Cybersecurity through Continuous Monitoring - Protecting Against Internal & External Threats

Mr. Ed Bender
Lead Federal Systems Engineer
SolarWinds

Government IT has long been focused on external cybersecurity threats and continues to apply the bulk of their resources both bandwidth and budget to defending against attacks from the outside. However, in a recent survey of 200 federal IT decision makers by SolarWinds and Market Connections, more than half (53%) of federal IT Pros identified careless and untrained insiders as the greatest source of IT security threats at their agencies, up from 42 percent last year. This growing insider threat brings to light a new set of challenges for IT pros who are now defending their agencies data from an enemy much closer to home.

SolarWinds software delivers actionable intelligence to proactively identify and thwart both internal and external threats and vulnerabilities with visibility into where, when, what and who is on a network, logged into a system, working with important data, and more. SolarWinds cybersecurity and continuous monitoring solutions provide different views of the same stream of raw IT data and take automated action to quarantine and mitigate damage, and analyze data to prevent future attacks. SolarWinds security solution combines several products which create a well-armed barrier to combat cyber-attacks:

- SolarWinds Log & Event Manager provides powerful security information and event management (SIEM) capabilities, including real-time log collection, correlation and analysis, file integrity monitoring, and active response

- SolarWinds Firewall Security Manager simplifies troubleshooting and models the effects of rule changes with multi-vendor firewall security and change management

- SolarWinds Network Configuration Manager provides automated network configuration and compliance management, including automated DISA STIG and NIST FISMA compliance reports

- SolarWinds Patch Manager allows for deployment and management of third-party applications and Microsoft patches from a central point of control across tens of thousands of servers and workstations

- SolarWinds User Device Tracker support network forensics by providing automated device tracking and switch port management while also helping keep rogue devices off the network

- SolarWinds NetFlow Traffic Analyzer identifies which IP addresses and applications are using bandwidth on critical links to help identify the who and when of network usage

- SolarWinds Server & Application Monitor provides rich capabilities to monitor and fix servers and applications, while also providing a complete inventory of all software and hardware installed on systems.

- SolarWinds Serv-U Managed File Transfer Server provides managed file transfer and secure file sharing for Windows and Linux and meets FISMA criteria

- All SolarWinds solutions mentioned are currently available and will be demonstrated during this presentation .