

Managed Endpoint Detection and Response (EDR) as a service

For a leading Automotive aftermarket company in U.S.-based with over 3,500 Team Members in over 270 locations throughout the country



Customer Objectives & challenges

- ▶ Ability to detect advanced threat.
- ▶ Zero day threat protection.
- ▶ Technology to support and provide information for proactive threat hunting.
- ▶ Faster time to respond to security incidents.
- ▶ Forensics investigation capabilities

Phase 1 Design

- ▶ Technical gap assessment to identify
- ▶ Right fit technical tool identification.
- ▶ Identify deployment landscape and integration methodology

Phase 2 – POC & Pilot

- ▶ EDR solution deployment and agent rollout on test environment, with 5 agents in each OS flavor.
- ▶ Capture tool functionality and system performance after rollout.
- ▶ POC on simulated attack scenarios and tool effectiveness



Our Solution approach

Solution that could complement the existing SOC environment. An EDR as solution was proposed to address the key challenges.

Phase wise approach, to evaluate, best fit tool, evaluate the functionality against objectives and then rollout to production

Phase 3 - Rollout

- ▶ Production Rollout on 6000 endpoints and 700 servers
- ▶ Planned onboarding of ~800 to 1000 endpoints in a week and
- ▶ Integration into overall SOC environment.



Key value deliverables

- ▶ Threat intelligence based IOC detection TTPs
- ▶ Proactive threat hunting
- ▶ Forensics analysis and support
- ▶ Data gathering for SOC security incidents.
- ▶ Support Incident remediation.
- ▶ Custom signature updates based on malicious Hash values, ips etc. identified.
- ▶ SLA based incident response with monthly tracking and reporting.



Technology Landscape

- ▶ Carbon black
- ▶ Qradar



Value adds

- ▶ Automation in case management
- ▶ Custom dashboards for different functions
- ▶ Proactive ransomware symptoms identified and virtual patch rollout.

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in the U.S., UK, The Netherlands, Australia and Middle East.