FLOWTRAQ®

SpectorSoft

SOLUTION OVERVIEW

COMBINED NETWORK BEHAVIOR AND USER ACTIVITY INTELLIGENCE: THE ULTIMATE IN INSIDER THREAT DETECTION AND MITIGATION

A recent survey[1] asked information security decision-makers — from financial services, professional services, healthcare, retail, and government organizations around the world — what keeps them up at night. And insider threats were high on the list for the 345 pros polled.

What scares them most about insider threats? It's the imposters — the bad actors who can infiltrate an organization by taking over an account and posing as a legitimate user. Their motivation can be anything from mischief to major fraud — and these breaches cost significant time, money and resources that the organization can't afford to spare.

Protection from imposters requires rapid and reliable detection that offers immediate insight into what's happening, how it's happening, where it's happening and how to stop it — fast. Leveraging a combination of **network behavior intelligence from FlowTraq®** and **user activity intelligence from SpectorSoft®**, organizations can quickly detect, mitigate and defend against these types of insider attacks.

FLOWTRAQ AND SPECTORSOFT: THE BEST DEFENSE AGAINST INSIDER THREATS

FlowTraq analyzes network traffic flow records to provide an unprecedented level of network situational awareness for fast and easy monitoring, quick security analysis and complete forensic recall of any network traffic. FlowTraq learns and understands the changing patterns of behavior in your network. When any system, mobile gadget, or server starts behaving outside the normally expected patterns, you are alerted so you can catch unknown attacks, botnet control channels, new viruses — and stop unwanted data leakage immediately. With an infinitely scalable traffic handling core, a fully parallel database, and a **powerful network behavioral intelligence engine**, FlowTraq is designed to detect and alert on suspicious activity in big networks with traffic flow rates of one million flows per second or more.

Spector 360 Recon and **Spector 360** work together seamlessly to analyze user behavior patterns, detect anomalies, and collect detailed user activity data to inform incident response and support investigations. Effective detection of insider threats requires focus on the insider. By logging a wide range of user activity data, the solutions are able to detect shifts in the behavior of a user and alert when those shifts suggest threat. Powerful reporting, search, and review capabilities — including the ability to replay user interactions with resources as they occurred — enable rapid assessment of, and response to, potential threats.

> "Often when we find anomalous user behavior, it's usually a compromised machine as opposed to finding an actual bad guy."
>
> — A CISO in response to the SpectorSoft/451 Group information security survey

[1] Survey conducted by the 451 Group on behalf of SpectorSoft in Q4 2014. 345 respondents. Financial Services, Professional Services, Healthcare, Retail, and Government verticals. All companies with 1,000+ employees in North America, APAC, and EMEA.

INSIGHT INTO NETWORK BEHAVIOR AND USER ACTIVITY DURING AN IMPOSTER ATTACK

There are typically three phases to the imposter's approach — and combining network behavior intelligence and user activity intelligence gives you the insight you need to minimize the impact of the attack.

1. Infiltration

Initial malicious activity often includes scanning, password cracking or attack propagation. Although a skilled imposter shouldn't have to resort to "noisy" techniques like this, 60 percent of "bad" network behavior fits into these categories. And due to weak passwords, forgotten default credentials and/or poor firewall policies, they're surprisingly successful. But, with FlowTraq's advanced network behavior intelligence, these are an easy catch.

2. Data Gathering

Once in, an imposter will look like a legitimate user from an authorization and authentication perspective, but won't behave like a normal user. The amount and frequency of data accessed will be unusually high compared to a legitimate user — because the imposter isn't interested in processing information as a user would. And while the data will appear to be going to a safe, internal system/user, the reality is that this is a precursor to a potential data exfiltration. SpectorSoft's unique user activity intelligence capability seeks out these types of anomalies — making it simple to detect, alert, and respond to insider threats.

3. Data Exfiltration

With data in hand, the imposter doesn't have access to "physical" options — removable media, laptop, or printing — so the data needs to be moved to a remote server (often cloud-provisioned, temporary accounts). **FlowTraq's** advanced network anomaly detectors will flag this immediately — its unique filtering, combined with its **full-fidelity storage**, ensures that no traffic flies under your radar. SpectorSoft's Recon solution flags shifts in user behavior related to cloud storage usage, ensuring nothing slips through the cracks.

With a strong solution in place to analyze both network and user behavior, you have immediate insight into these anomalies — the suspicious user behavior, the abnormal streams flowing out of your network and the unauthorized usage of cloud services — and the intelligence you need to react quickly.

This combined solution gives your network "eyes and ears" — and a long memory to remember what happened. And that knowledge is what will give you the power to anticipate, prepare for and deal with unknown future situations. In short, FlowTraq and SpectorSoft provide a level of depth that allows you keep the network safe and operational — and free from insider threats — today, tomorrow and beyond.

ABOUT FLOWTRAQ

FlowTraq® provides software and services for high-performance network monitoring, analytics, security and forensics to detect a range of network behaviors, including distributed denial of service (DDoS), brute force attacks, botnets, worms, network scans and other network traffic anomalies. To request a free trial of FlowTraq, visit **www.flowtraq.com/trial**, call +1 603.727.4477 or email us at **info@flowtraq.com**.

ABOUT SPECTORSOFT

More than 36,000 companies, schools, and government entities worldwide use SpectorSoft solutions to gain critical insight into their users' behaviors and activities, dramatically reducing the risk of an insider incident, and providing the intelligence needed to effectively respond to insider threats when they are detected. For more information, visit **www.spectorsoft.com**, call +1.888.598.2788 or email us at **sales@spectorsoft.com**.

FLOWTRAQ®