Threat Monitoring Policy   
  
Introduction   
Threat monitoring is a cornerstone of Orland Fire's Information Security Management System (ISMS) to protect the organization's IT systems. By proactively monitoring, detecting, analyzing, and responding to security threats, this policy ensures the integrity, confidentiality, and availability of critical organizational systems and information.   
  
Purpose   
The purpose of this Threat Monitoring Policy is to provide clear, actionable guidance for safeguarding Orland Fire’s IT infrastructure against evolving threats. This policy establishes roles, responsibilities, operational protocols, procedures, and compliance mandates necessary for effective threat management.   
  
Scope   
This policy encompasses Orland Fire's entire IT infrastructure, including servers, workstations, network devices, and applications accessed by employees, contractors, partners, and third parties. It mandates continuous, proactive monitoring without exception, applying to local, remote, and cloud-based systems across the organization.   
  
Background   
Prescient Solutions conducted an assessment of Orland Fire’s IT environment, identifying vulnerabilities and providing recommendations incorporated herein. This policy aims to align the organization with international security standards such as ISO 27001, HIPAA, and PCI DSS, while addressing identified risks comprehensively.   
  
Policy Statement   
Orland Fire commits to implementing and maintaining a robust Threat Monitoring framework grounded in international security standards. By employing a combination of advanced tools, systems, personnel training, and procedural guidelines, the organization aims to ensure readiness against all forms of cyber threats.   
  
Roles and Responsibilities   
  
Administrators:   
- Conduct daily log reviews of SYSLOG servers, escalating flagged incidents exceeding Medium Severity within 1 business day.   
- Configure and manage IDS/IPS systems to ensure optimal performance and continuous operations.   
  
IT Security Team:   
- Establish and enforce policies surrounding password complexity, account lockout mechanisms, and privileges.   
- Lead response coordination for detected threats based on the incident severity matrix.   
  
Network Engineers:   
- Create monthly updated network diagrams reflecting all devices and pathways.   
- Implement redundancy and failover mechanisms across critical network segments.   
- Regularly patch and update firmware, prioritizing vulnerabilities flagged during security assessments.   
  
Prescient Solutions:   
- Conduct periodic cybersecurity audits and evaluations, ensuring third-party oversight of threat monitoring capabilities.   
  
Orland Fire IT Department:   
- Execute enhancements to security protocols and systems based on the periodic reviews and assessments conducted.   
  
Policy Details   
  
Existing Practices and Tools   
Orland Fire’s IT Security utilizes the following tools:   
- Nessus Vulnerability Scanner for pinpointing OS and software vulnerabilities.   
- Rapidfire Tools Network Detective for network mapping and device characterization.   
- Wireshark Packet Analyzer for high-level real-time traffic analysis.   
- Microsoft Baseline Security Analyzer for system verification against industry recommendations.   
  
Logging and Monitoring   
- SYSLOG servers must be deployed within 30 business days post-policy adoption for centralized log aggregation. Logs must be retained securely for a minimum of 12 months for compliance purposes.   
- IDS/IPS systems, using Next-Generation Firewall (NGFW) technology, must be deployed organization-wide within six months. These systems must alert administrators in real time for any detected threats.   
  
Controls Implemented   
  
Access Controls:   
- Use encrypted password vaults for credential management to prevent unauthorized data access.   
- Implementation of Multi-Factor Authentication (MFA) across all accounts within 60 calendar days.   
  
Patch Management:   
- Patches flagged as “Critical” must be applied within 48 hours. A weekly review schedule ensures timely application for other updates.   
  
Vulnerability Categorization   
Orland Fire classifies vulnerabilities into:   
- High Severity: Must be mitigated within 24 hours due to impact on system integrity and operational continuity.   
- Medium Severity: Must be resolved within 7 calendar days due to moderate risks flagged.   
- Low Severity: Addressed based on priority during regular patch cycles.   
  
Implementation Process   
  
Step 1: Deploy SYSLOG servers as required for centralized logging. Secure configurations must meet encryption standards.   
Step 2: Equip IDS/IPS systems capable of dynamic threat detection and immediate escalation. Placement must include all internal and external network boundary segments.   
Step 3: Conduct vulnerability assessments monthly using Nessus to ensure early detection of weaknesses.   
Step 4: Enforce robust MFA policies and block old reuse passwords immediately.   
  
Incident Response Procedures   
1. High-severity incidents must be escalated to the Incident Response Lead within 2 hours.   
2. Security teams must initiate immediate mitigation, forensic analysis, and documentation within 24 hours.   
3. Compliance alignment must be verified within tracking files for post-incident review logs.   
  
Recommendations   
  
Enhancing the Threat Monitoring Scope:   
- Adopt Zero Trust Architecture (ZTA) principles to dynamically verify all internal and external endpoints.   
- Mandate quarterly phishing resistance training for all employees and prepare annual readiness scorecards.   
  
Compliance Standards   
All controls adhere to the compliance mandates set forth under ISO 27001, HIPAA, CIS Controls, and PCI DSS. The IT Department will conduct annual audits verifying adherence to these standards.   
  
References and Appendices   
- Annex A: Tool Configuration Instructions (Nessus, Wireshark, Rapidfire Tools).   
- Annex B: Incident Management Protocol Framework.   
  
By adopting this Threat Monitoring Policy, Orland Fire ensures compliance with international standards while proactively fortifying defenses against evolving cyber threats.