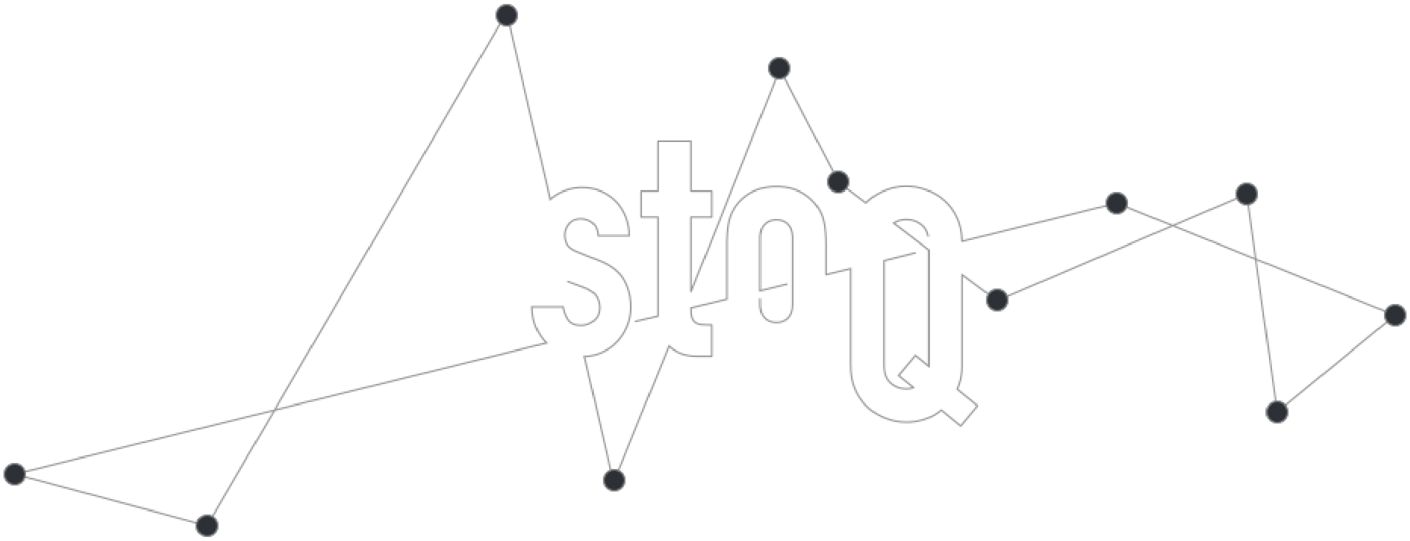

automation. simplified.

DOWNLOAD (HTTPS://GITHUB.COM/PUNCH-CYBER/STOQ)

OVERVIEW

stoQ saves time. It's a super-simple framework that allows cyber analysts to organize and automate repetitive, data-driven tasks, thus freeing them to focus more attention on what matters most. Any organization can use stoQ to better defend their networks. Set up is easy, and it scales to businesses small and large. We recommend you begin by reading a quick introduction (https://medium.com/stoq/introduction-to-stoq-b163b3ec9e08). Once you've read up on how to use stoQ you can download it here (https://github.com/PUNCH-Cyber/stoq/releases) and stop wasting time! Still have questions? Don't worry about it; we're here to help. E-mail us at info@punchcyber.com (mailto:info@punchcyber.com), and we'll do what we can to get you up and running.

Simplified Automation

A modern and highly modular framework that allows for quick and easy analysis of files, network traffic, IOC extraction, and just about anything else an analyst may need.

Individual and Enterprise Ready

From junior to senior analysts, everyone can use stoQ. By collecting analytic results from all sources utilized by an individual or a team, anyone can quickly search for previous examples of anything collected. From enterprise level automated analysis to an analyst processing individuals files, stoQ can do it.

Database Independent

Multiple databases to rule them all. Whether you want to use an RDBM, NoSQL, NewSQL, raw files, or a mixture of them all, stoQ has you covered.

Robust Plugin Architecture

The primary purpose of stoQ is to simplify repetetive analytic tasks. The modular plugin framework embedded within stoQ allows for analysts to quickly develop new plugins without having to worry about databases, input, or output.

Agile Template Engine

Have you ever needed to format data specifically for a device, database, or some archaic requirement? Well, you no longer need worry about how to transform your data since stoQ supports Jinja2 templating for all plugin outputs.

Advanced Content Extraction

Do you need to analyze content with multiple layers of obfuscation or encoding? Perhaps you have an XOR encoded Executable file within an OLE stream within a compressed archive? No problem. Using stoQ's dispatching capabilities, this is a completely automated process.

A modern framework to simplify analysis.

DOWNLOAD (HTTPS://GITHUB.COM/PUNCH-CYBER/STOQ)

ABOUT US

PUNCH Cyber Analytics Group

PUNCH is a boutique cyber-consulting firm that provides advanced analytics and strategic support to government and commercial clients. Our primary focus is in improving an organization's awareness of and ability to manage a growing cyber threat environment. We focus on bolstering cyber preparedness by improving an organization's analysts and the tools at their disposal.

STOQ

DOCUMENTATION (HTTPS://STOQ-FRAMEWORK.READTHEDOCS.IO/EN/LATEST/)

DOWNLOAD (HTTPS://GITHUB.COM/PUNCH-CYBER/STOQ)

CONNECT

PUNCH (HTTP://WWW.PUNCHCYBER.COM)

TWITTER (HTTPS://TWITTER.COM/PUNCHCYBER)