MSP1

Managed Detection and Response

Threat hunting, detection and response to even the most sophisticated and novel attacks - part of our wider MSS portfolio.

As the capabilities and sophistication of cyber-attacks evolve traditional technologies deployed are struggling to keep deal with the threat. The volumes of data across your infrastructure and alerts created by security equipment is overwhelming you and obscuring your detection and response to threats. Your analysts struggle to investigate every alert in a meaningful time and incident responders don't have the complete picture to affect a timely or complete response.

Harness the power of MSP1's detection and response services.

Managed Detection and Response (MDR) from MSP1 focuses on the importance of both the detection of, and complete response to, sophisticated attacks masquerading as legitimate activity to breach security.

Detection

Managed Detection and Response uses advanced threat analytics to detect both existing and entirely new attack types. The service has the ability to take a wide angled view of your organisation. MDR acquires as broad a set of data as possible using our expertise in Big Data to process, store, fuse, correlate and visualize a vast variety and volume of data.

It then creates an organisation baseline and uses advanced behavioural detection analytics to detect anomalies. When combined with context from sources such as HR, financial data, Technique, Tactics and Procedures (TTP) Intelligence and risk, these analytics can be used to detect a broad set of known, modified or brand new attack techniques across all stages of the kill chain.

Response

MSP1 SOC Analysts and responders have comprehensive visibility and rapid access to data to fully investigate potential threats. Aside from reducing the impact of attacks, this approach gives a wealth of data that facilitates the rapid and thorough investigation of even the most complex cyber threats. This allows full, comprehensive and step by step remediation advice to be shared with our customers, meaning our customers achieve answers, not alerts.

Integrated Threat Hunting

A key element of the managed detection and response service. MSP1 threat hunters act in two specific ways to combat new and innovative or novel threats:

- A team of highly trained subject matter experts search for and investigate behavioural anomalies and deviations from a customer's standard digital behaviour or baseline, which could be indicators of previously unknown attack.
- Using MSP1 privileged access to intelligence, hunters create and test hypotheses of possible attacks. They have the ability to fuse and interrogate large disparate data sets, calling on behavioural analytics, machine learning, raw data search and visualisation tools, to uncover new patterns of malicious behaviour and adversary TTPs.

Detection through hunting quickly flows into creation of new actionable threat intelligence leading to the development and enrichment of automated analytics, rules and signatures which improve existing detection and protection mechanisms.

Contact Sales

+1 (408) 769 5030

+91 9769757668

www.MSP1services.com
info@msp1services.com

MSP1 helps businesses fight cybercrime, protect data and reduce security risk. We are a leading provider of cybersecurity solutions and services. Through our global SOC and delivery center we monitor detect, contain and remediate IT threats.

With integrated technologies and our team of security experts we enable businesses to transform the way they manage their information security and compliance programs. Our services are customized, tailored and white labeled that fit your budget.