SYS IT SECURE XDR–END TO END BREACH PROTECTION

SYS IT Secure XDR is purpose-built to deliver complete protection, based on three pillars: prevention and detection of all common and advanced threats, full automation of the entire response flow from initial detection to complete eradication of the malicious activity and continuous monitoring of this process by security professionals to ensure and elevate the precision and quality of the process.

XDR

Endpoint Protection

Multilayered protection against malware, ransomware, exploits, and fileless attacks

Network Protection

Protecting against scanning attacks, MITM, lateral movement, and data exfiltration

User Protection

Preset behavior rules coupled with dynamic behavior profiling to detect malicious anomalies

Deception

Decoy files, machines, user accounts, and network connections to lure and detect advanced attackers

RESPONSE Automation

Investigation

Automated root cause and impact analysis

Remediation

Eliminate malicious presence, activity, and infrastructure across user, network, and endpoint attacks

Playbooks

Automate comprehensive responses across the environment for any attack scenario

Incident View

Intuitive graphical layout of the attack and the automated response actions

MDR

Alert Monitoring

Prioritize and notify customer on critical events

Attacks Investigation

Detailed analysis reports on the attacks that targeted the customer

Proactive Threat Hunting

Search for malicious artifacts and IoC within the customer's environment

Incident Response Guidance

Remote assistance in isolation and removal of malicious infrastructure, presence, and activity

Prevention is a Step. Protection is a Journey.

Protection must be end to end. Prevention or Detection of an attack's instance is critical – but it's only the beginning. One must assume that the malicious artifact that was identified is the mere tip of an iceberg. SYS IT Secure XDR is the only solution that triggers an automated investigation following each endpoint, user, or network alert, fully disclosing its root cause and scope and applying all the required remediation activities.