

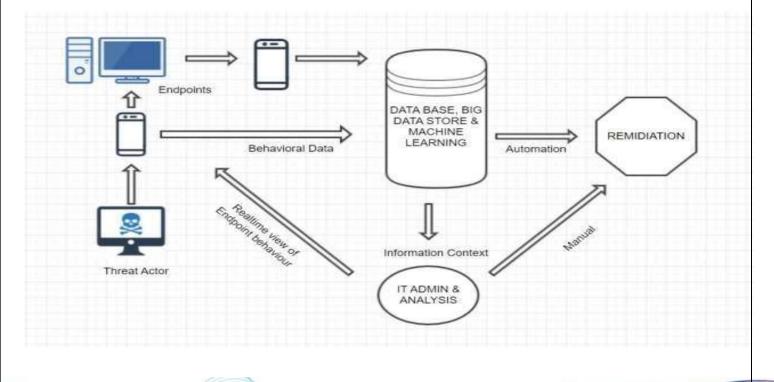


# SecureIT- Anti Virus End Point Detection and Response

# 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 ofstorage.

- 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?



# **SecureIT EDR- Dashboards**

### A) Alert Dashboard



# **B)** CVE Dashboard

|               | _         |                |            |                            |                       |               |                 |               |             |               |               |     |
|---------------|-----------|----------------|------------|----------------------------|-----------------------|---------------|-----------------|---------------|-------------|---------------|---------------|-----|
| Dashboard     | ٠         | CVE Details    | 3          |                            |                       |               |                 |               |             |               |               |     |
| Alerts        | < No. 100 | Show 10        | entries    |                            |                       |               |                 | S             | earch:      |               |               |     |
| Setting Panel | <         | CVE            | CVSS Score | Vulnerability Assessment   | Versions Affected     | Version Fixed | Notes           |               |             |               |               |     |
|               | 4         | CVE-2021-23450 | 9.8        | Remote code execution      | 17.0.0.3 - 22.0.0.2   | 22.0.0.3      | Affects the ad  | min-Center-   | 1.0 feature |               |               |     |
| Admin         |           | CVE-2021-26296 | 8.8        | Cross-site request forgery | 17.0.0.3 - 21.0.0.3   | 21.0.0.4      | Affects the jsf | 2.2 and jsf-2 | .3 features |               |               |     |
| Other         | <         |                | 7.5        | LDAP injection             | 17.0.0.3 - 22.0.0.1   | 22.0.0.2      | Affects the Ida | pRegistry-3   | 0 feature   |               |               |     |
|               |           | CVE-2022-22475 | 7.1        | Identity spoofing          | 17.0.0.3 - 22.0.0.5   | 22.0.0.6      | Affects the ap  | pSecurity-1.  | ), appSecu  | rity-2.0, ap  | pSecurity-3.0 | and |
|               |           |                | 5.4        | Spoofing attack            | 21.0.0.12 - 22.0.0.1  | 22.0.0.2      | Affects the op  | enapi-3.1, m  | pOpenAPI    | -1.0, mpOp    | enAPI-1.1, mp | Ор  |
|               |           | CVE-2020-10693 | 5.3        | Bypass security            | 17.0.0.3 - 20.0.0.10  | 20.0.0.11     | Affects the be  | anValidation  | 2.0 feature | э.            |               |     |
|               |           |                |            | Identity spoofing          | 17.0.0.3 - 22.0.0.7   | 22.0.0.8      | Affects the ap  | pSecurity-1.  | ), appSecu  | irity-2.0, ap | pSecurity-3.0 | and |
|               |           | CVE-2022-22310 | 4.8        | Information disclosure     | 21.0.0.10 - 21.0.0.12 | 22.0.0.1      | Affects the jax | ws-2.2 featu  | re          |               |               |     |
|               |           | CVE-2021-39038 | 4.4        | Clickjacking vulnerability | 17.0.0.3 - 22.0.0.2   | 22.0.0.3      | Affects the op  | enapi-3.1, m  | pOpenAPI    | -1.0, mpOp    | enAPI-1.1 and | mj  |
|               |           | CVE-2021-46708 | 4.3        | Clickjacking               | 21.0.0.12 - 22.0.0.1  | 22.0.0.2      | Affects the op  | enapi-3.1, m  | pOpenAPI    | -1.0, mpOp    | enAPI-1.1, mp | Ор  |
|               |           |                |            |                            |                       |               |                 |               |             |               |               |     |

### C) Threat Analysis Center

|                 |   | Threat Analysis Center-Dashb | oard     |                          |         |                  |               |
|-----------------|---|------------------------------|----------|--------------------------|---------|------------------|---------------|
| Dashboard       | < |                              |          |                          |         |                  |               |
| Alerts          | ٠ |                              |          | Most Recent Threat Graph |         |                  |               |
| 2 Setting Panel | • |                              |          |                          |         |                  |               |
| Admin           | • |                              |          |                          |         |                  | Search:       |
|                 | _ | Time Created                 | Priority | Name                     | User    | Device Name      | Device IP     |
| 2 Other         | < | Jun 30,2022 1:46 AM          | High     |                          |         | DESKTOP-6VM9OPF  | 172.29.64.1   |
|                 |   | Jun 30,2022 1:44 AM          | High     |                          |         | DESKTOP-42.AKFGA | 192.168.0.197 |
|                 |   | Jun 30,2022 1:44 AM          | High     |                          |         | DESICTOP-IMVHK59 | 192.168.0.78  |
|                 |   | Jun 30,2022 1:42 AM          | High     |                          |         | DESKTOP-AK9PHL1  | 192.168.0.43  |
|                 |   | Jun 30,2022 1:40 AM          | High     |                          | Velox_5 | DESKTOP-MUF7VFG  | 192.168.0.237 |
|                 |   | Showing 1 to 5 of 5 entries  |          |                          |         |                  |               |
|                 |   |                              |          |                          |         |                  |               |
|                 |   |                              |          |                          |         |                  |               |
|                 |   |                              |          |                          |         |                  |               |
|                 |   |                              |          |                          |         |                  |               |
|                 |   |                              |          |                          |         |                  |               |
|                 | - |                              |          |                          |         |                  |               |
|                 |   |                              |          |                          |         |                  |               |

Page 3 of 6

# D) Signaturewise Pattern Report

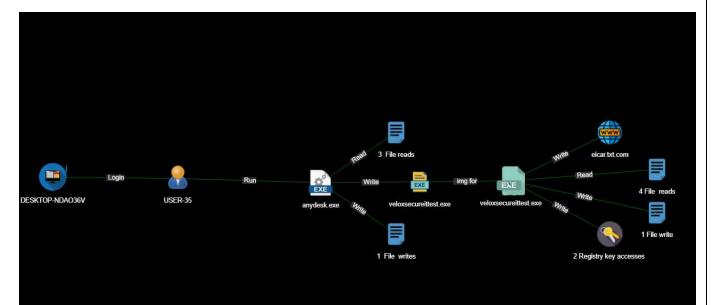
|                 | Event | Host i | EDR HIPS | 3            |                       |                          | \$                                 | Secure[] <sup>0</sup> -EDR   | ▲ <b></b>       | / e             | <b>-</b> 0                         | poc -        |
|-----------------|-------|--------|----------|--------------|-----------------------|--------------------------|------------------------------------|--|-----------------|-----------------|------------------------------------|--------------|
| n Dashboard     |       |        |          |              |                       |                          |                                    | Signature Base Pattern Report  |                 |                 |                                    |              |
| Alerts          | •     |        |          |              |                       |                          |                                    |  |                 |                 | Search:                            |              |
| 2 Setting Panel | ۲.    |        | Sr No *  | Pattern Type | Specification Version | Created Date             | Pattern Name                       | Domain Name  | Pattern Version | Description     | Modified Date                      | Valid Date   |
| 🕜 Admin         | •     |        |          | yara         |                       | 2017-07-24121-42-36.0002 | OTX pulse_name=PoS Scammers Toobox | nde BakoteRCM ( metz autor – "Alemault Labe" reference –<br>http://doc.brithec.compositions-anew-water.of.the-backat Pelaparant<br>- doc.brites.compositions-anew-analysis-of-backat Pelaparant-<br>duati-wise Stepparant – syma-two-filterparant – syma-sa Stepparant –<br>vieto-wise Stepparant – wise-wise Stepparant – syma-Stepparant –<br>vieto-wise Stepparant – syma-sket Stepparant – syma-sket Stepparant –<br>vieto-wise Stepparant – syma-ket Stepparant – syma-sket Stepparant –<br>vieto-wise Stepparant – syma-sket Stepparant – syma-sket Stepparant –<br>vieto-wise Stepparant – syma-sket Stepparant – syma-sket Stepparant –<br>sket – sket Stepparant – syma-sket Stepparant – syma-sket Stepparant –<br>sket – sket Stepparant – syma-sket Stepparant – syma-sket Stepparant –<br>sket – sket Stepparant – syma-sket Stepparant – syma-sket Stepparant –<br>sket – sket Stepparant – syma-sket Stepparant – syma-sket Stepparant –<br>sket – sket Stepparant – sket Stepparant – sket Stepparant –<br>sket – sket Stepparant – sket Stepparant – sket Stepparant –<br>sket – sket Stepparant – sket Stepparant – sket Stepparant –<br>sket – sket Stepparant – sket Stepparant – sket Stepparant –<br>sket – sket Stepparant – sket Stepparant – sket Stepparant –<br>sket – sket Stepparant – sket Stepparant – sket Stepparant –<br>sket – sket Stepparant –<br>sket – sket Stepparant – sket Stepparant –<br>sket – sket Stepparant –<br>sket – sket Stepparant –<br>sket Stepparant –<br>sket – sket Stepparant –<br>sket – sket Stepparant –<br>sket Stepparant –<br>ske |                 | BackoffROM      | 2017-07-24721:42:36.000            | Z 2017-07-2  |
|                 |       |        |          | yara         |                       | 2017-07-24121.42.36.0002 | OTX pulse_name=PoS Scammers Toobox | hale BocketROM-hashes (metz, autor – "Alexandri Late" notemen, bash – 3586/7386/7386/7386/7386/7386/7386/7386/73   |                 | BackottROMHashe | a 2017-07-24 <b>1</b> 21:42:36.000 | IZ 2017-07-3 |
|                 |       |        |          | yara         |                       | 2014-11-19719:00:59.7092 | PuS Scammers Toubox                | The backford Cut-states (rests, and $-$ Mercel Lat , restrict, hard , and the state of the states (rests, and the states (rests, and the states)) and the states (rests) and the state  |                 | BackottROMHashe | s 2017-10-31T23.40:15.891.         | Z 2017-07-2  |
|                 |       |        | 4        | yara         | 21                    | 2014-11-19719:00:59:7092 | Open Threat Exchange               | The BiodefFUAH setup (max, allow - Amminul Lady reference) sub-<br>metric (and a setup  |                 | BackoffROMHashe | s 2014-11-19719:00:59.709;         | 2 2017-07-2  |



### **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 ofsecurity by identifying, responding to, and deflecting both internal and external threats

# Topology





### **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 andIncident 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 singleagent 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 applicationwhitelisting 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



### **Default templates:-**

- GLBA: Gramm-Leach-Billey 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

| Linfo Alerts             |               | High Alerts | A Medium Alerts   | Low Alerts  |                        |                  |                     |                    |
|--------------------------|---------------|-------------|---|---|------------------------|------------------|---------------------|--------------------|
|                          |               |             |   |   |                        |                  | Search              |                    |
| Device Name              | Device IP     | Risk level  | Detection filter  | Description   | Taclic                 | Technique        | Delected            | Investigation      |
| WINCTRL-BLT1N00          | 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                 | T1562.004, T1112 | 2022-09-07 09:53:04 | Investigation_0209 |
| WINCTRL-4TP7FPM          | 192.168.0.98  | Info        | Potential Spear phishing Attachment - Archive File                      | An email with a potential spear phishing attachment - archive file                          | TAD001                 | T1568.001        | 2022-09-06 08:12:48 | Investigation_0209 |
| VSPL-PATCH-TEST          | 192.168.56.1  | Info        | New Service Creation Via Registry                                       | Detect creation of new service  | TAD003, TAD004, TAD005 | T1021.002, T1570 | 2022-09-09 09:19:42 | Investigation_0300 |
| VSPL-DEV-015             | 192.168.0.54  | linfo       | Data Compression via Command Line                                       | Detects the Creation of an Archive using Command Line                                       | TA0009                 | T1580.001        | 2022-09-06 08:12:48 | Investigation_0200 |
| e velox45-PC             | 192.168.0.217 | Info        | Process Injection   | An unsigned application injects code in the context of another process.                     | TA0004, TA0005         | T1055.012        | 2022-09-10 05:02:44 | Investigation_0109 |
| TSS                      | 192.168.48.1  | 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  |
| e taly-server            | 192.168.0.28  | Info        | Process Injection   | An unsigned application injects code in the context of another process                      | TA0004, TA0005         | T1055.012        | 2022-09-09 13:35:11 | Investigation_0209 |
| CAPTOP-D2QGH251          | 192.168.0.110 | Info        | Registry Shell Spawning Persistence                                     | Delisct modification of auto-start (shell spawning) registry                                | TAD003, TA0004, TAD005 | T1547.001, T1112 | 2022-09-10 05:01:30 | Investigation_0208 |
| CAPTOP-18A7JLDJ          | 192.168.0.234 | Info        | Service Execution   | A Windows System Utility was executed to start a service.                                   | TA0002                 | T1589.002        | 2022-09-09 08:16:03 | Investigation_0309 |
| 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                 | T1562.004, T1112 | 2022-09-09 10:11:51 | Investigation_0109 |
| Showing 1 to 10 of 25 en | itries        |             |   |   |                        |                  | Previous            |                    |
|                          |               |             |   |   |                        |                  | Previous            |                    |

### **Observed Techniques**