**Technical Incident Response Policy for Gotham Ltd.: Malicious Packet Threshold**

**Policy 1.1.** **Definition of Malicious Packets:** Malicious packets are data packets involved in unauthorized access attempts or attacks such as viruses, worms, DDoS (Distributed Denial of Service) attacks, and other forms of cyber threats.

**Policy 1.2. Threshold for Red Alert:** malicious packets shall not exceed 20% of the total network traffic at the Gotham factory, a red alert will be triggered to indicate a potential security intrusion.

**Policy 1.3. Calculation and Monitoring:** The threshold is calculated based on real-time network traffic analysis. The system should continuously monitor network traffic and check for malicious packets in defined time intervals (e.g., every 5 minutes).

**Policy 1.4. Response Protocol:**

Upon detection of malicious packets reaching the 20% threshold, the IT unit shall do the following:

**Policy 1.4.1. Automated Responses:** Implement automated measures such as blocking suspicious IP addresses, isolating affected segments of the network, and logging detailed information for further analysis.

**Policy 1.4.2. Notifications:** Immediately notify the cybersecurity team for investigation and mitigation.

**Policy 1.5. False Positives Mitigation:**

Incorporate additional checks to distinguish between malicious traffic and legitimate spikes in traffic.

Use machine learning algorithms to adapt detection thresholds based on historical data and network behavior patterns.

**Policy 1.6.** **Integration with Existing Security Measures:**

Ensure that the 20% threshold works alongside other security measures like firewalls, intrusion prevention systems (IPS), and endpoint protection solutions.

Coordinate with these systems for a layered defense approach.

**Policy 2.1. Categorization of Malicious Packets:**

Categorize malicious packets into types (e.g., DDoS traffic, phishing attempts) to enhance detection accuracy and response strategies.

**Policy 2.2.** **Alignment with Industry Standards:**

Review and align the policy with industry standards and best practices for cybersecurity to ensure effectiveness and recognition by security professionals.

**Policy 2.3 Tools and Technologies:**

Ensure that existing tools and technologies are capable of detecting, quantifying, and categorizing malicious packets.

**Policy 2.3.1.** All communication traffic shall be established using encryption technology e.g. TLS (transport layer security).

**Policy 2.3.2**. IT unit shall be responsible to maintain TLS communication and prevent it from broken.

**Policy 2.3.3.** Consider upgrading or adding new systems if necessary to meet these technology requirements.