BAE SYSTEMS
INSPIRED WORK

Business Defence Assessment

Understand your exposure, identify risk and demonstrate the value of security analytics

The Problem

Maintaining effective defences against cyber attacks is difficult for any business. Keeping it ahead of the threat is an even bigger challenge. It is an ongoing process that requires a combination of Threat Intelligence, the right technology and the creation and continual updating of procedures and best practises.

Given the ever-increasing volumes of information from logs, security alerts and threat intelligence combined with the need to harness data from mobile, Internet of Things and cloud infrastructures, it's easy for organsations to get swamped. Security managers struggle to get a complete and accurate view of the vulnerabilities, threats and risks. Turning that insight into adaption – allowing them to continue to control, protect and remediate - becomes increasingly difficult.

The job of collecting, organising and operationalising this information has pushed plenty of businesses towards security analytics to help them detect and sort the threats they face so they can work out how to respond against potential attacks.

The Solution

Before making a choice and deciding on a security analytics approach, it is critical to understand how security analytics will fit within your organisation and how it can be applied to your situation. Wouldn't it be great to see how it works, how it is relevant to the threats you face, how it will improve your security operations and ultimately whether it is hype or value? Now, with Business Defence Assessment, you can.

The Business Defence Assessment takes place in three key phases:

Understand your Cyber Threat Exposure

The Security Threat Landscape Assessment looks at the actual, probable and possible attack. It blends together sources from digital risk and Threat Intelligence with real industry relevant security incidents and applies this to your operating environment identifying potential threat vectors and attack scenarios to which you may be susceptible

Test for gaps in your existing security

Utilising the assessment, we generate a set of real life attack scenarios that an adversary might follow. Attack Scenarios are validated against the Kill Chain, our Behavioural Analytics, and evidence gained from investigations.

Experience the value of Security Analytics

We gather metadata over a four week period. This is then analysed in our Threat Analytics platform to search for patterns of behaviour indicative of targeted attacks. This analysis draws upon three distinct activities which will include:

- **Signature analysis -** BAE Systems will use its own network signature database to identify known threats within the network
- **Behavioural Analytics -** BAE Systems will apply its behavioural analysis and attack discovery techniques to identify possible targeted cyber attacks
- **Threat Hunting -** BAE Systems analysts will hunt through the data to identify hidden threats that may have successfully exploited gaps in existing security controls

The Outcome

Phases one to three are brought together in a detailed report outlining the findings, including remediation of issues and recommendations to improve your cyber security and risk profile. The report is presented in a debrief session located in the BAE Systems Security Operations Centre (SOC) where you can engage with the analysts, see how the tools were used and discuss our service offerings and next steps in more detail.

BDA Components

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

UK: +44 (0) 1483 816000

E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai