CASE STUDY

SANS | GIAC CERTIFICATIONS

A Discussion with Stephen Kinghan

Head of Cyber Operations

Can you provide a brief overview of your organisation's cyber team including its size, operations, and geographic reach?

We have seven overall FTEs with two augmentees from our MSSP.

What motivated your organisation to invest in cybersecurity training?

One of the main reasons we invest in cybersecurity is because our people are the most important asset, without them our cyber assurance is notional.

How long have you been conducting cybersecurity training with SANS?

We have been training with SANS for approximately 18 months.

What were the key objectives and goals Hiscox aims to achieve with SANS cybersecurity training?

Our key goal is attaining industry leading training and development that would be sufficient to enable the creation of an internal purple team / pen testing capability. That capability establishment could save our business hundreds of thousands over the next 4 years if done correctly.

How did you tailor Hiscox's training programs with SANS to the specific needs and challenges of the insurance industry?

We looked into the detail of the offensive Cyber Pathway and realised it met our requirements. Our account manager Miles Vertigen helped significantly in our understanding of what to expect and focus on.

Can you provide specific examples of improvements or security enhancements that have resulted from SANS training?

The team have already added significant efficiency savings to the way in which security tickets are processed and resolved. Much of the improvements are down to their heightened awareness of adversary activity and what is being seen.

What has been the feedback from your employees regarding the SANS training?

The feedback from the team after returning from a SANS courses has been very complimentary from the most junior to most seasoned member of the team. The courses are very thorough and the instructors are world class. SANS course are really tailored and exactly what was needed for the team.

Are there any success stories or testimonials from employees who have benefited from the training?

The daily impact of SANS upskilling is notable with regards to the team's awareness of hacker techniques and methods, as well as adversarial approaches to our estate.

How does SANS training align with regulatory compliance requirements in the insurance sector?

The impact to our own security assurance statements to both regulators and insurers is significant given SANS's position as leading edge training.

Outside of the available training offerings at SANS, do you also take advantage of the complimentary resources, summits or events available?

Yes, the team will take advantage of the free resources and summits wherever is possible however, due to the cadence of work this is not always possible.

What advice or recommendations would you give to other insurance institutions looking to train with SANS?

The advice I would give to other insurance institutions would be to make sure you pursue SANS training because you value your employees, you invest in them with the most valued and trusted cybersecurity training provider and trust in them to maximize the opportunity to learn and grow their capabilities. This provides a complete circle from supporting your employees with globally recognised training and certifications to protecting your organisation. By enabling the right conditions to allow those skillsets to flourish, we are hopefully generating a desired location for individuals to work.

All views are Stephen's own.