deep sky blue

CASE STUDY: AUTOMATING CYBER DEFENCE RESPONSES

In September 2014 the MOD's Defence Science and Technology Laboratory[1] launched an "Automating Cyber Defence Responses" innovation competition.

Applicants were invited to bid for research funding into tools and techniques that could support the planning and execution of automated responses to cyber threats, with a focus on approaches that support the determination, description and analysis of courses of action.

At Deep Sky Blue we want to protect our nation's infrastructure from cyber attacks so that we are all safer and more secure and this competition gave us an ideal opportunity to build on our experience of developing systems in the defence, cyber and intelligence arenas with a novel and innovative idea.

We drafted an innovative and exciting proposal to investigate whether recommendation algorithms, more commonly used in retail and news sites, could be adapted to suggest appropriate courses of action to take in response to complex cyber events which was awarded first stage funding by Dstl. Our highly skilled and dedicated team of software and test engineers then set to work on proving our hypothesis by researching, designing and building a working proof of concept.

"At Deep Sky Blue we want to protect our nation's infrastructure from cyber attacks so that we are all safer and more secure..."

One year after the competition's closing date we delivered our proof of concept and accompanying research report to Dstl, having demonstrated that recommendation engines can be used in an environment quite different to those for which they were originally designed and intended - the cyber security domain.

More success followed when we were awarded additional funding to progress to Phase 2 of the Automating Cyber Defence Responses work - a fantastic opportunity to further demonstrate our skills and capabilities and take our proof of concept to a higher technology readiness level.

Deep Sky Blue is an agile software delivery company, and we began building potentially releasable software right away. We worked from a backlog of requirements - constantly reviewed and prioritised - so both we and Dstl were confident that we were developing the most important items at any given time. Every month for the duration of the project we were able to deliver a new iteration, demonstrating our progress and enabling us and Dstl to agree what we would work on next.

[1]: Dstl, an executive agency of the MOD

To find out more about Deep Sky Blue and how we can help your business, get in touch now:

deepskyblue.com
info@deepskyblue.com

Deep Sky Blue
Cheltenham Office Park
Hatherley Lane
Cheltenham GL51 6SH

The Innovation Centre
Daresbury
Cheshire WA4 4FS

deep sky blue

The research project came to an end in March this year with the submission of a detailed and comprehensive report and a final demonstration to Dstl of the finished software. As a company, Deep Sky Blue believes in the awesome potential of technology to make a positive difference to our world - and we also believe in the power of people to do the same. That's why the technology we delivered to and in collaboration with Dstl was designed as a tool to help cyber analysts in their challenging role, not as a product to replace their invaluable skills.

Our recommendation engine suggests courses of action on the basis of similar recommended courses of actions. The more users rate the appropriateness of a course of action against a cyber event, the better the recommendation engine becomes and as the recommendation engine learns from the cyber analysts, less experienced cyber analysts can learn from their more experienced colleagues.

Deep Sky Blue's final delivery to Dstl also comprises an auto-bundling algorithm, which aggregates events on the basis of previous, similar groupings, an auto-prioritisation algorithm which, like a sophisticated spam filter, prioritises events as they enter the system, and a library of tactics, techniques and procedures (TTPs) influenced by STIX, the structured language for describing cyber threat intelligence and attack patterns.

Deep Sky Blue expertise:

- Java
- AngularJS
- Elasticsearch
- MongoDB
- ActiveMQ

Our prototype integrates with two common open source intrusion detection systems, and therefore ingests both network and host-based events. Our separate test harness application - also produced as part of our project - emulates a real world installation of those two systems. Recognising the cognitive strain experienced by cyber analysts, we also researched theories of cognitive load and dual process models of thinking, and worked with user experience specialists to design and build an intuitive user interface to make the cyber analyst's life as stress-free as possible, reducing the cognitive burden of what is an incredibly challenging job.

Our work with Dstl demonstrates our expertise in languages and technologies such as Java, AngularJS, Elasticsearch, MongoDB and ActiveMQ and as well as in agile delivery and Behaviour Driven Development. Even more importantly, though, it demonstrates our passion for and commitment to influencing and informing cyber defence capability and strategy for the MOD and beyond.

Although we've now finished our research and development project, we're still working with Dstl. The technology we delivered is just part of a much wider piece of work, and Dstl will be taking our software, along with the outputs of research carried out by other software companies and universities in the UK to a meeting in Toronto later this year of the "Five Eyes" intelligence alliance of the UK, USA, Canada, Australia and New Zealand. We're extremely proud to be part of this exciting and important work.

To find out more about Deep Sky Blue and how we can help your business, get in touch now:

deepskyblue.com
info@deepskyblue.com

Deep Sky Blue
Cheltenham Office Park
Hatherley Lane
Cheltenham GL51 6SH

The Innovation Centre
Daresbury
Cheshire WA4 4FS

deep sky blue