

PLANNED
01:29:18
01:29:18 / 01:29:18

DOWNTIME
01:29:18
Time in Downtime
01:29:18 / 01:29:18

SETUP
01:29:18
Time in Setup
01:29:18

RUNNING
Time in Running
01:51:33
Time in Running
01:51:33 / 01:58:18

Managed Detection and Response (MDR) using CRPP Platform

For a large Retail chain with more than 200 stores in Australia and New Zealand and ~2000 stores globally ; 30000 + employees; 4GDC



Customer Objectives & challenges

- ▶ There was no centralized security monitoring.
- ▶ Multiple detection tools were deployed but was not being monitored.
- ▶ Security incident handling was a challenge
- ▶ No security Incident response process
- ▶ Wide spread network with inability to detect incidents at remote locations.
- ▶ Limitations in incident remediation support.

Phase 1

- ▶ Initial assessment of the environment – Technology & business landscape
- ▶ Right fit SIEM deployment to efficiently integrate customer estate
- ▶ Integration of primary monitoring components like, AD, Servers, endpoints, PoS terminals, firewalls, IPS and network devices.
- ▶ Initiation of security monitoring.

Phase 2

- ▶ Normalization and finetuning of event correlation.
- ▶ Built in TI based event correlation.
- ▶ Integration of network and host based APT solutions.
- ▶ Integration of network behavioral analytics
- ▶ Integration of cloud based security controls like email security, CASB etc.



Our Solution approach

Multiphase approach in centralizing security event monitoring and remediation support with our CRPP platform as the base for rollout.

Phase 3

- ▶ Integration of Anomaly based detection
- ▶ Integrations of endpoints and POS vulnerability assessments into security monitoring.
- ▶ Monitoring and incident response of APT feeds and behavioral analytics



Key value deliverables

- ▶ Centralized 24*7 security monitoring, response, and visibility.
- ▶ Integration of on prem, cloud ,SaaS environment for security monitoring.
- ▶ Artificial intelligence based detection and alerting.
- ▶ Addressed more than 400 open incidents pending on security analytics queue.
- ▶ Implementation of security incident response process.
- ▶ SLA based incident response with monthly tracking and reporting.



Value adds

- ▶ Ticketing Automation
- ▶ Automation in case management
- ▶ Customized playbooks
- ▶ Custom dashboards for different functions



Technology Landscape

- ▶ LogRhythm
- ▶ Darktrace
- ▶ FirEye
- ▶ Nexpose
- ▶ Extrahop

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.