

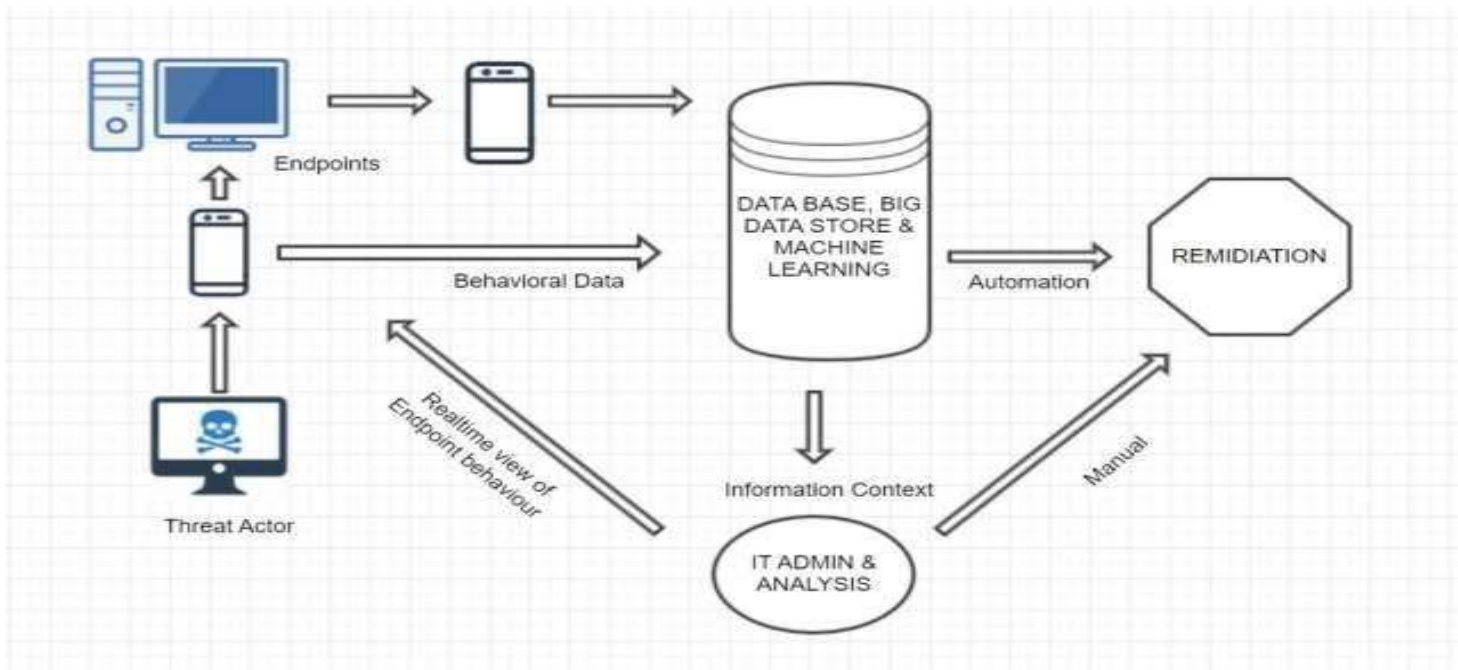
TECHNICAL DATASHEET

SecureIT- Anti Virus End Point Detection and Response

Why SecureIT- EDR ?

- The system prevents tentative damage to data/set up, by preventing persistent attacks, by enabling data security.
- Incident Response Capabilities help the users, to be proactive in managing the security of the endpoints meticulously. Also, ensures preventive actions for any such future vulnerabilities.
- By protecting the environment from multiple threats, it works proactively and ensures comprehensive protection.
- The system avoids unnecessary clogging of logs, which further leads to optimal usage of storage.
- DLP feature helps the system administrator, to monitor the activities in the End Points, from the central console
- It's worked as an independent module without relying on other endpoint and networksystems for its functionality.
- Easy deployment and support and not limited to deployment through third party systemsmanagement tools.
- Provides global and local real-time threat intelligence based on good file reputation data correlated across a global network.

How SecureIT EDR works?



TECHNICAL DATASHEET

SecureIT EDR- Dashboards

A) Alert Dashboard



B) CVE Dashboard

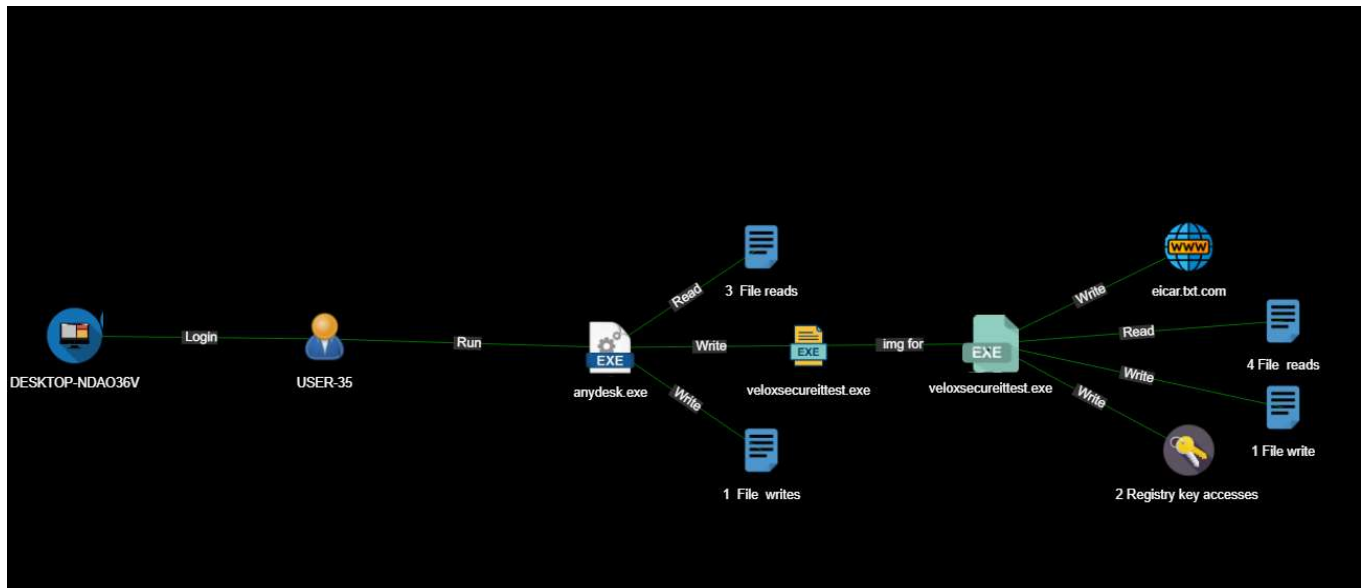


TECHNICAL DATASHEET

Functions:

- SecureIT-Endpoint Detection and Response solution works by monitoring endpoints, and network events, and recording the information in a central database
- Further steps involving the analysis, detection, investigation, reporting, and alerting also takes place.
- A client software agent, installed on the host system provides the foundation for event monitoring and reporting
- It facilitates continuous monitoring and detection through the use of analytical tools. These tools identify tasks that can improve a company's overall state of security by identifying, responding to, and deflecting both internal and external threats

Topology



TECHNICAL DATASHEET

Key Features:

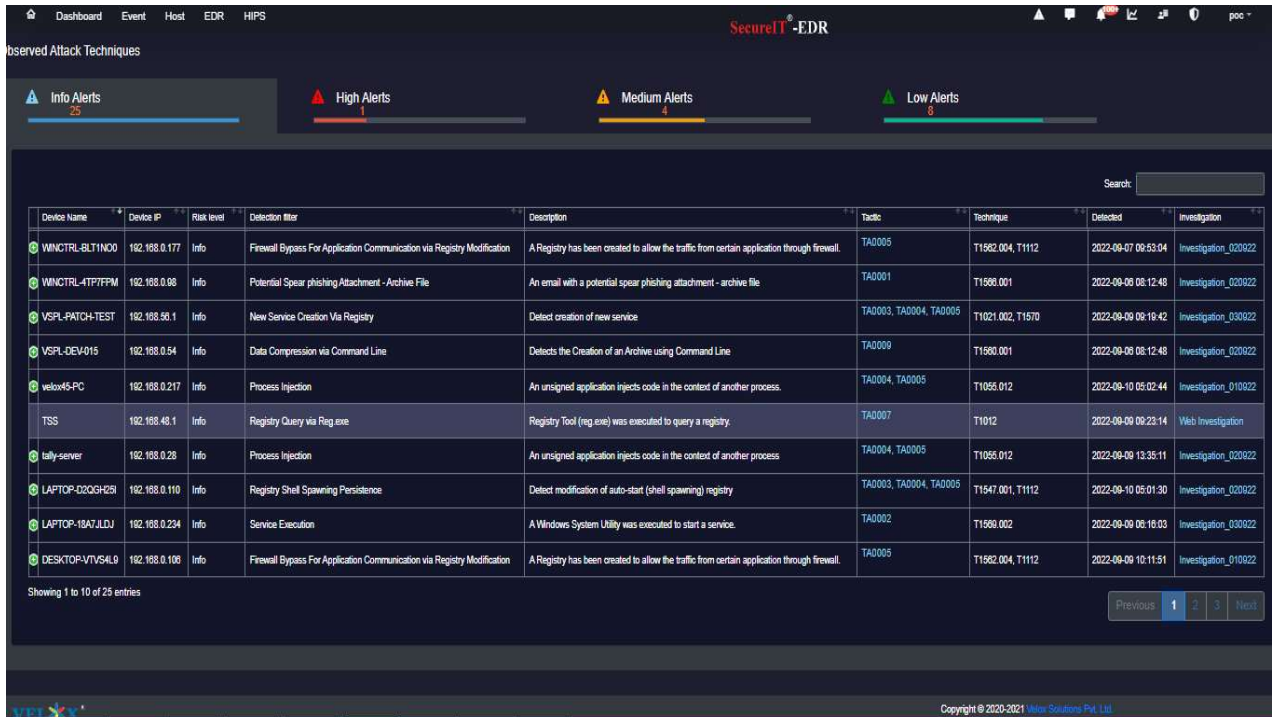
- **Filtering:** It is capable of filtering out false positives.
- Single Integrated Agent.
- **Advanced Threat Blocking:** It identifies the persistent attacks and blocksthem, to ensure that the impact of the threat is minimized/ negated.
- **Incident Response Capabilities:** It has the capability of Threat Hunting and Incident Response, which can help prevent full-blown data breaches.
- **Multiple Threat Protection:** Prepared to handle multiple types of threats at the same time such as ransomware, malware, trojan, and many more.
- **DLP:** Inbuilt Data Loss/Leak Prevention (DLP) feature
- Signature-based and signature-less defense mechanisms to stop threats via a single agent on the endpoint.
- Prevents potential damage from unknown applications.
- Provides patches updates status associated with whitelisted applications.
- Provides Real-time behavior against a cloud model to detect previously unknown threats.
- Detects mutations of malicious samples by recognizing known fragments of malware code.
- Root cause analysis.
- Blocks known and unknown vulnerabilities exploited before patches are deployed.
- Signature-less techniques.
- Machine Learning.
- Blocks known and unknown vulnerability exploits before patches are deployed.
- Capabilities of IOC Sweeping, Patient Zero ID/Root Cause Analysis, and IOA Behavior Hunting/ Detection.
- Packer Detection to identify packed malware.
- Protects operating system and common applications from known and unknown attacks.
- Submit unknown files on sandbox
- Supports detection of all malware types (known and unknown).
- Supports continuous and root cause analysis to help in triggering security incidents.
- Capability of AV, Vulnerability Protection, Firewall, Device Control, Application Control, Virtual Patching, EDR, DLP, and MDR in a single agent.
- Proven capability of pre and runtime machine learning
- File and Web reputation - Variant protection - Census check.
- Supports IPv4 and IPv6.
- Controls the data in motion of sensitive information—whether it is in email, webmail, etc., and networking protocols such as FTP, HTTP/HTTPS, and SMTP.
- Uses application name, path, regular expression, or certificate for basic application whitelisting and backlisting.
- Provides protection to critical platforms, including legacy operating systems such as MS XP.
- Integrates with other security products locally on the network and delivers network sandbox rapid response.
- Dynamically adjusts security configuration based on the location of an endpoint
- Allows threat analysts to rapidly assess the nature and extent of custom detection, intelligence, and controls.
- Automatically assesses the required virtual patches for specific environments.
- Possesses Isolation, Quarantine, Process Kill, Execution block and Damage Rollback.
- Rule based capabilities on vulnerabilities

TECHNICAL DATASHEET

Default templates:-

- GLBA: Gramm-Leach-Bliley Act.
- HIPAA: Health Insurance Portability and Accountability Act.
- PCI-DSS: Payment Card Industry Data Security Standard
- SB-1386: US Senate Bill 1386
- US PII: United States Personally Identifiable Information
- Indicators of Compromise: Database Dumps/ Backup Files for Discovery, .REG Files for Discovery, Suspected Malicious Dissemination for Discovery.
- Employee Discontent: CV and Resume, Salary Slip.
- Individual Identification: Aadhar Card, Pan Card, Voter ID, Driving License, Voter ID, Driving, License, Passport.
- Company Confidential and intellectual property: Financial Information, Database Files.
- Digitally Signed PDF Files, Password Protected Files, IMEI for Discovery, Network Security Information for Discovery, License Keys for Discovery.
- Software Source code for Discovery

Observed Techniques



Device Name	Device IP	Risk level	Detection filter	Description	Tactic	Technique	Detected	Investigation
WINCTRL-BL1ND00	192.168.0.177	Info	Firewall Bypass For Application Communication via Registry Modification	A Registry has been created to allow the traffic from certain application through firewall.	TA0005	T1592.004, T1112	2022-09-07 09:53:04	Investigation_020022
WINCTRL-4TF7FPM	192.168.0.09	Info	Potential Spear phishing Attachment - Archive File	An email with a potential spear phishing attachment - archive file	TA0001	T1596.001	2022-09-08 08:12:48	Investigation_020022
VSPR-PATCH-TEST	192.168.50.1	Info	New Service Creation Via Registry	Detect creation of new service	TA0003, TA0004, TA0005	T1021.002, T1570	2022-09-09 09:16:42	Investigation_030022
VSPR-DEV-015	192.168.0.54	Info	Data Compression via Command Line	Detects the Creation of an Archive using Command Line	TA0009	T1590.001	2022-09-08 08:12:48	Investigation_020022
velox45-PC	192.168.0.217	Info	Process Injection	An unsigned application injects code in the context of another process.	TA0004, TA0005	T1056.012	2022-09-10 05:02:44	Investigation_010022
TSS	192.168.40.1	Info	Registry Query via Reg.exe	Registry Tool (reg.exe) was executed to query a registry.	TA0007	T1012	2022-09-09 09:23:14	Web Investigation
lally-server	192.168.0.28	Info	Process Injection	An unsigned application injects code in the context of another process	TA0004, TA0005	T1056.012	2022-09-09 13:35:11	Investigation_020022
LAFPTOP-D20GH29	192.168.0.110	Info	Registry Shell Spawning Persistence	Detect modification of auto-start (shell spawning) registry	TA0003, TA0004, TA0005	T1547.001, T1112	2022-09-10 05:01:30	Investigation_020022
LAFPTOP-18A7.LDJ	192.168.0.234	Info	Service Execution	A Windows System Utility was executed to start a service.	TA0002	T1590.002	2022-09-09 06:16:03	Investigation_030022
DESKTOP-VTVS4L9	192.168.0.106	Info	Firewall Bypass For Application Communication via Registry Modification	A Registry has been created to allow the traffic from certain application through firewall.	TA0005	T1592.004, T1112	2022-09-09 10:11:51	Investigation_010022

