TITLE: SOC Fundamentals and Operations

Executive Summary

On August 18, 2025, our detection systems identified an attempted exploitation of the VSFTPD 2.3.4 backdoor vulnerability on an internal Linux VM. The attacker IP (192.168.1.100) triggered high-severity alerts in Wazuh corresponding to MITRE ATT&CK Technique T1190 (Exploit Public-Facing Application). The SOC team executed containment by isolating the affected VM and applying network-level IP blocking via CrowdSec. No evidence of persistence or data exfiltration was found.

Timestamp	Action / Observation
2025-08-18 11:00:00	Wazuh alerts triggered: suspicious FTP connection attempts with payload signature matching Metasploit's vsftpd_234_backdoor exploit. Alert ID: 20250818-WZS-FTPD-EXP001
2025-08-18 11:01:30	Alert analysis initiated; payload confirmed as exploit attempt targeting vsftpd backdoor vulnerability (CVE-2011-2523).
2025-08-18 11:05:00	Isolation of VM "Server-X" executed via segmentation on network VLAN to block outbound traffic and prevent lateral movement.
2025-08-18 11:07:00	CrowdSec rules updated to block source IP 192.168.1.100 across perimeter firewalls and internal IDS.
2025-08-18 11:10:00	Ping and TCP connection tests confirmed attacker IP connectivity blocked successfully.
2025-08-18 11:15:00	Comprehensive log collection initiated (Wazuh, system logs, FTP logs) and memory dump acquired for forensic analysis.

Detailed Timeline and Technical Actions

Technical Findings

- **Exploit Details:** The attack exploited a known backdoor present in vsftpd 2.3.4, allowing remote code execution and a potential shell backdoor.
- **Alert Signatures:** Multiple Wazuh rules matched on FTP control commands containing non-standard payloads typical of vsftpd_234_backdoor exploit attempts.
- **IOC Validation:** Source IP 192.168.1.100 correlated with threat intelligence feeds from AlienVault OTX as a known hostile actor conducting brute-force and exploit attempts.

- **Containment Effectiveness:** Network isolation and IP blocking prevented successful exploit execution.
- **Evidence Captured:** Volatile data (memory dump), netstat outputs, and logs were collected with integrity hashes to preserve forensic chain-of-custody.

Remediation Steps

1. **Patch Deployment:** Immediate recommendation to upgrade vsftpd instances to versions > 3.x where the backdoor is patched.
2. **Firewall and IDS Updates:** Enforce stricter FTP inspection and anomaly detection rules to detect similar exploit payloads.
3. **Harden Network Segmentation:** Segment critical systems to limit exposure in case of lateral movement attempts.
4. **Routine Threat Intel Integration:** Update CrowdSec and Wazuh signatures regularly based on latest public CVEs and threat intelligence.
5. **Continuous Monitoring:** Maintain vigilant alert monitoring and proactive triage workflows.

Conclusion and Recommendations

This incident demonstrates the criticality of patch management and the importance of integrated detection and automated response tools to mitigate exploitation of legacy vulnerabilities. While the exploit was successfully blocked prior to compromise, the incident reaffirms the need for continuous threat hunting and network defense hardening.

END OF TASK