Cyber Security & ICT Solutions

CYBER THREAT INTELLIGENCE

Threat Intelligence provides the situational awareness and foresight needed to improve the resilience of your critical business operations and provides tangible benefits by protecting your business winning critical information and intellectual property. It will enable your Cyber Security Operations to move from reactive to proactive by enhancing your ability to understand, predict and target threat factors.

Most security operations depend upon the reactive mind set of the well intentioned security professional. Without intelligence most security operations prioritise resources based on narrow and incomplete data using only the experience of the people at their disposal.

Threat Intelligence focusses security operations and business activity to cyber risk and its management. It provides analysis and insight into the threats most likely to have a detrimental business impact. The management of risk helps to justify targeted investment in cyber security.

Enhanced situational awareness, insight and proactivity helps security operations teams to start to understand the threat landscape. It allows you to analyse your business behaviour and how it affects the threat landscape in order to adapt and change to mitigate the risk.

The concept of bringing together Cyber Security Operations with other forms of business activity to reduce Cyber risk can only be achieved through an intelligence-led understanding of your company's threat landscape. Without this insight your Security Operations team remains behind the curve and completely reactive.

WHAT DOES IT ACTUALLY LOOK LIKE?

Threat Intelligence comes in many forms. An agile and flexible business needs a product and level of understanding that is appropriate for the business. We can provide this in many forms and in a variety of ways.

CTI

CYBER THREAT REPORTING

Reporting is in a human readable report with the job to inform key decision makers at an operational and strategic level. The monthly Cyber Intelligence reports specific to your company inform on wider trends as well as industry specific threats.

Threat reports are aimed at your operational teams so when high priority threats are discovered your operational teams have up to date information in order to mitigate the threat. We can deliver these in a format that integrates seamlessly into your current reporting templates.

TECHNICAL THREAT FEED

Our technical threat information feeds your SIEM harnessing over 30 OSINT feeds, sources from closed communities as well as threat data from our Italian SOC which protects 40 European customers. This fused technical feed is constantly analysed for source credibility and threat impact to ensure the information reaching your SIEM keeps your operational teams ahead of the curve.

INTELLIGENCE BRIEFINGS

Aimed at senior decision makers, these intelligence briefings update your C-level stakeholders on the threat environment affecting you. These customised briefings can be technical or non-technical and demonstrate how the current Cyber Threat relates to wider business activity and business risk, thus supporting timely tactical change in business responses to emerging threats.

ANALYST SUPPORT

We offer a reach back service to our analysis team for the investigation of particular issues or threats leading to bespoke products relevant to your team and current situation. Whether it is trend analysis in order to inform investment activity or a requirement for some in-depth research on malware, our analysts will ensure you receive actionable, timely and relevant reporting.

EMERGENCY RESPONSE

If you need emergency response support from our CIRT then our Threat Intelligence team will work closely, providing support and analysis to incidents. Such incidents often require deep expertise when dealing with complex threat actors, especially surrounding ransomware scenarios.

OTHER SERVICES OFFERED

Our Cyber Operations Group offers a range of associated services which can be tailored and integrated with the Protective Monitoring Service including:

- Incident Response
- Vulnerability Assessment
- Security Device Management
- Behavioural based Threat Detection
- Penetration Testing
- Red Team testing
- Vulnerability Management.

LEONARDO
SECURITY & INFORMATION SYSTEMS

For more information please email infomarketing@leonardocompany.com
Leonardo MW Ltd
430 Bristol Business Park - Coldharbour Lane - Bristol - BS16 1EJ - United Kingdom - Tel: +44 (0) 117 988 0033