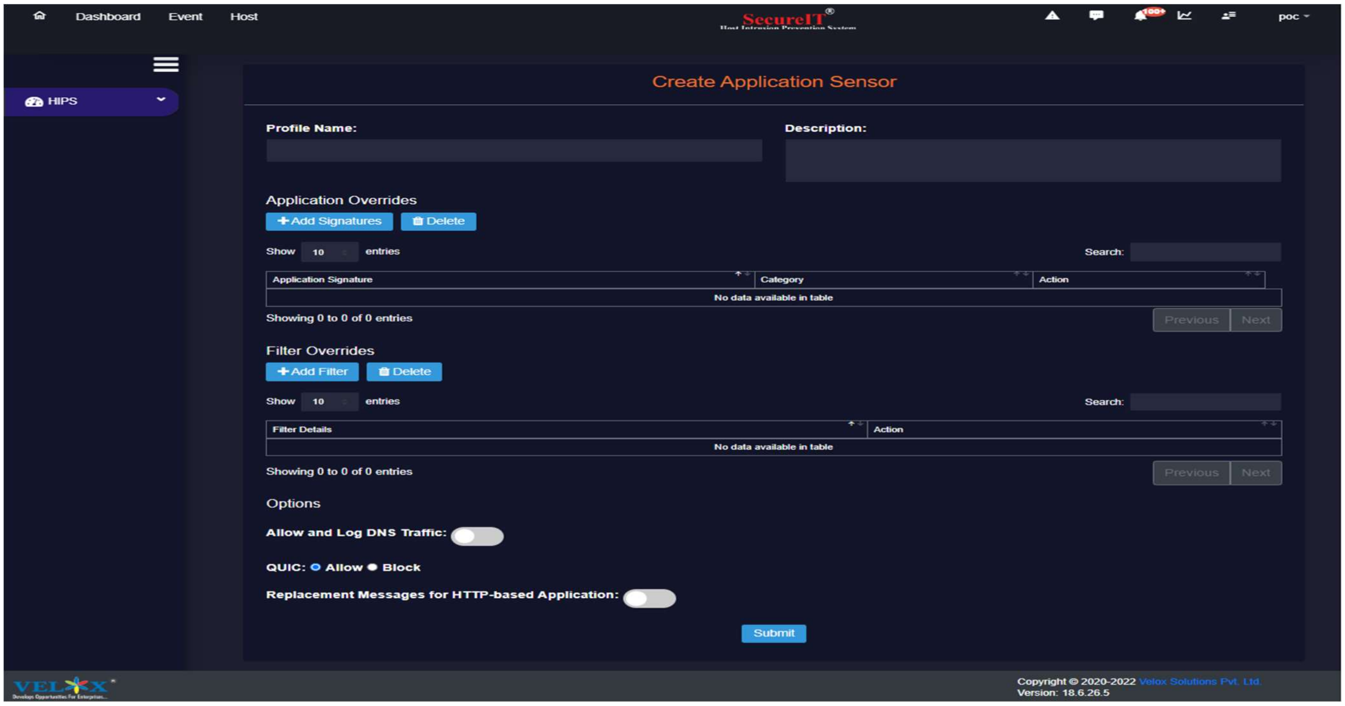
Traffic Analysis Report

Search:

Date/Time	Severity	Threat Score	Protocol	Source IP	Source Port	Source Interface	Destination IP	Destination Port	Destination Interface
2022/09/01 07:332:47	High	30	tcp	194.26.228.174	56558	wan	192.168.0.96	80	lan
2022/09/01 11:51:10	Critical	50	tcp	117.32.64.76	10981	wan	192.168.0.96	80	lan
2022/09/02 01:55:59	High	30	tcp	95.32.90.208	4990	wan	192.168.0.190	8443	lan
2022/09/02 03:52:35	Critical	50	tcp	178.211.139.4	46142	wan	192.168.0.190	8443	lan
2022/09/02 08:52:59	Critical	50	tcp	193.56.29.27	57794	wan	192.168.0.96	80	lan
2022/09/03 06:52:59	High	30	tcp	152.89.196.62	40806	wan	192.168.0.96	80	lan
2022/09/03 07:45:59	Critical	50	tcp	66.240.205.34	35450	wan	192.168.0.96	443	lan
2022/09/03 08:15:59	Critical	50	tcp	185.225.73.174	51783	wan	192.168.0.96	80	lan
2022/09/01 01:24:59	High	30	tcp	27.43.205.9	11850	wan	192.168.0.190	8443	lan
2022/09/01 05:25:39	Critical	50	tcp	159.203.59.44	36386	wan	192.168.0.96	80	lan

Showing 1 to 10 of 10 entries

APPLICATION CONTROL



Create Application Sensor

Profile Name:

Description:

Application Overrides

Show 10 entries

Search:

Application Signature	Category	Action
No data available in table		

Showing 0 to 0 of 0 entries

Filter Overrides

Show 10 entries

Search:

Filter Details	Action
No data available in table	

Showing 0 to 0 of 0 entries

Options

Allow and Log DNS Traffic:

QUIC: ○ Allow ● Block

Replacement Messages for HTTP-based Application:

Copyright © 2020-2022 Velox Solutions Pvt. Ltd.
Version: 18.6.26.5

Key Features:

- Provides automatic recommendations of removing assigned policies and against existing vulnerabilities, dynamically tuning IDS/IPS sensors.
- Monitors a single host for suspicious activity by analyzing events occurring within that host.
- Protects the host from the network layer all the way up to the application layer against known and unknown malicious attacks.
- Agentless solution has the feature of scheduling scans.
- Provision from the policy server and rules are automatically provisioned and de-provisioned.
- Automatic recommendations against existing vulnerabilities.
- Allows integrity monitoring rules to be configured for groups of systems, or individual systems.
- Capable of blocking and detecting IPv6 attacks.
- Blocks the unknown action on operating system or application changes by a hacker or malware and alerts the user so an appropriate decision on next steps can be made.
- Taking a backup of infected files and restoring the same.
- Supports CVE cross referencing for Vulnerabilities.
- Provides protection against DDoS attacks and has the ability to lock down a computer except with management server.
- Supports virtual patching of both known and unknown vulnerabilities.
- Supports inspection firewall, anti-malware, deep packet inspection with HIPS, integrity monitoring, application control, and recommended scanning in a single module with agentless and agent.
- Machine learning and analysis of unknown files with ransomware protection in behaviour monitoring.
- Possesses container security automation processes for critical security controls.
- Provision from the policy server and rules are automatically provisioned and de provisioned.
- Submits unknown files and suspicious object samples with on premise sandbox solution.
- Supports pre-defined lists of critical system files for various operating system applications (web servers, DNS, etc.) and also supports custom rules as well.

Benefits:

- Reputation-managed protection.
- Multiple threat protection.
- Monitor and evaluate threats, catch intruders and take action in real time to thwart such instances that firewall or antivirus software may miss.
- Selective logging.
- Privacy protection
- Prevents DoS/DDoS attacks.
- Location based security configuration
- IT Stops attacks on the SSL protocol or prevent attempts to find open ports on specific hosts.
- Detect and foil OS fingerprinting attempts that hackers use to find out the OS of the target system to launch specific exploits.
- Dynamic threat response
- Supporting platform: Windows/Linux/Mac