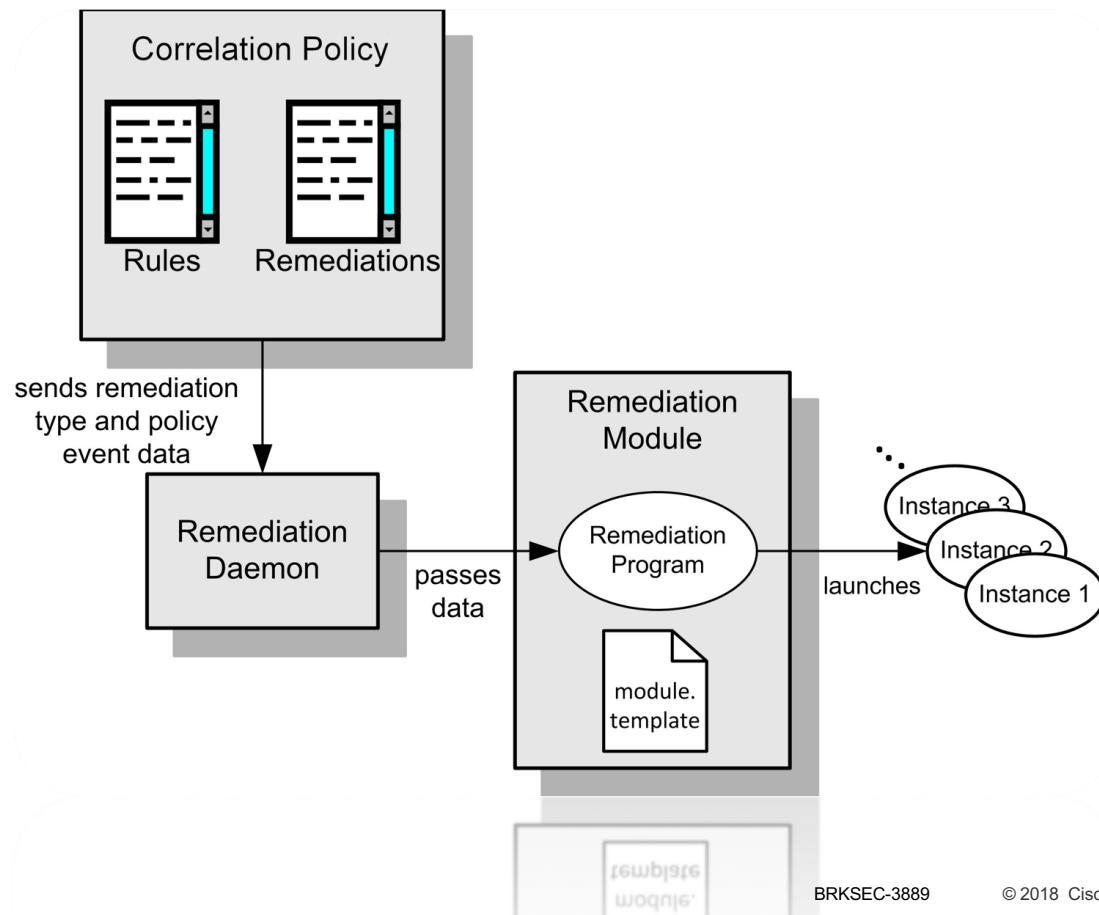
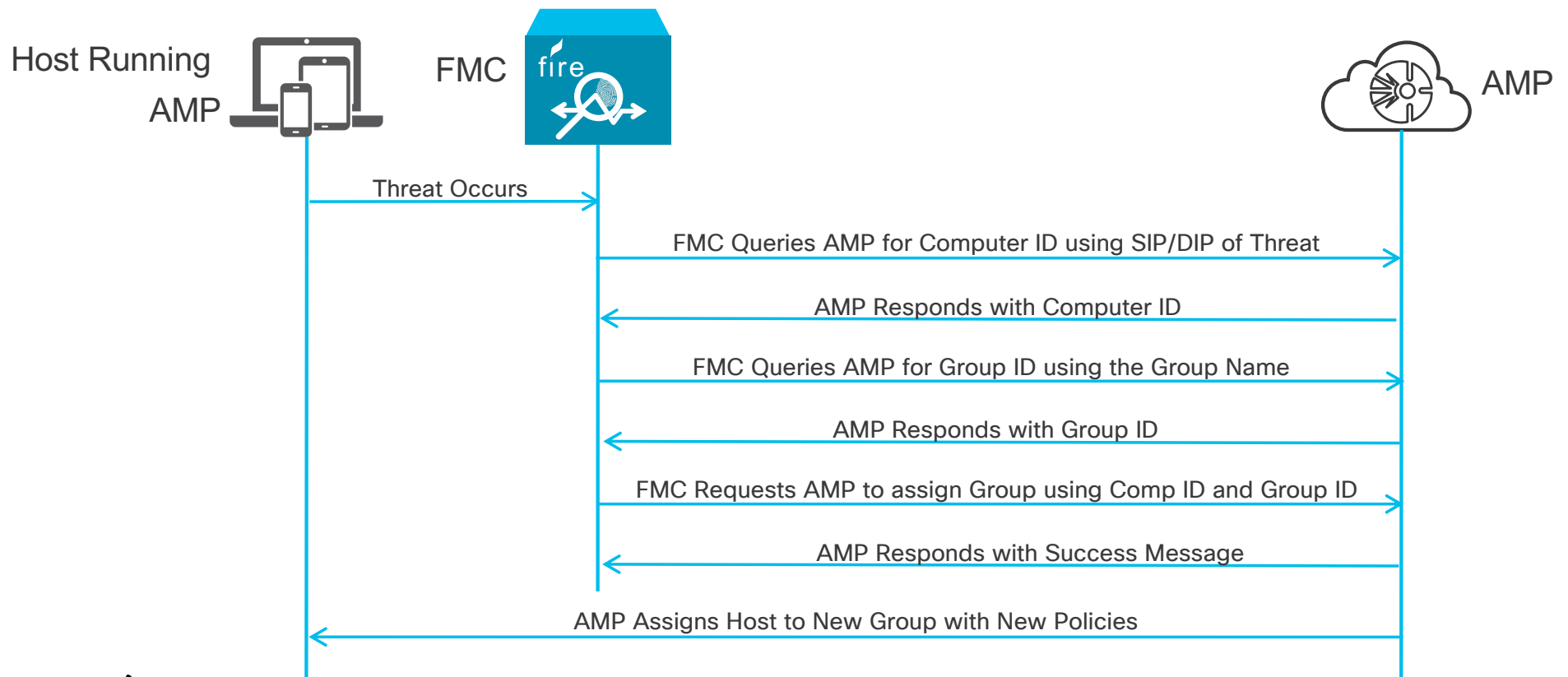


Firepower Remediation Subsystem Components

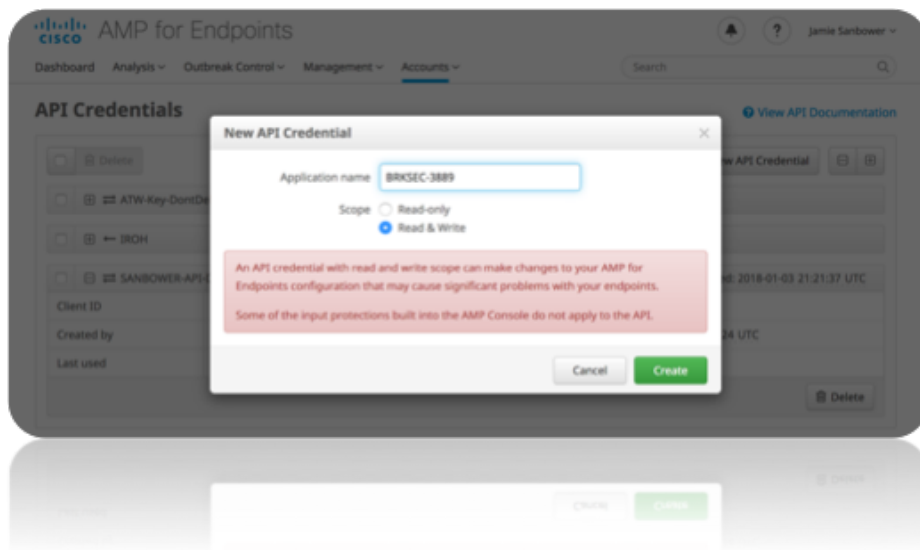


CUSTOM: AMP Rapid Threat Containment Overview



Create a new API Credential in AMP Cloud

Accounts > API Credentials



< API Key Details

The API credentials have been generated. Keep the new API credentials in a password manager or encrypted file.

3rd Party API Client ID

7538ca0efa3226d4d605

API Key

ba4d3598-5d96-4aa4-8de0-75603b375d57

API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a username and password, and should be treated as such.

Delete the API credentials for an application if you suspect they have been compromised and create new ones.

Deleting API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.

Your API credentials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.

[View API Documentation](#)

Create a new "Quarantine" Group in AMP Cloud

Management > Groups > Create Group

The screenshot shows the Cisco AMP for Endpoints Management console. The top navigation bar includes 'Dashboard', 'Analysis', 'Outbreak Control', 'Management' (selected), and 'Accounts'. The user 'Jamie Sanbower' is logged in. The 'Groups: Search' page shows a search bar with 'SANBOWER' and a 'Create Group' button. The search results list two groups: 'SANBOWER' and 'SANBOWER-TRIAGE'. The 'SANBOWER-TRIAGE' group is selected, and its details are shown on the right. The details include a table of policies and a section for 'Computers'.

SANBOWER-TRIAGE	
Last Modified	2018-01-04 01:52:51 UTC
Created by	Jamie Sanbower
Windows Policy	Exploit Prevention Policy
Android Policy	Droid_Test
Mac Policy	ATW-MacPolicy
Linux Policy	ATW-LinuxPolicy
Network Policy	Default Network
IOS Policy	Default IOS
Parent Groups	SANBOWER

Computers
No computers have been assigned to this group
No child members

Allows
Unique
Policy

Add AMP Remediation Module to FMC

Policies > Actions > Remediation > Modules

Overview

Analysis

Policies

Devices

Objects

AMP

Intelligence

Access Control ▾

Network Discovery

Application Detectors

Correlation

Actions ▶ Modules

Installed Remediation Modules

Module Name	Version	Description
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
Nmap Remediation	2.0	Perform an Nmap Scan
pxGrid Mitigation	1.0	Perform a pxGrid mitigation against the involved IP addresses
Set Attribute Value	1.0	Set an Attribute Value

Install a new module


Browse...

No file selected.

Install

Add AMP Remediation Module to FMC

Policies > Actions > Remediation > Modules

 **Success**
Module successfully installed

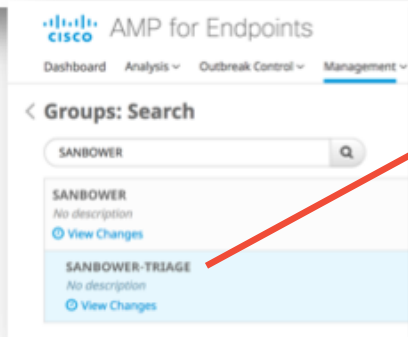
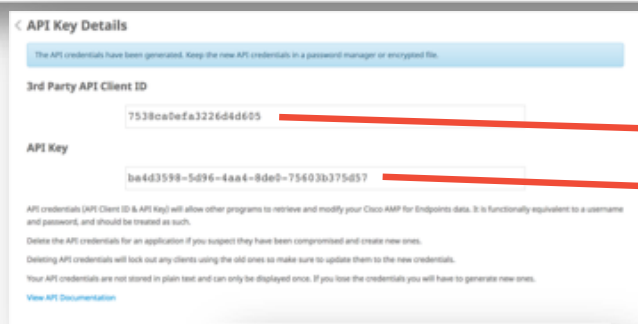
Installed Remediation Modules

Module Name	Version	Description
AMP Remediation	0.99.1	Change AMP Computer Group by IP addresses using AMP Cloud
Cisco IOS Null Route	1.0	Block an IP address in a Cisco IOS router
Nmap Remediation	2.0	Perform an Nmap Scan
pxGrid Mitigation	1.0	Perform a pxGrid mitigation against the involved IP addresses
Set Attribute Value	1.0	Set an Attribute Value

Install a new module
 No file selected.

Add a New Instance of AMP Remediation Module to FMC

Policies > Actions > Remediation > Instances



Edit Instance

Instance Name: BRKSEC-3889

Module: AMP Remediation(v0.99.1)

Description: Move Systems to New AMP Group

API Client ID: 0350d42f55e09079a78e

API Key: Retype to confirm

Group Used as Quarantine: SANBOWER-TRIAGE

SYSLOG Logging: On

White List: 10.28.128.0/24

Create Cancel

Add Remediation Type to FMC

Policies > Actions > Remediation > Instances

- Destination Based Remediation
 - Used when admin wants to quarantine the target/destination of an event
 - E.G. Malware Download
- Source Based Remediation
 - Used when admin wants to quarantine the attacker/source of an event
 - E.G. Host becomes pivot point and starts launching attacks

Edit Instance

Instance Name: BRKSEC-3889

Module: AMP Remediation(v0.99.1)

Description: Move Systems to New AMP Group

API Client ID: 0350d42f55e09079a78e

API Key:

Group Used as Quarantine: SANBOWER-TRIAGE

SYSLOG Logging: ☒ On ☐ Off

White List: 10.28.128.0/24

Save Cancel

Configured Remediations

Remediation Name	Remediation Type	Description
AMP-TRIAGE-DESTINATION	Quarantine Destination IP	
AMP-TRIAGE-SOURCE	Quarantine Source IP	

Add a new remediation of type: Quarantine Destination IP Add

Create Correlation Rule

Policies > Correlation > Rule Management > Create Rule

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control Network Discovery Application Detectors **Correlation** Actions

Alerts Remediations Groups

Policy Management **Rule Management** White List Traffic Profiles

Rule Information

Rule Name: BRKSEC-3889-RULE

Rule Description: Match Traffic going to Bad Security IP/Domains

Rule Group: Ungrouped

+ Add Connection Tracker + Add User Qualification + Add Host Profile Qualification

Select the type of event for this rule

If a connection event occurs at either the beginning or the end of the connection and it meets the following conditions:

+ Add condition + Add complex condition

OR	X	Security Intelligence Category	is	CnC
	X	Security Intelligence Category	is	Malware
	X	Security Intelligence Category	is	Exploitkit

Rule Options

+ Add Inactive Period

Snooze: If this rule generates an event, snooze for 0 hours

Inactive Periods: There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

Save Cancel

Connection Event

Sec Intelligence matching
CnC, Malware or Exploitkit

Create Correlation Policy

Policies > Correlation > Policy Management > Create Policy

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy 1 System Help admin

Access Control Network Discovery Application Detectors **Correlation** Actions

Alerts Remediations Groups

Policy Management Rule Management White List Traffic Profiles

Create Policy (1)

Name BRKSEC-3889-POLICY Sort by State

Make Sure to Enable (6)

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy 1 System Help admin

Access Control Network Discovery Application Detectors **Correlation** Actions

Alerts Remediations Groups

Policy Management Rule Management White List Traffic Profiles

Correlation Policy Information

Policy Name BRKSEC-3889-POLICY

Policy Description

Default Priority None

Policy Rules

Rule	Responses	Priority
BRKSEC-3889-RULE Match Traffic going to Bad Security IP/Domains	EMAIL JAMIE CISCO (Email) AMP-TRIAGE-SOURCE (Remediation)	Default

Responses for Malware-Download

Assigned Responses

AMP-TRIAGE-SOURCE
EMAIL JAMIE CISCO

Unassigned Responses

AMP-TRIAGE-DESTINATION

Update Cancel

Save Cancel (5)

Add Rules (2)

Responses (3)

Responses (4)

Test Configuration

The screenshot shows the Cisco AMP console interface. The top navigation bar includes tabs for Overview, Analysis (selected), Policies, Devices, Objects, AMP, and Intelligence. Below this, a secondary navigation bar lists various categories: Context Explorer, Connections, Intrusions, Files, Hosts, Users, Vulnerabilities, Correlation (selected), Correlation Events, Custom, Lookup, and Search. The main content area is titled 'Correlation Events' and shows a table with one row of data. The table has columns for Time, Impact, Inline Result, Source IP, Source Country, Destination IP, Destination Country, Security Intelligence Category, Source User, Destination User, Source Port / ICMP Type, Destination Port / ICMP Code, Description, Policy, Rule, and a partial 'Pr' column. The data row shows a timestamp of 2018-01-04 11:28:15, source IP 10.28.10.100, destination IP 58.195.1.4, and destination country CHN. The description mentions '8 (Echo Request) / icmp' and '0 (No Code) / icmp'. The policy is 'BRKSEC-3889-POLICY' and the rule is 'BRKSEC-3889-RULE'. The status is 'Expanding'.

Time	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Security Intelligence Category	Source User	Destination User	Source Port / ICMP Type	Destination Port / ICMP Code	Description	Policy	Rule	Pr
2018-01-04 11:28:15			10.28.10.100		58.195.1.4	CHN	CrC			8 (Echo Request) / icmp	0 (No Code) / icmp	Connection Type: FireSIGHT	BRKSEC-3889-POLICY	BRKSEC-3889-RULE	No

The screenshot shows the Cisco AMP console interface for Remediation Status. The top navigation bar is the same as the previous screenshot. The secondary navigation bar lists: Context Explorer, Connections, Intrusions, Files, Hosts, Users, Vulnerabilities, Correlation (selected), Status, Custom, Lookup, and Search. The main content area is titled 'Remediation Status' and shows a table with one row of data. The table has columns for Time, Remediation Name, Policy, Rule, and Result Message. The data row shows a timestamp of 2018-01-04 11:28:17, remediation name 'AMP-TRIAGE-SOURCE', policy 'BRKSEC-3889-POLICY', rule 'BRKSEC-3889-RULE', and result message 'Successful completion of remediation'. The status is 'Expanding'.

Time	Remediation Name	Policy	Rule	Result Message
2018-01-04 11:28:17	AMP-TRIAGE-SOURCE	BRKSEC-3889-POLICY	BRKSEC-3889-RULE	Successful completion of remediation

Validate Changes in AMP

The screenshot shows the Cisco AMP for Endpoints Management console. The 'Groups' page is active, displaying a list of groups on the left and the details of the selected 'SANBOWER-TRIAGE' group on the right. The 'SANBOWER-TRIAGE' group is highlighted in blue. The details panel on the right shows the group's configuration, including policies for Windows, Android, Mac, Linux, Network, and iOS. A red box highlights the 'Computers' section, which shows '1 direct member' named 'optimus'.

Groups

Search

« < 1 2 > »

SANBOWER
No description
[View Changes](#) [Edit](#) [Delete](#) 1 Child Group

SANBOWER-TRIAGE
No description
[View Changes](#) [Edit](#) [Delete](#)

Bui Test Group
Test Group for all new and beta features.
[View Changes](#) [Edit](#) [Delete](#)

Beta Features Root Group
Beta Features Root Group
[View Changes](#) [Edit](#) [Delete](#) 1 Child Group

« < 1 2 > »

SANBOWER-TRIAGE
No description

Last Modified	2018-01-04 01:52:51 UTC
Created by	Jamie Sanbower
Windows Policy	Exploit Prevention Policy
Android Policy	Droid_Test
Mac Policy	ATW-MacPolicy
Linux Policy	ATW-LinuxPolicy
Network Policy	Default Network
iOS Policy	Default iOS
Parent Groups	SANBOWER

Computers
1 direct member
[optimus](#)
No child members

Validate Changes in AMP

The screenshot shows the Cisco AMP for Endpoints interface. The top navigation bar includes the Cisco logo, the product name 'AMP for Endpoints', and user information 'Jamie Sanbower'. The 'Accounts' menu is selected. Below the navigation bar is the 'Audit Log' section. It features a filter panel with dropdowns for 'Type', 'Event', and 'Item', and input fields for 'Date Range' (Start/End), 'User' (set to 'API client'), and 'IP Address' (set to 'Single IP or CIDR'). 'Clear Filters' and 'Apply Filters' buttons are present. The audit log table has columns for 'Event', 'Details', 'User', 'IP Address', and 'Date'. The 'User' column is highlighted with a red box, showing 'API client'. The first log entry shows an 'Update' event for 'optimus' with the timestamp '2018-01-04 16:28:19 UTC'. A message 'Moved to group SANBOWER-TRIAGE' is displayed at the bottom of the log.

Event	Details	User	IP Address	Date
Update	optimus	API client		2018-01-04 16:28:19 UTC

Moved to group SANBOWER-TRIAGE

AMP Remediation Module

Load Instance Configuration
API Parameters, Group Name, Whitelist

Get Parameters Passed from Policy
IPs that needs to be Quarantined

Read the Config File into Variables

```
56 #####
57 # Main
58 #####
59
60 # Load Config File
61 # FOR TESTING USE THE INSTANCE name my $config_file = './JAMIE/instance.conf';
62 my $config_file = "instance.conf";
63
64 # Get and save the program name, without path
65 my $prog = $0;
66 $prog =~ s/^.*\\///;
67
68 # Show usage if not enough parameters
69 if (@ARGV < 5)
70 {
71     warn("Usage: $prog <remediation_type> <ip> <policy> <rule_id> <sid>\n\n");
72     exit(INPUT_ERR);
73 }
74
75 # Get the parameters
76 my ($rem,          # Remediation type
77     $ip,           # Address to be killed
78     $policy,       # Compliance Policy that called this remediation
79     $rule,         # Compliance Rule that called this remediation
80     $sid) = @ARGV; # SID that fired (if this was an intrusion event based rule)
81
82 # create xml object
83 my $xml = new XML::Simple;
84
85 # read XML file
86 my $data = $xml->XMLin($config_file, ForceArray=>['network_li', 'string']);
87
88 # Move Data into variables
89 my $apiclient = $data->{config}->{string}->{user_name}->{content};
90 my $apikey = $data->{config}->{password}->{content};
91 my $groupname = $data->{config}->{string}->{group_name}->{content};
92 my $log = $data->{config}->{boolean}->{content};
93
```

AMP Remediation Module

Whitelist Check
"Do Not Modify" IP List

Main Program

Final Status Reporting

```
100
101 logInfo('Starting AMP remediation');
102
103 # Whitelist Check
104 if ($data->{config}->{list}->{network_li}) {
105     foreach my $list (@{$data->{config}->{list}->{network_li}}) {
106         my $netblock = Net::Netmask->new($list);
107         if ($netblock->match($ip)) {
108             logInfo("Whitelist match ($ip is in $netblock): Remediation aborted");
109             print "Whitelist match ($ip is in $netblock): Remediation aborted\n" if $debug;
110             exit(WHITELIST);
111         }
112     }
113 }
114
115
116 # Call our subs that makes the requests.
117 my $compid = get_compID();
118 my $groupid = get_groupID();
119 my $returnstatus = set_group($compid,$groupid);
120
121
122 logInfo("AMP Remediation Success: $returnstatus");
123 exit;
124
125 # if we get here something unhandled happened...
126 logWarn("We encountered an unhandled exception: $returnstatus");
127
128 exit(UNDEF);
129
```

AMP Remediation Module

Easy Accomplished in sh, Python, Go, etc.

API Credentials

API URL

Use IP and Get Computer ID from AMP Cloud

Use Group Name and Get Group ID from AMP Cloud

Assign new Group using Comp ID and Group ID

<https://github.com/QuiLoxx/ATS-APIs>