Cybersecurity Threat Management Standard

Version: 1.0
Effective Date: 01/02/2025
Owner: CISO
Last Reviewed: 31/12/2024

Contents

1. Background

1.1. Introduction

This Threat Management Standard is designed to safeguard PiggyCo's information assets, ensure business continuity, and uphold customer trust in our services. It reflects our commitment to robust cybersecurity practices by adhering to industry-standard frameworks such as NIST CSF and the Microsoft Cloud Security Benchmark (MCSB v1). Given our fully remote work environment and the sensitive nature of our clients' data, this standard outlines the measures, procedures, and best practices that all employees, contractors, and stakeholders must follow to protect the confidentiality, integrity, and availability of our Azure-based information systems.

1.1.1. Purpose

The purpose of the Threat Management Standard is to establish a consistent and effective approach to identifying, monitoring, and mitigating threats to PiggyCo Azure-based infrastructure and applications, This standard ensures the implementation of robust threat detection mechanisms and continuous monitoring to protect organizational assets, data, and operations against evolving cybersecurity risks.

1.1.2. Scope

This standard applies to all PiggyCo environments hosted on Azure, including virtual machines, applications, databases, storage resources, and network components. It covers threat management practices for employees, contractors, and third-party service providers.

1.1.3. Compliance

All PiggyCo personnel are required to comply to any new or updated requirements in this standard within six months of the approval date.
In addition to the provisions outlined in this standard, PiggyCo employees, contractors, and stakeholders must comply with all applicable laws and regulations related to the matters addressed herein.

2. Requirements

2.1. Logging and Monitoring Requirements

The following requirements are designed to safeguard the security and integrity of PiggyCo's systems and data by implementing comprehensive logging practices and continuous monitoring. Comprehensive security logging must be enabled across all cloud resources, applications, and services.

2.1.1. Microsoft Defender for Cloud shall be utilized for threat detection across PiggyCo's Azure services.
2.1.2. Logging must be enabled across all resource tiers, including Azure resources, operating systems, and applications within virtual machines.
2.1.3. Logs must be categorized into management/control plane and data plane activities, ensuring complete visibility into security events.
2.1.4. Activity Logs must be retained for a minimum of 12 months to support forensic investigations and compliance requirements.
2.1.5. Logging policies must be standardized across all cloud environments, and all logs must be ingested into a centralized SIEM platform.
2.1.6. Azure services must use Microsoft's default Network Time Protocol (NTP) servers unless specific PiggyCo requirements necessitate a custom NTP server.
2.1.7. Time synchronization configurations must be secured, and unauthorized modifications must be prohibited.
2.1.8. Log storage and analysis must be centralized to enable data correlation.
2.1.9. Each log source must have an assigned data owner, defined access controls, a designated storage location, processing tools, and retention requirements.

2.2. Threat Detection for Identity and Access Management (IAM)

The following requirements ensure continuous monitoring of identity and access management by detecting user and application sign-in anomalies.

2.2.1. IAM systems must be continuously monitored to detect unauthorized access, credential compromise, and privilege escalations.
2.2.2. Microsoft Entra ID logs must be collected, analyzed, and correlated with SIEM solutions to detect anomalies.
2.2.3. Authentication failures, privilege escalations, and account modifications must trigger automated alerts for security teams to investigate.
2.2.4. Multi-factor authentication (MFA) must be enforced and monitored for suspicious activities, such as excessive failed login attempts, or login attempts from high-risk locations.
2.2.5. Dormant accounts and deprecated access credentials must be identified and disabled to prevent unauthorized access.

2.3. Threat Detection and Mitigation

The following are requirements for detecting and mitigating threats to PiggyCo's cloud resources.

2.3.1. Azure resources, services, and applications must be continuously monitored for security threats and anomalies.
2.3.2. All security alerts must be analyzed, categorized, and escalated based on criticality to minimize false positives and enhance response efficiency.
2.3.3. For services that lack native security monitoring, additional threat intelligence tools must be deployed, and logs must be ingested into a SIEM solution like Microsoft Sentinel.
2.3.4. Azure Monitor Operations Suite must be used to centralize and analyze security event data.
2.3.5. Role-based access control (RBAC) must be enforced to restrict access to security logs based on the principle of least privilege.
2.3.6. SOAR playbooks shall be configured to automate response actions for security incidents

2.4. Vulnerability Management Requirements

The following are the requirements for managing vulnerabilities

2.4.1. Automated vulnerability scans and assessments must be performed on all PiggyCo's Azure cloud assets to identify potential vulnerabilities.
2.4.2. A structured process must be established and followed to promptly address and mitigate identified vulnerabilities.
2.4.3. Integrated threat intelligence feeds must be used to enhance vulnerability detection and prioritize remediation efforts based on the latest threat landscape.
2.4.4. The security posture of Azure cloud assets must be continuously monitored, and regular reports must be generated to track vulnerability management progress and compliance.

2.5. Network Logging Requirements

The following outline PiggyCo's network logging requirements to support incident investigations, threat hunting, and security alerting.

2.5.1. All network traffic must be logged and monitored for anomalies to support threat detection, forensic investigations, and compliance reporting.
2.5.2. Network Security Group (NSG) flow logs must be enabled and stored securely.
2.5.3. DNS query logs must be collected to detect potential command-and-control (C2) activities or exfiltration attempts.
2.5.4. firewalls, intrusion detection/prevention systems, and web application firewalls (WAF) must log all security events for further analysis.

2.6. Roles and Responsibilities

Chief Information Security Officer (CISO)	• Communicating this standard and its implications to senior leadership. • Facilitating the adoption of this standard.
Security Team	• Monitor and manage threat detection systems and processes. • Ensure compliance with this standard and MCSB controls.
Development Team	• Incorporate security controls into the software development lifecycle. • Implement logging and monitoring capabilities in applications.
All Employees	• Report any suspicious activities or security incidents promptly.
Third-Party Vendors	• Adhere to PiggyCo' security requirements when interacting with the organization's systems.

3. Terms and Definitions

Term	Definition
Compliance	Adherence to laws, regulations, and organizational standards, including MCSB controls.
MCSB	Microsoft Cloud Security Benchmark
NIST	National Institute of Standards and Technology
Threat	Any potential event or action that could compromise the confidentiality, integrity, or availability of PiggyCo's systems.
Vulnerability	A weakness in a system or process that could be exploited by a threat.

4. References

The MCSB serves as the primary reference for this standard, providing a comprehensive framework for securing Azure-based environments. Other references include NIST CSF and industry best practices for cloud security.

5. Approval

Approved by:	Akinjames Lincoln
Title:	CEO
Date:	February 02, 2025