Cybersecurity Threat Report

Generated: 2025-07-28 14:02:14
Business Context: i run an online clothing business

Summary of Findings

Here's a summary of the suspicious activities detected in your system logs:

1. **Suspicious User-Agent Activity**:
- Several IP addresses (192.168.0.6, 192.168.0.7, 192.168.1.2, 192.168.1.3, 192.168.1.4, 192.168.2.2, 192.168.3.1, 192.168.3.2, 192.168.3.5) have been flagged for using a "Suspicious User-Agent." This means that the way these users are accessing your website is unusual and could indicate automated tools or bots trying to find vulnerabilities.
- These activities targeted various sensitive paths like '/admin', '/login.php', '/wp-admin', '/admin/config', '/.env', '/private', and '/config.php'.

2. **Path Traversal Attempt**:
- The IP address 192.168.0.8 attempted a "Path Traversal" attack by trying to access a file path ('/../../../etc/passwd') that should be off-limits. This is a technique used to access restricted files on your server.

3. **SQL Injection Attempts**:
- Two IP addresses (192.168.0.9 and 192.168.3.3) attempted "SQL Injection" attacks. This involves inserting malicious code into your website's search function to try and manipulate your database.

Risk Assessment:
- **Suspicious User-Agent Activity**: Medium Risk. While not all suspicious user-agent activities are harmful, they can indicate probing for weaknesses.
- **Path Traversal Attempt**: High Risk. This is a direct attempt to access sensitive files and could lead to data breaches.
- **SQL Injection Attempts**: High Risk. These are serious attempts to manipulate your database and can lead to data theft or corruption.

Next Steps:
1. **Block IP Addresses**: Consider blocking the IP addresses involved in high-risk activities (192.168.0.8, 192.168.0.9, 192.168.3.3) to prevent further attempts.
2. **Monitor and Review**: Keep an eye on the IPs involved in medium-risk activities. If they continue to show suspicious behavior, consider blocking them as well.
3. **Strengthen Security**: Ensure your website and database are up-to-date with the latest security patches. Consider consulting with an IT professional to review your security settings.
4. **Reassurance**: While these activities are concerning, taking the above steps can help protect your business. It's good that these attempts were detected, allowing you to take action.

Remember, staying vigilant and proactive is key to maintaining your business's cybersecurity.

Type	IP	Reason	Path
web_attack	192.168.0.6	Suspicious User-Agent	/admin
web_attack	192.168.0.7	Suspicious User-Agent	/login.php
web_attack	192.168.0.8	Path Traversal	/../../../etc/passwd
web_attack	192.168.0.9	SQL Injection	/search.php?q=test' OR '1'='1
web_attack	192.168.1.2	Suspicious User-Agent	/wp-admin
web_attack	192.168.1.3	Suspicious User-Agent	/admin/config