pathSolutions

TotalView Security Operations Manager

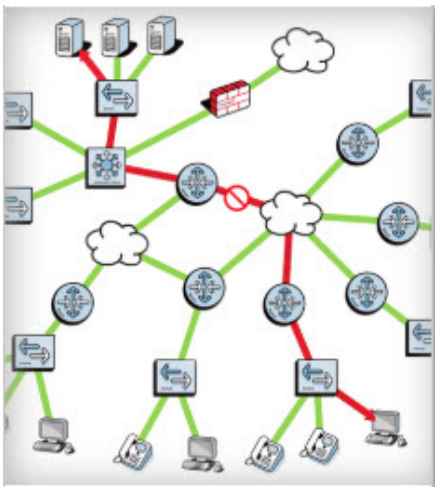
Product Features

TotalView Security Operations Manager is a SecOps and SOAR solution that will dramatically speed up SIEM/IDS event research and resolution by giving you Total Network Visibility® into your entire footprint. This security application tells your team: what is connected to your network, where they are connected, who is logged in, what they are doing, whom they are communicating with, and where data is going so security events can be resolved within a minute. This gives your SecOps team the ability to research and enrich events rapidly with the right information so a single analyst can resolve over 200 events in an 8 hour day versus 20 events with typical playbooks. Additional features are included to help improve your overall security posture.

SCOPE

SecOps Monitor the security footprint of an entire network and connected devices.

SOAR Monitor and respond to SIEM events and cybersecurity issues.



Communications Policy Monitor

Nightly Security Report

FEATURES

- **Geographic Risk Management**

  Know where your data is going and who is communicating with whom to help eliminate exfiltration events.

- **Event Response Acceleration**

  Everything is provided to fully research a SIEM alert and respond within minutes in this comprehensive solution

- **Exposures Reporting**

  If you knew about poor practices in your environment, you could work to remediate them, or accept the risk by whitelisting.

- **New Device Discovery**

  When new devices pop onto your network, instantly know where they are, what they are, and whom they communicate with.

Contact PathSolutions for more information or to schedule a demo.

www.PathSolutions.com

Sales@PathSolutions.com

(877) 748-1777

FEATURES

- **Rogue IT**

  Instantly become aware of Rogue IT devices like WiFi APs, DHCP servers, DNS servers, and switches in the environment.

- **Rapid Quarantine**

  Rapidly or automatically quarantine suspicious devices in the network.

- **Security Footprint Awareness**

  Become aware of everything you are responsible for within the entire enterprise footprint: all computers, devices, and infrastructure elements.

- **Suspicious Communications**

  Communications are analyzed to detect known bad actors like Bot controllers and Tor Servers.

- **Nightly Security Report**

  TotalView sends out a nightly security report so the team can know what exposures exist and what problems are developing every morning.

- **Communications Policy Manager**

  Define acceptable usage policies for your organization and get notifications when policies are violated.

- **Infrastructure OS Vulnerability Detection**

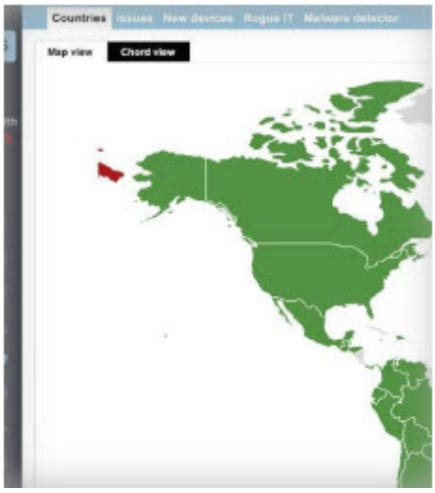
  The risk level and CVE summary of each exposure is automatically tracked. The system fetches nightly updates from the NIST National Vulnerability Database (www.NIST.gov), on any known vulnerabilities for all of your infrastructure devices.

- **Communications Risk Monitoring**

  Communications flows are monitored for their threat level as well as the city and country where the communications is going. This helps to identify the risk level with each external communications.

- **IoT Security**

  Automatically detect IoT devices along with when, where, and whom they communicate with to help reduce risks and exposures generated by these devices.



Geographic Risk Management

IoT Security

Rogue IT

Contact PathSolutions for more information or to schedule a demo.

www.PathSolutions.com

Sales@PathSolutions.com

(877) 748-1777