Operational Threat Intelligence

CYBERFORT

Businesses today much contend with an unprecedented range and volume of cyber threats

A growing army of state-sponsored attackers, cybercriminals, hacktivists and other perpetrators are at work trying to breach businesses defences with ever-more inventive and complex attacks.

Security monitoring alone is no longer enough to keep your business protected. Only up-todate knowledge of the ever-changing tools, techniques and procedures used by attackers can truly flush out those persistent threats that lurk in the shadows, often undetected, trying to gain a foothold into your networks, devices and social circles.

While most threats can be neutralised with strong risk management processes, there are always a few threats that will filter through security gaps in your people, processes and technology.

Cyberfort's Operational Threat Management Service will support your security operation by combining highly-tuned threat intelligence delivery with skilled human analysis. We'll provide you with understandable and actionable intelligence that will enable the most cost-effective and powerful security operations.

Cyberfort's expert team will enable your business to demonstrate its commitment to security. We'll help you inspire customer confidence, strengthening your marketability and ensuring legal and regulatory compliance.

Beginning with the identification of your critical assets, data patterns and current vulnerabilities, Cyberfort provides a live threat assessment that will enable targeted threat management, including:

- Internationally recognised technical intelligence feeds drawn from:
  - Live Global Attack, Threat and Indicator of Compromise Intelligence
  - Human, Open Source and Social Media Intelligence (HUMINT, OSINT, SOCMINT)
  - Intelligence gathered by operatives within the Deep and Dark Webs
  - CiSP – The NCSC's Cyber Security Information Sharing Partnership
  - MISP – The international Malware Information Sharing Platform
- Intelligence provided either as a feed for your operatives or as an analysed product with emphasis on Tactical, Technical, Operational and Strategic uses
- Intelligence to drive the Security Operations Triad of Automated Vulnerability Management, Alert Monitoring and Analysis; and Operational Threat Hunting as a Managed Service

Starting with a thorough assessment of your business, Cyberfort Operational Threat Management services include:

Foundation Assessment Phase

Combining Asset Discovery, Data Mapping, Vulnerability Assessment and Live Threat Intelligence to create a highly specific, personalised and up-to-date threat assessment relating specifically to your organisation, critical assets and the most likely attack vector (entry points).

Optional Incident Preparation and Planning Phase

Using Cyberfort's technical expertise to optimise the operational visibility of your environment, we'll develop bespoke incident plans, policies and procedures. We'll then guide your organisation through education and testing phases to prepare, manage and mitigate against cyberattacks.

Operational Threat Management Services

Combining varied threat intelligence feeds with human analysis, Cyberfort will deliver tailored and effective information to provide you with - or support – your security operations triad of:

- Automated Vulnerability Management
- Incident/Event Logging Monitoring and Analysis
- Effective Threat Hunting

Your threat intelligence challenges

At Cyberfort, we understand the cost-effective security operations conundrum that weighs on the minds of organisational C-Level and security teams across the globe. These challenges include:

- Lack of in-house skills and capabilities to carry out effective risk management and compliance activity, including logging, 24/7/365 protective monitoring and incident analysis
- Despite well-designed rule-sets, the sheer volume of data generated by your business is too great to manage. Events are missed, vulnerabilities aren't remediated and no real insight is gained into your security posture
- Despite reducing rule sets and muting smaller alerts, your teams still struggle to identify suspicious activity from 'noise'
- You've tried to implement technical solutions without sufficient guidance, advice or due diligence to ensure return on investment, leaving the C-suite disillusioned by security endeavours

How Cyberfort can help you

Cyberfort's Threat Management Service enables organisations to automate their vulnerability management processes, and define alert rulesets that are effective and specific to their environment. We go beyond passive monitoring to hunt out those early indications that an attack is underway. The services will help you achieve the following benefits:

- Tailored security operations devised implementing findings of your personalised threat assessment
- You gain relevant and actionable threat intelligence aligned to your organisation's priorities
- Automated vulnerability management
- Personalised and effective incident alerting, triage and escalation
- Targeted threat hunting
- Robust incident response capability
- Compliant security operations practices that are aligned to your legal, regulatory and compliance obligations