Federal Cybersecurity

How Analytics Helps Safeguard Your Network

If someone's broken into your house, you can spot it. An open window, a door ajar, a chair out of place, a footprint…these clues all scream "intruder". You know that the window and door were closed when you left, that the chair was pushed in, and that the footprint in the hallway doesn't belong to any member of your household.

Now, let's say the bad guy was in your neighborhood, but had chosen a different house. Would you have spotted something out of the ordinary then?

Identifying an intrusion is easy in our own home. But broaden that view to your neighborhood, or even the whole city, and it becomes much harder. The same principal applies to your network.

As a defender, your biggest advantage is knowing what's normal. When bad guys break in, they just need ONE vulnerability. Once they find that weakness, they get in and hide under the radar. The more you know about your network, the quicker you'll be able to spot an intruder.

What's "normal" for my network?

The key to knowing what's normal is to know your data. While that may seem obvious, odds are you currently have insight into less than 5% of your network activity. That's because most of that data is immediately discarded. But imagine how much better you'd know your network if you stored and analyzed all that data.

Like people, every network is unique. There is no overarching "normal" for network activity. The experts at AlphaSix can work with you to analyze your network and identify key scenarios indicating unusual activity. It's akin to setting up trip wires.

Qlik unlocks the power of information

Find your "aha" moment

Uncover hidden insights or anomalies by viewing all your data. You'll be able to see and explore not only what data is associated to your selected query, but also what's unrelated, which can provide unexpected insights.

Search data like you do the web

Searching the web is easy. Why should your data be any different? Find what you're looking for quickly, so you can move on to the next question.

Be empowered, everywhere

Don't wait to get to the office. Get answers to your questions anywhere, on any device, with an intuitive interface designed for mobility.

Share your story

Save time and keep your presentations on track. Create and publish findings in one place, so you can shift seamlessly from discovery mode to presentation mode and back.

Get answers now

Be up and running in a matter of days, not months. 44% of Qlik customers are live within a month; 77% are live in fewer than 3 months.

Minimize purchasing headaches

Software buying should be easy (and fun!). We work with you throughout the procurement process, offering flexible and scalable license models to deliver outstanding performance and low TCO to user communities consisting of 1 to 50,000+ people.

For example, these scenarios could indicate an intruder:

- **Timing of logins.** Desktop users typically log in between 7am – 5pm, and a user logs in at 2am.
- **Volume of data transfers.** Normal volumes are typically small (i.e., webpage downloads), yet a single connection is transferring gigabytes of data.

While these scenarios might indicate *insider threat*:

- **System queries.** HR and Accounting systems typically don't speak to each other. Someone in HR is running a query on accounting.
- **User behavior.** Executives typically view a high-level dashboard. One exec is viewing the source code.

While there might be perfectly logical explanations for each scenario, having the ability to quickly spot and investigate these anomalies puts you in a much greater position to defend your network and protect your Agency's data.

Collect, Keep, and Analyze Network Data

Collect more information. Keep it longer. Perform deeper analytics. Sounds simple, but with sensors and firewalls and applications all spitting out mountains of data, how can you possibly store all that data? Let alone bring it together to analyze?

AlphaSix can help by using big data strategies on the back end to collect and store all of that data in a Data Lake. Then, using Qlik you can bring all of that siloed data into focus, analyze it, and spot patterns over time. This process enables you to establish a baseline, more deeply understand your network, and recognize (even prevent) both external and internal threats.

About Qlik

Qlik is a leader in data discovery, delivering intuitive solutions for self-service data visualization and guided analytics. Qlik empowers the organization with a flexible analytics tool that not only answers queries, but also helps uncover additional questions to ask of the data. Qlik's products deploy rapidly and customers realize rapid time to value, often in less than 45 days. Contact us at **UncleSam@qlik.com** to schedule a discussion and live demonstration, or visit us at **www.qlik.com**.

About AlphaSix

AlphaSix Corporation™ is a VA CVE-verified Service Disabled Veteran Owned Small Business (SDVOSB) located in the Washington, DC, area. Our mission is to bring our customers innovative technology and solutions to help them in their efforts to reduce costs and improve performance. Areas of expertise include Cybersecurity, Data Center Consolidation, Cloud Computing, Managed Print, Virtualization, Applications Development, and Big Data. Contact us at **team@alphasixcorp.com** or **703-579-6444**, or visit us at www.alphasixcorp.com.