mint Create tomorrow

IN PARTNERSHIP WITH:

Nedscaper

Protecting against today's threat landscape

BUSINESS JUSTIFICATION FOR MXDR SERVICE

Date: 4-4-2024

Version: 1.0

// SECURING CLOUDS AND GIVING BACK

Business justification for MXDR service

1. Executive Summary

In an increasingly complex threat landscape, organisations require a proactive, integrated approach for cybersecurity. The Microsoft XDR solution, brought to you by Nedscaper and Mint Technologies, provides a robust platform surpassing traditional SIEM and EDR solutions, enhancing your security posture through the following focus areas:

1.1. Prioritisation –

- Centralised Visibility: XDR consolidates security signals from endpoints, email, identities, cloud workloads, and more into a single pane of glass.
- AI-Driven Prioritisation: Machine learning models and rich threat intelligence help prioritise the most critical threats, reducing alert fatigue and enabling focused security team responses.

1.2. Hunting –

- Proactive Threat Detection: XDR goes beyond signature-based detection to uncover anomalous behaviour patterns. Security teams can proactively hunt for threats lurking within the environment.
- Cross-Domain Queries: Advanced hunting capabilities enable analysts to query data across multiple domains, uncovering the attack chain's full scope.

1.3. Investigation –

- Incident Correlation: XDR automatically links related alerts into comprehensive incidents, providing contextual information for rapid investigation.
- Deep-Dive Forensics: Analysts can drill down into detailed forensic data for root cause analysis and gain a deeper understanding of attack techniques.

1.4. Remediation –

- Automated Response Playbooks: Pre-defined and customisable playbooks allow for swift, automated response actions, reducing attack dwell time.
- Centralised Containment: Isolate infected devices, block malicious files, and reset compromised accounts from a single interface for immediate containment.

1.5. Neutralisation –

- Hardening Recommendations: XDR provides data-driven insights into vulnerabilities and recommended hardening measures to prevent future attacks, addressing the attack's root cause.
- Integrated Threat Intelligence: Continuous updates from Microsoft's vast security research arm ensure that defences are aligned with the latest threats.

2. Benefits of Microsoft XDR

- Reduced Risk: Minimise the impact of cyberattacks with earlier detection and comprehensive response.
- Increased Security Team Efficiency: Streamlined workflows, automation, and integrated intelligence free up analysts to focus on strategic tasks.
- Improved Security Posture: Proactive hunting and hardening recommendations strengthen overall security posture and resilience.

3. Closing summary

The effective licencing position of the IDC, allows the company to leverage the above mentioned services thanks to the adoption of the E5 licencing suite from Microsoft. By adopting the Microsoft XDR solution, brought to you by Nedscaper and Mint Technologies, we position our organisations to help the IDC stay ahead of evolving cyber threats, protecting critical assets and maintaining business continuity.