50 DFIR detections tailored to uncover suspicious activities, cybersecurity threats, and potential data exfiltration, focusing on elements relevant to Digital Forensics and Incident Response (DFIR).

DFIR Detection Rules

1. **Unauthorized Privilege Escalation**
   Detects unexpected changes in user privileges that could indicate compromised accounts or insider threats.
2. **Suspicious Remote Access**
   Flags remote access from unusual IP addresses, particularly those originating from high-risk locations.
3. **Multiple Failed Login Attempts**
   Identifies repeated failed logins, which may indicate brute-force attacks.
4. **Unusual File Access Patterns**
   Flags access to sensitive files outside of typical work hours or by unauthorized users.
5. **New User Accounts with Admin Privileges**
   Detects newly created admin accounts, which could be used to establish persistent access.
6. **Use of Known Malware or Exploit Tools**
   Flags activity associated with known malicious software or tools frequently used in cyber attacks.
7. **Abnormal Network Traffic Volume**
   Detects large spikes in network traffic that may indicate data exfiltration or DDoS attacks.
8. **Outbound Connections to Suspicious IPs**
   Flags outgoing connections to IPs associated with command-and-control (C2) servers.
9. **Anomalous Geo-Location Activity**
   Identifies logins or activity originating from unexpected countries or regions.

10. **Use of Encryption Tools**
    Detects the use of encryption tools or processes, potentially signaling data obfuscation.
11. **Unexpected Changes to System Configurations**
    Flags configuration changes that could weaken security, such as disabling firewalls or antivirus software.
12. **Repeated Access to High-Risk Data Stores**
    Identifies repeated access attempts to databases containing sensitive information.
13. **Unusual File Modification Activity**
    Flags file modifications that deviate from typical user behavior.
14. **Suspicious VPN Usage**
    Detects VPN usage patterns indicative of an attempt to conceal login locations.
15. **High Volume of Small Transactions**
    Flags multiple small transactions that may be attempts to evade detection.
16. **Data Transfer to External Storage Devices**
    Identifies large data transfers to USB or other external devices.
17. **Use of Tor or Proxy Services**
    Detects connections to Tor networks or proxies, often used to hide identity.
18. **Anomalous File Downloads from the Internet**
    Flags downloads of files from suspicious or blacklisted websites.
19. **Rogue DHCP Servers**
    Detects unauthorized DHCP servers, which could be used to intercept network traffic.
20. **New Port Forwarding Rules Established**
    Identifies new port forwarding rules, potentially enabling external access.
21. **Installation of Suspicious Software**
    Flags installation of software linked to cyber threats or known vulnerabilities.
22. **Use of Password Cracking Tools**
    Detects the execution of known password-cracking tools.
23. **Unauthorized Software Uninstallations**
    Flags removal of security or monitoring tools from systems.
24. **High-Entropy File Transfers**
    Identifies files with high entropy, often indicating encryption or obfuscation.
25. **Multiple User Accounts Logging in from the Same IP**
    Flags instances of multiple accounts accessing the network from a single IP.
26. **Unauthorized Access to Backup Files**
    Detects unauthorized access to backup or recovery files.
27. **Suspicious Use of Remote Desktop Protocol (RDP)**
    Flags unusual RDP sessions, often linked to remote attacks.
28. **Executable Files in Non-Standard Directories**
    Identifies executables stored in unusual locations, which may be an attempt to bypass detection.

29. **Excessive User Account Creation**
    Detects high volumes of new account creation, potentially for establishing persistence.
30. **Suspicious Script Execution**
    Flags unusual or malicious script executions on critical systems.
31. **High-Frequency Firewall Log Drops**
    Identifies repeated drops in firewall logs, indicating potential DDoS or intrusion attempts.
32. **Unusual Use of System Utilities**
    Detects unusual use of tools like PowerShell or Command Prompt, often linked to lateral movement.
33. **Suspicious DNS Requests**
    Flags DNS requests for known malicious domains or domains associated with tunneling.
34. **Use of Remote File Transfer Protocols (FTP, SFTP)**
    Detects unexpected use of FTP/SFTP, which may be used for data exfiltration.
35. **Creation of Unauthorized Shares**
    Identifies unauthorized network shares, often used for lateral movement or data theft.
36. **Unexpected Changes to Registry Keys**
    Flags changes to critical registry settings, potentially indicating malware persistence.
37. **Suspicious Email Activity with Attachments**
    Detects unusual email patterns, especially those involving attachments linked to malware.
38. **Unauthorized Access to System Logs**
    Flags attempts to access or modify system logs, which may indicate attempts to cover tracks.
39. **Abnormal Outbound Traffic Volume on Non-Standard Ports**
    Detects high volumes of traffic on ports not typically used, a sign of exfiltration.
40. **Suspicious Cloud Storage Activity**
    Flags unusual activity in cloud storage accounts, potentially indicating data theft.
41. **Suspicious Use of SSH or Telnet**
    Detects SSH or Telnet use that deviates from typical patterns, often linked to remote access.
42. **Excessive Password Reset Requests**
    Identifies a high frequency of password reset attempts, possibly indicative of account compromise.
43. **Repeated Access to Administrative Shares**
    Flags repeated attempts to access administrative shares without proper authorization.
44. **Hidden or Suspicious Scheduled Tasks**
    Detects creation of hidden or unusual scheduled tasks, often used for persistence.
45. **Unauthorized Application of Security Group Policies**
    Flags changes to security policies that could weaken system defenses.
46. **Data Exfiltration via DNS Tunneling**
    Identifies data exfiltration attempts using DNS tunneling techniques.

47. **Unusual Browser History Patterns**
    Detects suspicious browsing behavior, such as frequent access to blacklisted sites.
48. **Unexpected System Reboots or Shutdowns**
    Flags unexpected reboots, which could indicate malware or remote manipulation.
49. **Suspicious Use of Windows Management Instrumentation (WMI)**
    Detects WMI usage for unusual purposes, a technique often used by advanced persistent threats.
50. **Repeated Access to Financial Systems Outside Business Hours**
    Flags attempts to access financial applications or databases during non-business hours, potentially indicating unauthorized access.