Intel Security SIEM – *Content Packs*

Authored by

Nishant Ranjan
Enterprise Technology Architect – APAC

Contents

1. Content Packs – Overview 5
   1.1. Benefits 5
2. Authentication Content Pack 6
   2.1. Views: 6
3. Case Management Content Pack 6
   3.1. Views: 7
   3.2. Reports: 7
4. Database Content Pack 7
   4.1. Views: 8
   4.2. Correlation Rules: 9
   4.3. Reports: 9
5. DNS Content Pack 10
   5.1. Alarms: 10
   5.2. Correlation Rules: 10
   5.3. Views: 11
   5.4. Reports: 11
6. Domain Policy Content Pack 11
   6.1. Alarms: 12
   6.2. Correlation Rules: 13
   6.3. Reports: 13
   6.4. Views: 13
   6.5. Watchlists: 13
7. DoS Content Pack 13
   7.1. Alarms: 14
   7.2. Correlation Rules: 14
   7.3. Reports: 15
   7.4. Views: 15
8. Exploit Content Pack 15
   8.1. Alarms: ..... **Error! Bookmark not defined.**
   8.2. Correlation Rules: 16
   8.3. Reports: 16

8.4. Views: 16
8.5. Watchlists: **Error! Bookmark not defined.**
9. Executive Content Pack 16
9.1. Reports: 17
9.2. Views: 17
10. Exploit Content Pack 20
10.1. Alarms: 20
10.2. Correlation Rules: 20
10.3. Reports: 21
10.4. Views: 21
10.5. Watchlists: 21
11. Firewall Content Pack 21
11.1. Alarms: 22
11.2. Correlation Rules: 22
11.3. Views: 22
11.4. Reports: 23
12. Malware Content Pack 24
12.1. Alarms: 25
12.2. Correlation Rules: 26
13. Reports: 26
13.1. Views: 26
14. Operation SMN Content Pack 26
14.1. Correlation Rules: 27
14.2. Watchlists: 27
15. Reconnaissance Content Pack 27
15.1. Alarms: 28
15.2. Correlation Rules: 28
15.3. Reports: 30
15.4. Views: 30
15.5. Watchlists: 31
16. Wireless Access Point Content Pack 32
16.1. Reports: 33

16.2. Views: 33
17. Web Filtering and Web Application Control Content Pack 34
17.1. Correlation Rules: 35
17.2. Views: 35
17.3. Reports: 36
18. Windows Authentication Content Pack 36
18.1. Correlation Rules: 37
18.2. Views: 37

1. Content Packs – Overview

When a specific threat situation occurs, you can respond immediately by importing and installing the relevant content pack from the rules server. Content packs contain use-case driven correlation rules, alarms, views, reports, variables, and watchlists to address specific incident or threat activity. Content packs enable you to respond to threats without wasting time creating tools from scratch.

Requirements

Content packs shall be downloaded from the Rules Server to the ESM.

The ESM shall provide group and/or user privileges to limit access to content pack management.

Users, with proper privileges, shall be allowed to view, install, and uninstall content packs.

Content packs may include

- Views
- Reports
- Rules
- Correlation
- Data Source
- Policy
- Others
- Watch Lists
- Alarms
- Variables
- Policies

1.1.Benefits

- Start generating meaningful and relevant reports, Dashboard views from Day1
- Reduces time to create custom and relevant content such as – Correlations Rules, Dashboard Views, Reports, Watchlists etc
- Improves Operational Efficiency
- Reduces time to value after installation thus improving ROI in shorter time period

2. Authentication Content Pack

Normalization Category:

- Authentication > Login

Use this content pack to:

- Monitor authentication events.
- View failed and successful logons, as well as specific administrator logons.
- Track system default privileged user names.

After you install this content pack:

- Change view filters to meet your organization's specific requriements.
- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

2.1.Views:

- Authentication Content Pack Views (Folder)
  - Administrator Login Overview
  - Detailed Administrator Logins
  - Failed Host Logins
  - Failed Service Logins
  - Successful Host Logins
  - Successful Service Logins

3. Case Management Content Pack

Use this content pack to:

- Monitor Case Management cases.
- View Open or closed cases.
- Track different users that are working on cases and the status of changes.

- View cases that have been created.

After you install this content pack:

- This Content Pack is only beneficial if using the Case Management system of the ESM.

- The system defaults with 'Open' and 'Closed' as a status. If you create another case status, such as 'On Hold' in order to see the status, applicable reports would need to have the filter adjusted by having the new status added. If you choose a different name, change the report case status filter to the name chosen.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

3.1. Views:

- Case Management Content Pack Views (Folder)

  - Case Management Summary

3.2. Reports:

- Case Management - Closed Monthly Report

- Case Management - Created Monthly Report

- Case Management - Daily Report

- Case Management - Open Monthly Report

- Case Management - Summary Report

References:

- See KnowledgeBase article KB85199 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB85199)

4. Database Content Pack

Normalization Categories:

- Application > Database

- Authentication > Login

Use this content pack to:

- Monitor database authentication events.

- Monitor successful and potential database exploit activity.

- Monitor SQL events by language type.

- Monitor general database events.

Before you install this content pack:

- Ensure that the CORP_GEOS variable includes all trusted company geolocations.

- Ensure that the DB_SERVERS variable includes all database servers.

After you install this content pack:

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- Change report templates to run at specified times, to e-mail specific recipients, and to save to remote locations automatically.

- Change report layouts to include additional data or to change the look of the report.

- Existing standard rules are included in this content pack. To avoid duplicate events, please disable the following rules:

47-4000091, 47-4000093, 47-4000094, 47-4000095, 47-4000135, 47-4000146.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

4.1.Views:

- Database Content Pack Views (Folder)

  - Database Events by Language Type

  - Database Events by Subtype

  - Database Exploit Activity

- Failed Database Logons

- Successful Database Logins

4.2.Correlation Rules:

- Database - Activity Outside Company Geolocation

- Database - Attempted Database Configuration Change by a Remote Host

- Database - Bulk Data Transfer after Exploit Activity

- Database - Database Event Activity after Exploit Activity

- Database - Excessive Database Connections From a Single Source

- Database - Possible Exploit Activity

- Database - Increased Number of DCL Events

- Database - Increased Number of DDL Events

- Database - Increased Number of DML Events

- Database - Increased Number of TCL Events

- Database - Multiple Database Access Attempt Failures

- Database - Multiple Audit Trail Modifications

- Database - Possible SQL Injection Activity - Low Severity Queries

- Database - Possible SQL Injection Activity - Query Failure by Destination User

- Database - Possible SQL Injection Activity - Query Failure by Source IP

- Database - Source User Logon Different From Destination User Logon

4.3.Reports:

- Database - Database Events

  - Database - Database Events (Report Layout)

- Database - Database Logon Events

  - Database - Logon Event Summary (Report Layout)

References:

- See KnowledgeBase article KB85251 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB85251)

5. DNS Content Pack

Use this content pack to:

- Monitor DNS activity.

- Assist in detecting, monitoring, and preventing attacks or other unwanted DNS traffic.

Before you install this content pack:

- Your organization must have McAfee Global Threat Intelligence (GTI) to use some of the correlation rules in this content pack.

- Insure that Watchlists are enabled to use some of the correlation rules in this content pack.

- Change default values of the DNS_CHANGER_IPS and DNS_SERVERS variables for included components to function correctly.

After you install this content pack:

- Configure alarms to send notifications and take automated actions.

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Adjust variables to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- Existing standard rules are included in this content pack. To avoid duplicate events, please disable the following rules:

47-4000057, 47-4000076, 47-4000129, 47-4000131, 47-4000142, 47-4000154, 47-4000181, 47-4000191.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

5.1.Alarms:

- DNS - DNS Changer IP Activity

5.2.Correlation Rules:

- DNS - Communication with Malicious Host - Event or Flow

- DNS - DNS Changer Activity - Event or Flow
- DNS - GTI Communication with Malicious Host - Event or Flow
- DNS - Local Host Communicating with External DNS Server - Flow
- DNS - Multiple NXDomain Events
- DNS - Multiple Recon Events from a Local Host
- DNS - Multiple Recon Events from a Remote Host
- DNS - Possible DNS Amplification Attack
- DNS - Possible DNS connection or Unauthorized DNS server
- DNS - Traffic with a Passive DNS known Malware Domain

5.3. Views:

- DNS Content Pack Views (Folder)
  - DNS NXDOMAIN View
  - DNS Query View

5.4. Reports:

- DNS - DNS Traffic
  - DNS - DNS Traffic Report Layout (Report Layout)

References:

- See KnowledgeBase article KB85375 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB85375)

6. Domain Policy Content Pack

Applicable Device Types:

- Microsoft Windows

Use this content pack to:

- Track changes related to Microsoft Windows policy in your environment.

Before you install this content pack:

- Review your current audit logging settings for Active Directory (AD).

- Adjust the audit logging settings to align with the correlation rules in the content pack.

- Set the variable HOME_NET to a value that matches your internal network.

- Some of the views and correlation rules require "Audit account management" and "Audit object access" to be enabled at either the domain or local level.

- Some of the views and correlation rules require "Audit Directory Service Changes" to be enabled. More information can be found here http://blogs.msdn.com/b/canberrapfe/archive/2012/05/02/auditing-group-policy-changes.aspx.

After you install this content pack:

- Adjust the content pack components to meet your organization's specific requirements.

- Configure alarms to send notifications and take automated actions.

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Change report templates to run at specified times, to e-mail specific recipients, and to save to remote locations automatically.

- Change report layouts to include additional data or to change the look of the report.

- Adjust static watchlists to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

6.1.Alarms:

- Domain Policy - Suspect domain changes

- Domain Policy - Suspect local changes

6.2.Correlation Rules:

- Domain Policy - Domain policy changed
- Domain Policy - Group policy object deleted
- Domain Policy - Group policy object created
- Domain Policy - Group policy object modified
- Domain Policy - Suspicious domain privilege changes
- Domain Policy - Suspicious local privilege changes
- Domain Policy - User added to domain security group
- Domain Policy - User added to local security group
- Domain Policy - User removed from domain security group
- Domain Policy - User removed from local security group

6.3.Reports:

- Domain Policy - Weekly policy overview

6.4.Views:

- Domain Policy Content Pack views (Folder)
  - Domain security group changes
  - GPO changes by user
  - Local security group changes Dest SID
  - Local security group changes Dest User

6.5.Watchlists:

- Domain Policy - Security Groups

References:

- See KnowledgeBase article KB84501 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB84501)

7. DoS Content Pack

Normalization Categories:

- DoS

- DoS > Protocol DoS

Use this content pack to:

- Monitor DoS events.

- Monitor behavior of DoS events to determine first attack.

Before you install this content pack:

- Ensure that the CORP_GEOS variable includes all trusted company geolocations.

After you install this content pack:

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- Existing standard rules are included in this content pack. To avoid duplicate events, please disable the following rules:

47-4000028, 47-4000125, 47-4000160, 47-4000161, 47-4000162, 47-4000163

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

7.1.Alarms:

- DoS - Attempts on Network

7.2.Correlation Rules:

- DoS - Network DoS Activity Detected

- DoS - Possible DDoS Against Single Host - ICMP - Flow

- DoS - Possible DDoS Against Single Host - Other - Flow

- DoS - Possible DDoS Against Single Host - TCP - Flow

- DoS - Possible DDoS Against Single Host - UDP - Flow

- DoS - Successful Logon After DoS Activity

7.3.Reports:

- DoS - DoS Activity Analysis

7.4.Views:

- DoS Content Pack Views (Folder)
  - All DoS Events
  - DoS Events by Protocol Used

References:

- See KnowledgeBase article KB85303 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB85303)

8. Email Content Pack

Applicable Device Types:

- Email

Use this content pack to:

- Monitor email traffic coming in and out of your organization's network.

Before you install this content pack:

- Your organization must have McAfee Global Threat Intelligence (GTI) to use some of the correlation rules in this content pack.
- Set the variable HOME_NET to a value that matches your internal network.

After you install this content pack:

- Adjust the content pack components to meet your organization's specific requirements.
- Adjust correlation rule parameters to meet your organization's specific requirements.
- Change report templates to run at specified times, to e-mail specific recipients, and to save to remote locations automatically.
- Change report layouts to include additional data or to change the look of the report.
- Change view filters to meet your organization's specific requirements.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

8.1. Correlation Rules:

- Email - Email Device Communicating with GTI Address
- Email - Abnormal Email Traffic From GTI Address
- Email - Abnormal Volumes of Outbound Email

8.2. Reports:

- Email - Weekly email overview

8.3. Views:

- Email Content Pack Views (Folder)
  - Email Overview
  - GEO overview
  - Inbound email
  - Outbound email

References:

- See KnowledgeBase article KB84404 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB84404)

9. Executive Content Pack

Applicable Device Types:

- McAfee SIEM

Use this content pack to:

- Get a quick overview of events in the McAfee ESM.

After you install this content pack:

- Adjust the content pack components to meet your organization's specific requirements.

- Change report templates to run at specified times, to e-mail specific recipients, and to save to remote locations automatically.

- Change report layouts to include additional data or to change the look of the report.

- Change view filters to meet your organization's specific requirements.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

9.1. Reports:

- Executive - Correlation Overview
- Executive - Event Summary
- Executive - Normalization Summary
- Executive - Summary and Performance

9.2. Views:

- Executive Content Pack Views (Folder)
  - Administrator Logon Summary
  - Asset Severity Summary
  - Configuration Management Summary
  - Correlation Overview
  - Logon Summary
  - Malware Overview
  - Normalization Summary
  - SIEM Performance (Folder)
    - Asset and Risk Summary
    - Combined Summary and Performance
    - Event Summary and Performance

- Flow Summary and Performance

References:

- See KnowledgeBase article KB84745 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB84745)

10. Exfiltration Content Pack

Applicable Device Types:

- All Devices

Use this content pack to:

- Monitor methods of network uploads used for data exfiltration.

- Detect tampering of confidential data.

- Detect leakage of digital information via printing physical copies.

- Analyze suspicious user behavior and their access to specific resources, gauging how often they access sensitive resources on the network.

Before you install this content pack:

- Gather a list of hostnames for systems considered to contain sensitive data or confidential internal information for your organization.

After you install this content pack:

- Configure alarms to send notifications and take automated actions.

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Setting up correlation rules to use flows requires the Advanced Correlation Engine (ACE).

- Change report templates to run at specified times, to e-mail specific recipients, and to save to remote locations automatically.

- Change report layouts to include additional data or to change the look of the report.

- Adjust variables to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- Adjust static watchlists to meet your organization's specific requirements.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

10.1. Alarms:

- Exfiltration - Possible Exfiltration

10.2. Correlation Rules:

- Exfiltration - Abnormal Communication and Exfiltration from High Value Host - Events and Flows

- Exfiltration - FTP Traffic with High Value Host

- Exfiltration - High Number of File Status Events on High Value Hosts

- Exfiltration - IM Client File Transfers with High Value Hosts

- Exfiltration - P2P Activity with High Value Hosts

10.3. Reports:

- Exfiltration - Exfiltration Analysis

- Exfiltration - Insider Threat Analysis

10.4. Variables:

- FTP Servers

10.5. Views:

- Exfiltration Content Pack Views (Folder)

  - High Value Host Activity

  - Potential Insider Threat Activity

  - Zone Exfiltration Summary

  - DLP Device Activity

10.6. Watchlists:

- High Value Hosts (Intel Security)

- Exfiltration - Possible User Threats

- Exfiltration - User Whitelist

References:

- See KnowledgeBase article KB85402 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB85402)

11. Exploit Content Pack

Applicable Device Types:

- All Devices

Use this content pack to:

- Track exploit events and possible exploits that could be appearing within the network.

- Identify attack behavior on specific systems, which you can then isolate from your network.

After you install this content pack:

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Setting up correlation rules to use flows requires the Advanced Correlation Engine (ACE).

- Change report templates to run at specified times, to e-mail specific recipients, and to save to remote locations automatically.

- Change report layouts to include additional data or to change the look of the report.

- Adjust variables to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- See KnowledgeBase article KB85403 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB85403)

This content pack contains:

11.1. Alarms:

- Exploit - Attempt on Internal Host

11.2. Correlation Rules:

- Exploit - FTP Login after Possible Exploit

- Exploit - Increasing Number of Exploit Events Occurring on an Internal Host

- Exploit - SSH Login after Possible Exploit

- Exploit - Shellshock Exploit Attempt

11.3. Reports:

- Exploit - Potentially Compromised Hosts

- Exploit - Potential Exploit Report

11.4. Views:

- Exploit Content Pack Views (View Folder)

  - Exploit Overview

  - Potentially Exploited Device Activity

  - Potential Exploit Activity

11.5. Watchlists:

- Exploit - Potentially Compromised Hosts

References:

- See KnowledgeBase article KB85403 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB85403)

12. Firewall Content Pack

Applicable Device Types:

- Firewall

- UTM

Use this content pack to:

- View and access firewall information based on events from correlation rules, alarms, reports, and parsed log data.

- Assist in detecting, monitoring, and preventing attacks or other unwanted traffic behavior.

After you install this content pack:

- Configure alarms to send notifications and take automated actions.

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Change report templates to run at specified times, to e-mail specific recipients, and to save to remote locations automatically.

- Change report layouts to include additional data or to change the look of the report.

- Adjust variables to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- Change default values of Variables; Home_Net and HTTP_SERVERS for content pack to function correctly.

- Existing standard rules are included in this content pack. To avoid duplicate events, please disable the following rules:

47-4000019, 47-4000020, 47-4000031, 47-4000045, 47-4000145.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

12.1. Alarms:

- Firewall - Firewall policy change

12.2. Correlation Rules:

- Firewall - Excessive Firewall/ACL connections accepted from single host
- Firewall - Excessive Firewall/ACL connections denied from single host
- Firewall - Firewall accept after recon event on a local host
- Firewall - Multiple Firewall or ACL events to multiple hosts that are blocked
- Firewall - Excessive Firewall and ACL acceptance from single host
- Firewall - Firewall policy change

12.3. Views:

- Firewall Content Pack Views (Folder)
  - Firewall View
  - Firewall View - Allowed Traffic
  - Firewall View - Blocked Traffic
  - Firewall Normalization View

- Vendor Firewall Views (Folder)
  - Check Point Firewall View
  - Cisco Firewall View
  - Cyberoam Firewall View
  - Dlink Firewall View
  - Fortinet Firewall View
  - Global Technical Association Firewall View
  - Juniper Firewall View
  - Kerio Firewall View
  - McAfee Firewall View
  - Microsoft Firewall View
  - Palo Alto Firewall View
  - Dell Firewall View
  - Tofino Firewall View
  - Secure Crossing Firewall View

12.4. Reports:

- Firewall - Daily Activity Report
- Firewall Report Layout (Report Layout)

References:

- See KnowledgeBase article KB84519 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB84519)

13. Hardware Health Content Pack

Normalization Categories:

- System > Hardware Status

Use this content pack to:

- Monitor system status events relating to hardware health.

Before you install this content pack:

- Ensure that "Reports" and "Alarms" are enabled.

After you install this content pack:

- Configure alarms to send notifications and take automated actions.

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- Change report templates to run at specified times, to e-mail specific recipients, and to save to remote locations automatically.

- Change report layouts to include additional data or to change the look of the report.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

13.1. Alarms:

- Hardware Health - High Severity Fan/Temperature Events

13.2. Correlation Rules:

- Hardware Health - Multiple Hardware Malfunction or Error Events

13.3. Reports:

- Hardware Health - Status

  - Hardware Health - Status Report (Report Layout)

13.4. Views:

- Hardware Health Content Pack Views (Folder)

  - Hardware Status View

References:

- See KnowledgeBase article KB85561 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB85561)

14. Malware Content Pack

Applicable Device Types:

- All Devices

Use this content pack to:

- Monitor events caused by malware.

- Analyze compromise and infection of the network, including activity from worms, trojans, viruses, spyware, adware, botnets, and other malware.

- Know which systems to isolate when major infections occur.

After you install this content pack:

- Configure alarms to send notifications and take automated actions.

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Setting up correlation rules to use flows requires the Advanced Correlation Engine (ACE).

- Change report templates to run at specified times, to e-mail specific recipients, and to save to remote locations automatically.

- Change report layouts to include additional data or to change the look of the report.

- Adjust variables to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- If applicable, specify zones from Asset Manager in Corporate Zone Trending View.

- Existing standard rules are included in this content pack. To avoid duplicate events, please disable the following rules:

47-4000088, 47-4000132, 47-4000136, 47-4000147.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

14.1. Alarms:

- Malware - Conficker Activity

- Malware - Shellshock Activity

- Malware - Stuxnet Activity

14.2. Correlation Rules:

- Malware - Botnet Activity
- Malware - Increasing Number of Malware Events Occuring on Internal Hosts
- Malware - Malware Activity Detected on Local Host
- Malware - Malware Sent from Internal Host
- Malware - Virus Activity Across Multiple Systems
- Malware - Botnet Detection
- Malware - Rootkit Detection

14.3. Reports:

- Malware Analysis
- Zone Analysis

14.4. Views:

- Malware Content Pack Views (Folder)
  - Infection Analysis
  - Malware Host and User Trending View
  - Malware Geolocation Trending View
  - Corporate Zone Trending View

References:

- See KnowledgeBase article KB84746 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB84746)

15. Operation SMN Content Pack

Applicable Device Types:

- IDS/IPS
- Antivirus

Use this content pack to:

- Monitor possible Operation SMN events, such as Antivirus events for specific known Axiom malware.

- Identify systems which have been infected by Axiom malware.

- For more information about Operation SMN, see the following links:

http://blogs.technet.com/b/mmpc/archive/2014/10/27/novetta-leads-first-coordinated-malware-eradication-campaign.aspx

http://www.novetta.com/2014/10/operation-smn-detailed-reporting-released/

This content pack contains:

15.1. Correlation Rules:

- Attack - Operation SMN

15.2. Watchlists:

- Operation SMN Malware

16. Reconnaissance Content Pack

Applicable Device Types:

All Devices

Use this content pack to:

- Monitor possible reconnaissance events, such as network sweeps and unusual use of specific protocols from external sources.

After you Install This Content Pack:

- Configure alarms to send notifications and take automated actions.

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Setting up correlation rules to use flows requires the Advanced Correlation Engine (ACE).

- Change report templates to run at specified times, to e-mail specific Recipients, and to save to remote locations automatically.

- Change report layouts to include additional data or to change the look of the report.

- Change view filters to meet your organization's specific requirements.

- Existing standard rules are included in this content pack. To avoid duplicate events, please disable the following rules:

47-4000043,47-4000044,47-4000046,47-4000047,47-4000048,47-4000049,47-4000050,47-4000051,47-4000052,47-4000053,47-4000054,47-4000055,47-

4000056,47-4000057,47-4000058,47-4000059,47-4000060,47-4000061,47-4000062,47-4000063,47-4000064,47-4000065,47-4000066,47-4000067,47-4000068,47-4000069,47-4000070,47-4000071,47-4000072,47-4000073,47-4000074,47-4000075,47-4000076,47-4000077,47-4000078,47-4000078,47-4000079,47-4000080,47-4000081,47-4000082,47-4000083,47-4000087,47-4000096,47-4000097,47-4000098,47-4000099,47-4000100,47-4000102,47-4000103,47-4000104,47-4000105,47-4000106,47-4000107,47-4000108,47-4000109,47-4000110,47-4000111,47-4000112,47-4000113.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

16.1. Alarms:

- Recon - Network Sweep Activity

16.2. Correlation Rules:

- Recon - Application Query Events from a Local Host
- Recon - Application Query Events from a Remote Host
- Recon - DNS Recon Events from a Local Host
- Recon - DNS Recon Events from a Remote Host
- Recon - Database Recon Events from a Local Host
- Recon - Database Recon Events from a Remote Host
- Recon - Detected Anomaly of TCP or UDP Packet Activity from Internal Host
- Recon - FTP Recon Events from a Local Host
- Recon - FTP Recon Events from a Remote Host
- Recon - Horizontal FTP Scan: Events or Flows
- Recon - Horizontal HTTP Scan: Events or Flows
- Recon - Horizontal HTTPS Scan: Events or Flows
- Recon - Horizontal NETBIOS Scan: port 137 and 138
- Recon - Horizontal NetBIOS Scan: port 139: Events and flows
- Recon - Horizontal RDP Scan: Events or Flows
- Recon - Horizontal RPC Scan: Events or Flows

- Recon - Horizontal SMB Scan: Events or Flows
- Recon - Horizontal SMTP Scan: Events or Flows
- Recon - Horizontal SNMP Scan: Events or Flows
- Recon - Horizontal SSH Scan: Events or Flows
- Recon - Horizontal Telnet Scan: Events or Flows
- Recon - Host Port Scan Events from a Local Host
- Recon - Host Port Scan Events from a Remote Host
- Recon - Host Query Events from a Local Host
- Recon - Host Query Events from a Remote Host
- Recon - ICMP Recon Events from a Local Host
- Recon - ICMP Recon Events from a Remote Host
- Recon - IP Address Recon Events from a Local Host
- Recon - IP Address Recon Events from a Remote Host
- Recon - Mail Recon Events from a Local Host
- Recon - Mail Recon Events from a Remote Host
- Recon - Misc Form of Reconnaissance Events from a Local Host
- Recon - Misc Form of Reconnaissance Events from a Remote Host
- Recon - Multiple TCP Recon Events from a Local Host
- Recon - Network Sweep Activity Detected from a Local Host to Multiple Hosts
- Recon - Network Sweep Activity Detected from a Local Host to Multiple Ports
- Recon - Network Sweep Activity Detected from a Remote Host to Multiple Local Hosts
- Recon - Network Sweep Activity Detected from a Remote Host to Multiple Local Ports
- Recon - Network Sweep Events from a Local Host
- Recon - Network Sweep Events from a Remote Host
- Recon - Other Protocol Recon Events from a Local Host
- Recon - Other Protocol Recon Events from a Remote Host

- Recon - RPC Request Events from a Local Host
- Recon - RPC Request Events from a Remote Host
- Recon - Recon Events from a Local Host to Multiple External Hosts
- Recon - Recon Events from a Remote Host
- Recon - SNMP Recon Events from a Local Host
- Recon - SNMP Recon Events from a Remote Host
- Recon - SSH Recon Events from a Local Host
- Recon - SSH Recon Events from a Remote Host
- Recon - TCP Recon Events from a Remote Host
- Recon - Telnet Recon Events from a Local Host
- Recon - Telnet Recon Events from a Remote Host
- Recon - UDP Recon Events from a Local Host
- Recon - UDP Recon Events from a Remote Host
- Recon - Web Recon Events from a Local Host
- Recon - Web Recon Events from a Remote Host

16.3. Reports:

- Recon - Network Scan Analysis Report
  - Recon - Network Scan Analysis Layout (Report Layout)
- Recon - Protocol Analysis Report
  - Recon - Protocol Analysis Layout (Report Layout)
- Recon - Recon Analysis Report
  - Recon - Recon Analysis Layout (Report Layout)

16.4. Views:

- Recon Content Pack Views (Folder)
  - Destination to Source Network Scan Analysis
  - Destination to Source Protocol Analysis
  - Destination to Source Recon Events
  - Source to Destination Network Scan Analysis

- Source to Destination Protocol Analysis

- Source to Destination Recon Events

16.5. Watchlists:

- Recon - Network Scan Devices

References:

- See KnowledgeBase article KB85200 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB85200)

17. TIE Content Pack

Applicable Device Types:

- TIE

Use this content pack to:

- View and access TIE information based on events from correlation rules, alarms, reports, watchlists, and parsed log data.

- Assist in detecting, monitoring, and preventing attacks or other unwanted traffic behavior.

After you install this content pack:

- Configure alarms to send notifications and take automated actions.

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Change report templates to run at specified times, to e-mail specific recipients, and to save to remote locations automatically.

- Change report layouts to include additional data or to change the look of the report.

- Adjust variables to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- Existing standard rules are included in this content pack. To avoid duplicate events, please disable the following rules:

47-4000174, 47-4000175, 47-4000176, 47-4000177, 47-4000178, 47-4000179.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

17.1. Alarms:

- TIE - Bad File Threshold
- TIE - Malicious File Found

17.2. Correlation Rules:

- TIE - GTI Reputation Changed from Clean to Dirty
- TIE - GTI Reputation Changed from Dirty to Clean
- TIE - Malicious file SHA-1 Found on Increasing number of Hosts
- TIE - Increase in Malicious Files Found Across All Hosts
- TIE - Malicious Filename Found on Increasing Number of Hosts
- TIE - Multiple malicious file Found on Single Host
- TIE - TIE Reputation Changed from Clean to Dirty
- TIE - TIE Reputation Changed from Dirty to Clean

17.3. Reports:

- TIE - Daily Overview

17.4. Views:

- TIE Content Pack Views (Folder)
  - TIE View
  - TIE Malicious File Watchlist View

17.5. Watchlists:

- TIE - Malicious Files Found

References:

- See KnowledgeBase article KB84533 to view the documentation for this content pack. (https://kc.mcafee.com/corporate/index?page=content&id=KB84533)

18. Wireless Access Point Content Pack

Applicable Device Types:

- All Wireless Devices

Use this content pack to:

- Provide visual high level metrics and bring transparency to all wireless device activity

- Tracking of device association, disassociation, and reassociation events

- Monitoring activity from the devices deriving from the association events

- Discovering anomalous or suspicious activity

- Promoting awareness of wireless system events to ensure Quality of Service

Before you install this content pack:

- Ensure your wireless device solution is supported under the official device list.

After you install this content pack:

- No actions must be performed after installation.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

18.1. Reports:

- WAP - Abnormal Wireless Events

- WAP - Association Events

- WAP - Wireless Event Summary

18.2. Views:

- WAP Content Pack Views (Folder)

  - Abnormal Wireless Events

  - Rogue Events Analysis

  - Wireless Association Events

  - Wireless Disassociation Events

  - Wireless Event Summary

  - Wireless Reassociation Events

  - Wireless System Events

References:

- See KnowledgeBase article KB85550 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB85550)

19. Web Filtering and Web Application Control Content Pack

Applicable Device Classes:

- Web filtering and web Application Control

- HTTP

Use this content pack to:

- View and access web filtering information based on events from devices that offer web filtering or web Application Control.

- Assist in detecting, monitoring, and preventing attacks or other unwanted traffic behavior.

After you install the content pack:

- Configure alarms to send notifications and take automated actions.

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Change report templates to run at specified times, to e-mail specific recipients, and to save to remote locations automatically.

- Change report layouts to include additional data or to change the look of the report.

- Adjust variables to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

Applicable data sources include:

- Barracuda Networks - Barracuda Web filter (ASP)

- Cisco - IronPort Web Security Appliance (ASP)

- EdgeWave - iPrism Web Security (ASP)

- Fortinet - FortiWeb Web Application Firewall (ASP)

- McAfee - WebShield (ASP)

- McAfee - Web Gateway (ASP)

- Radware - AppWall (ASP)

- Sophos - Web Security and Control (ASP)

- Squid - Squid (ASP)

- Symantec - Symantec Web Gateway (ASP)

- Trend Micro - InterScan Web Security Suite (ASP)

- TrustWave - WebDefend (ASP)

- Websense - Websense - CEF, Key Value Pair (ASP)

After you install this content pack:

- Adjust the content pack elements to meet your organization's specific requirements.

This content pack contains:

19.1. Correlation Rules:

- Web Filter - Excessive Web Connections

- Web Filter - Multiple Allowed Web Policy Connections

- Web Filter - Multiple Blocked Web Policy Connections

- Web Filter - Possible Web Exploit Event

19.2. Views:

- Web Filter Content Pack Views (Folder)

  - Web Filter Normalization View

  - Web Filter View

  - Web Filter View - Allowed

  - Web Filter View - Blocked

  - Vendor Web Filter Views (Folder)

    - Barracuda Web View

    - Cisco Web View

- EdgeWave Web View

- Fortinet Web View

- McAfee Web View

- Radware Web View

- Sophos Web View

- Squid Web View

- Symantec Web View

- TrendMicro Web View

- TrustWave Web View

- Websense Web View

19.3. Reports:

- Web Filter - Daily Activity Report

References:

- See KnowledgeBase article KB84521 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB84521)

20. Windows Authentication Content Pack

Applicable Device Types:

- Microsoft Windows Event Log - WMI

Use this content pack to:

- Monitor Microsoft Windows authentication events.

- Identify actionable intelligence within a network on correlated Windows-specific events.

Before you install this content pack:

- Set the Microsoft Windows Audit Policy to log both failed and successful logons.

- Forward logs to the Enterprise Security Manager.

- Ensure that the $CORP_GEOS variable includes all trusted company geolocations.

After you install this content pack:

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Adjust variables to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- Correlation rules found in this content pack function best when Aggregation is disabled for the following WMI events:

43-211005280, 43-211005281, 43-211005400, 43-211005760, 43-263046240, and 43-263046720.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

20.1. Correlation Rules:

- Windows Authentication - Administrator Account Logon on Vista-2008 or Later

- Windows Authentication - Administrator Account Logon on 2000-2003-XP

- Windows Authentication - Admin Logon From Non-Company Geolocation on Vista-2008 or Later

- Windows Authentication - Admin Logon From Non-Company Geolocation on 2000-2003-XP

- Windows Authentication - Admin Logon From Suspicious Geolocation on Vista-2008 or Later

- Windows Authentication - Admin Logon From Suspicious Geolocation on 2000-2003-XP

- Windows Authentication - Restricted Domain Account Failed Logon

- Windows Authentication - Domain User Failed Logon Due To Invalid Password

- Windows Authentication - Domain User Logon After Multiple Failed Attempts

- Windows Authentication - Failed Domain Logon on Restricted Host

- Windows Authentication - Failed Logon Due To Invalid Domain Username

20.2. Views:

- Windows Authentication Content Pack Views (Folder)

- Detailed Successful Windows Logons
- Successful Windows Logon Overview
- Administrator Views (Folder)
  - Correlated Views (Folder)
    - Correlated Admin Logons
    - Correlated Other Admin Logons
    - Correlated Service Account Admin Logons
    - Correlated Successful Admin Logon Overview
  - Normalized Views (Folder)
    - Admin Logons By Normalization
    - Other Admin Logons By Normalization
    - Service Account Admin Logons By Normalization
    - Successful Admin Logon Overview By Normalization

21. Windows Content Pack

Use this content pack to:

- Monitor failed Windows system errors.
- Monitor service errors in Windows.
- Monitor application crashes and hangs.
- Monitor system blue screens caused by applications.
- Monitor Applocker events.

Before you install this content pack:

- Your organization must have at least one Windows Event Log - WMI data source added in the McAfee ESM.
- In order to monitor Applocker events:

  Enable Applocker within Group Policy.

  Create an Applocker whitelist ruleset and configure rules to be enforced or audited.

  Ensure that the "Application Identity" service is running on monitored hosts.

After you install this content pack:

- Configure alarms to send notifications and take automated actions.

- Adjust correlation rule parameters to meet your organization's specific requirements.

- Change view filters to meet your organization's specific requirements.

- Adjust report filters to meet your organization's specific requirements.

- See KnowledgeBase article KB83783 to learn how to change the content pack components.

(https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

This content pack contains:

21.1. Alarms:

- Windows - High Value Host External Media Activity

21.2. Correlation Rules:

- Windows - System or Service Failures on a Single Host

- Windows - System or Service Failure with Malicious Activity

- Windows - Application Crashes or Hangs on a Single Host

- Windows - Application Crashes or Hangs on Multiple Hosts

- Windows - BSoD System Crashes on Multiple Hosts

- Windows - BSoD System Crashes on a Single Host

- Windows - Multiple Failed EXE or DLL Applocker Events on Multiple Hosts

- Windows - Multiple Failed EXE or DLL Applocker Events on a Single Host

- Windows - Multiple Failed MSI or Script Applocker Events on Multiple Hosts

- Windows - Multiple Failed MSI or Script Applocker Events on a Single Host

- Windows - Multiple Failed Packaged App Applocker Events on Multiple Hosts

- Windows - Multiple Failed Packaged App Applocker Events on a Single Host

21.3. Views:

- Windows Content Pack Views (Folder)

  - Windows System and Service Failures

  - Windows External Media Activity

  - Windows Application Failures

- Applocker Views (Folder)

- Applocker EXE and DLL Events

- Applocker MSI and Script Events

- Applocker Overview

- Applocker Packaged App Events

21.4. Reports:

- System and Service Failure Report

21.5. Report Layouts:

- System and Service Failure Layout

21.6. Watchlists:

- High Value Hosts (Intel Security)

References:

- See KnowledgeBase article KB86525 to view the documentation for this content pack.

(https://kc.mcafee.com/corporate/index?page=content&id=KB86525)