

FortiSIEM Rules Diff 7.5.0-7.5.1

Rules Added

- Google Threat Intel: Malware Hash found in Mail
- Google Threat Intel: Ransomware Hash found in Mail
- MS Defender XDR: High Severity Collection Alert
- MS Defender XDR: High Severity Command and Control Alert
- MS Defender XDR: High Severity Credential Access Alert
- MS Defender XDR: High Severity Defense Evasion Alert
- MS Defender XDR: High Severity Discovery Alert
- MS Defender XDR: High Severity Execution Alert
- MS Defender XDR: High Severity Exfiltration Alert
- MS Defender XDR: High Severity Impact Alert
- MS Defender XDR: High Severity Incident Detected
- MS Defender XDR: High Severity Initial Access Alert
- MS Defender XDR: High Severity Lateral Movement Alert
- MS Defender XDR: High Severity Malware Alert
- MS Defender XDR: High Severity Persistence Alert
- MS Defender XDR: High Severity Privilege Escalation Alert
- MS Defender XDR: High Severity Reconnaissance Alert
- MS Defender XDR: High Severity Resource Development Alert
- MS Defender XDR: Medium Severity Collection Alert
- MS Defender XDR: Medium Severity Command and Control Alert
- MS Defender XDR: Medium Severity Credential Access Alert
- MS Defender XDR: Medium Severity Defense Evasion Alert
- MS Defender XDR: Medium Severity Discovery Alert
- MS Defender XDR: Medium Severity Execution Alert
- MS Defender XDR: Medium Severity Exfiltration Alert
- MS Defender XDR: Medium Severity Impact Alert
- MS Defender XDR: Medium Severity Incident Detected
- MS Defender XDR: Medium Severity Initial Access Alert
- MS Defender XDR: Medium Severity Lateral Movement Alert
- MS Defender XDR: Medium Severity Malware Alert
- MS Defender XDR: Medium Severity Persistence Alert
- MS Defender XDR: Medium Severity Privilege Escalation Alert
- MS Defender XDR: Medium Severity Reconnaissance Alert
- MS Defender XDR: Medium Severity Resource Development Alert
- Outbreak: Cisco ASA and FTD Firewall RCE Detected on Network
- Outbreak: Interlock Ransomware Attack Detected on Host
- Outbreak: Interlock Ransomware Attack Detected on Network
- Outbreak: React2Shell Remote Code Execution Detected on Network

- Outbreak: SmarterTools SmarterMail RCE Detected on Network
- Outbreak: UNC1549 Critical Infrastructure Espionage Attack Detected on Network
- Outbreak: Versa Concerto SD-WAN Authentication Bypass Detected on Network
- Outbreak: Zimbra Collaboration Local File Inclusion Detected on Network
- Permitted Traffic from Anyrun Malware Domain List
- Permitted Traffic from Anyrun Malware IP List
- Permitted Traffic from GTI Malware Domain List
- Permitted Traffic from GTI Malware IP List
- Traffic to Anyrun Malware Domain List
- Traffic to Anyrun Malware IP List
- Traffic to Anyrun Malware URL List
- Traffic to GTI Malware Domain List
- Traffic to GTI Malware IP List
- Traffic to GTI Malware URL List
- Veeam: Backup Storage or Repository Disconnected
- Veeam: Brute Force MFA Logon Attempts Detected
- Veeam: Critical Infrastructure Component Removed
- Veeam: Global Multi-Factor Authentication Disabled
- Veeam: High Severity Job Failure or Service Outage Detected
- Veeam: License or Resource Quota Capacity Warning Detected
- Veeam: Medium Severity Configuration Change Detected
- Veeam: MFA for Specific User Disabled
- Veeam: Multi-Double Authorization Disabled
- Veeam: Ransomware Activity Detected
- Veeam: Security Exclusion or Policy Modification Detected
- Veeam: Storage or Storage Object Deleted
- Windows Logging Service Shutdown Without Restart
- Windows: Potential Pass the Hash Attack
- Windows: System Halted because of Failure to Record Security Log

Rules Deleted

- MS 365 Defender: Exploit Detected
- MS 365 Defender: High Severity Generic Alert
- MS 365 Defender: High Severity Generic Incident Triggered
- MS 365 Defender: High Severity Ingress Tool Transfer Alert
- MS 365 Defender: High Severity LSASS Memory - Credential Access Alert
- MS 365 Defender: High Severity Masquerading - Execution Alert
- MS 365 Defender: High Severity OS Credential Dumping - Suspicious Activity Alert
- MS 365 Defender: High Severity Process Injection - Defense Evasion Alert
- MS 365 Defender: High Severity Suspicious PowerShell command line Execution Alert
- MS 365 Defender: High Severity Suspicious Process Discovery - Discovery Alert

- MS 365 Defender: High Severity Suspicious Task Scheduler activity - Persistence Alert
- MS 365 Defender: High Severity System Network Configuration Discovery - Discovery Alert
- MS 365 Defender: High Severity System Service Discovery - Discovery Alert
- MS 365 Defender: Malware Detected
- MS 365 Defender: Medium Severity Generic Alert
- MS 365 Defender: Medium Severity Generic Incident Triggered
- MS 365 Defender: Medium Severity Ingress Tool Transfer Alert
- MS 365 Defender: Medium Severity LSASS Memory - Credential Access Alert
- MS 365 Defender: Medium Severity Masquerading - Execution Alert
- MS 365 Defender: Medium Severity OS Credential Dumping - Suspicious Activity Alert
- MS 365 Defender: Medium Severity Process Injection - Defense Evasion Alert
- MS 365 Defender: Medium Severity Suspicious PowerShell command line Execution Alert
- MS 365 Defender: Medium Severity Suspicious Process Discovery - Discovery Alert
- MS 365 Defender: Medium Severity Suspicious Task Scheduler activity - Persistence Alert
- MS 365 Defender: Medium Severity System Network Configuration Discovery - Discovery Alert
- MS 365 Defender: Medium Severity System Service Discovery - Discovery Alert
- MS 365 Defender: Persistence Detected
- MS 365 Defender: Suspicious Activity Detected
- MS 365 Defender: Unwanted Software Detected
- Unregistered EMC Clariion Host
- Windows: CrashOnAuditFail Value is set to Continue
- Windows: CrashOnAuditFail Value is set to Halt
- Windows: Outgoing Logon with New Credentials
- Windows: Pass the Hash Activity 2

Rules Renamed

- Cisco Email Security: Excessive Emails Detected from a Awful Domain -> Cisco Email Security: Excessive Emails Detected from a Untrusted Domain
- Cisco Email Security: Excessive Emails Detected from a Poor Domain -> Cisco Email Security: Excessive Emails Detected from a Questionable Domain
- Cisco Email Security: Mail Permitted From a Awful Domain Reputation -> Cisco Email Security: Mail Permitted from a Untrusted Domain
- Cisco Email Security: Mail Permitted From a Poor Domain Reputation -> Cisco Email Security: Mail Permitted from a Questionable Domain
- Windows: Access to ADMIN\$ Share -> Windows: Access to ADMIN Share

- Windows: New or Renamed User Account with \$ in Attribute SamAccountName -> Windows: New or Renamed User Account with dollar sign in Attribute SamAccountName
- Windows: Successful Overpass the Hash Attempt -> Windows: NewCredentials Logon via Secondary Logon Service
- Windows: System Halted because of Failure to Record Security Log -> Windows: CrashOnAuditFail Value is set to Continue