FLOWTRAQ®

CASE STUDY

USING FLOWTRAQ, GEORGIAN COLLEGE QUICKLY IDENTIFIES AND REMEDIATES NETWORK PERFORMANCE AND SECURITY ISSUES

THE CHALLENGE: IDENTIFYING VIRUS ACTIVITY PRODUCING LOW NETWORK VOLUMES

As a member of the Security & Infrastructure Group at Georgian College, Randy Baker started assessing the existing network management tool that had been underutilized due to the lack of available IT resources. As Baker experimented with the software, he investigated a single workstation and discovered only a few network connections and a low volume of small packets destined to a server in China.

While the college has international students from China, the low volume activity was suspicious and indicated a potential security threat. The college was also in the process of replacing its anti-virus solution, and at that time, neither solution detected this threat.

Baker then ran a report to see what Georgian College systems were visiting that server in China and discovered there was a fixed limit on the number of systems included in the report. In this particular case, it took more than a week of rerunning the reports to identify and remediate all of the impacted systems.

“We also could not use all the fingerprints of the behavior to identify other potential hostile servers,” Baker added. “While working with the vendor on how to generate the required results, we realized this version of the old tool did not have all the capabilities we required, and the features were not on the vendor’s product road map.”

The existing network flow tool presented an issue with detecting activity that produced low volumes. Baker could not search for flows that matched the size of the communications he was observing, which prevented the identification of other potential external servers as well as internal compromised destination systems related to the virus.

“When we discovered a network-related security incident, the limitations of the network flow tool impacted our ability to completely identify and adequately respond to the situation,” Baker said. “I started looking for

GEORGIAN COLLEGE

Established in 1967 and based in Ontario, Canada with seven campuses, Georgian College has consistently generated one of the highest graduate employment rates among Ontario colleges for more than a decade.

Student enrollment averages more than 10,000 fulltime students per year and includes close to 500 international students from 33 countries.

The college employs approximately 750 full-time and 1,500 part-time staff.

a replacement solution that could not only function as a performance tool, but also as a security tool. I also wanted a solution that would provide quick and easy access to network flow data and represent that data in one report rather than having to run multiple reports for a complete view."

As a customizable software application, FlowTraq increases insight into network behavior, making it easy to spot risks before they become problems.

THE SOLUTION: FLOWTRAQ PROVIDES REQUIRED NETWORK INSIGHT

To address the challenge, Baker evaluated several solutions including FlowTraq, which uses network flow records to provide integrated monitoring and forensic analysis capabilities. Baker found FlowTraq to be quite flexible, significantly allowing for greater insight into network behavior, which makes it possible to easily spot performance trends before they become performance issues visible to the end user.

When Baker tested FlowTraq, he found the interface quite intuitive: "Within the first hour, I created, saved and scheduled eight different workspaces that gave us the charts we need on a daily basis. I was able to accomplish this by simply using combinations of the pre-defined filters found in the advanced filtering options. After a few days of collecting data flows, we conducted a Web session with the FlowTraq team and identified our pain points. They then demonstrated how FlowTraq solved each problem."

During the evaluation period, when Baker identified an issue, the FlowTraq technical team responded quickly and with informative actions. "Some issues were related to our lack of understanding of the software, which FlowTraq helped us work out," Baker explained. "But they also listened when we identified capabilities we felt they needed to add. All of these issues were addressed in the next release of FlowTraq, with our suggestions incorporated into the product. That shows how FlowTraq does more than just listen to clients — they also react to keep improving their solutions."

What ultimately sold Baker on FlowTraq was the quality and usefulness of the software as well as the responsiveness of the technical support team during the evaluation. "FlowTraq also offers a price point that I felt management would accept," Baker added.

THE RESULTS: IMPROVED ABILITY TO DETECT THREATS AND INVESTIGATE ISSUES IN LESS TIME

While management knew Baker was looking at alternative network flow solutions, he did not yet have a mandate and the budget to acquire a new solution. But Baker demonstrated that just by automatically generating scheduled reports, FlowTraq reduced the amount of time for working with the flows tool on regular daily tasks from one hour down to 10 minutes. "The ability to generate reports that clearly represent the information we need using less IT-resource time played a key role in our overall cost justification," Baker said.

Because Georgian College is an active participant in World IPv6 events, management's first question was, "Does FlowTraq support IPv6?" Having passed that qualification, management then started asking for reports that required increased complexity. "Using the advanced FlowTraq features, I produced the desired results every time," Baker said. "This further demonstrated the value in saved resource time and improved our ability to respond to network issues. This also prompted management to create the necessary budget to invest in FlowTraq."

While the team at FlowTraq was responsive during the evaluation period, Baker wondered how that might change once Georgian College purchased the software. He has been impressed with the continued level of response: "They listen, and their feedback is excellent. For one small bug we identified, FlowTraq quickly created a patch that resolved the issue. I have a very high degree of confidence in the technical support team."

> "Our ability to seek out undetected threats and investigate issues has been significantly increased, and FlowTraq has dramatically reduced the time required to perform these tasks."

Over 99.9% of security events are failed attempts reported in log files, but FlowTraq easily gives Georgian College the ability to audit random events to identify all servers an attacker attempted to breach. "We are able to compare the traffic patterns of an attack on the various servers and have a level of assurance that we are secure when the patterns remain very similar," Baker said. "The IT staff can also see all connections to a specific server based on the country associated with each IP address."

"With our previous tool, we would have had to search for every range of IP addresses that are registered to the country that the attack originated from," Baker added. "But with FlowTraq, one of the pre-defined filters already includes all the ranges of IP addresses registered to each country. Instead of generating multiple reports for a complete view of activity, we can use combinations of pre-defined FlowTraq filters that allow us to run a single report for the complete view."

The Georgian College IT team can search on multiple address ranges at one time while creating complex filters by selecting and combining any of the 33 predefined FlowTraq filter types as many times as necessary. FlowTraq also provides the ability to create raw queries if more detail is needed beyond what the filter options provide.

In summarizing the overall value of FlowTraq, Baker concluded, "Our ability to seek out undetected threats and investigate issues has been significantly increased, and FlowTraq has significantly reduced the time required to perform these tasks."

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**.

FLOWTRAQ®

16 Cavendish Court, Lebanon, New Hampshire 03766 USA
Phone +1 (603) 727–4477 | Email info@flowtraq.com