

# تاديدهتلا ضرعل "MITER" لمع راطا "مدختسا" محوللا ةرادا يف مكحتلا ةدحو يف ةلمتحملا يدصتلا ىلع لمعل او ةنمآلا (FMC) ةيساسا اهل

## تايوتحملا

[ةمدقملا](#)

[ةيساسا تامولعم](#)

[ةيساسا اناابلطتلا](#)

[ناابلطتلا](#)

[ةمدختستلا تانوكملا](#)

[رتيم لمع راطا دىاوف](#)

[للسننلا جهن يف MITER لمع راطا ضرع](#)

[لفطتلا تادحا ضرع](#)

## ةمدقملا

لمعل او ةلمتحملا تاديدهتلا ضرعل MITER لمع راطا مادختسا ةيفيك دننستسما اذه حضوي (FMC) نمآلا FirePOWER ةرادا زكرم يف اهيلع

## ةيساسا تامولعم

ةدعاق وه (ةكرتشملا فراعمل او تاي نقتلاو ةيئادعلا تاكيكتلا) "هيك دنآ رتيم" لمع راطا نا اءارجلاو تاي نقتلاو تاكيكتلا لوح ةبقات يور رفوت قاطنلا ةعساو ةيجهنمو ةيفرم قاحلا ىلى فدهت يتلا تاديدهتلا يف ةلعافلا تاهجلا لبق نم اهعيزوت متي يتلا (TTPs) ةصنم وأ لپغشت مظن اهنم لك لثمت تافوفصم يف ATT&CK عمجتو. ةمظنألاب ررضلا ةدحملا بيلاسالا ىلع ادمتعم نوكيو "كيكتلا" ب فرعت موجهلا لهارم نم ةلحرم لك. ةنيعم "بيلاسالا" مساب ةفورعمل او، لهارملا كلت قيقت يف ةمدختستلا

، ةينقتلا نع تامولعم اهبصت كوكصل او تامدخل يف ةراجتلا قافتا راطا يف ةينقت لكو. يقيقتلا ملال نم ةلثمأو، فشكلا تاي لمعو، ةلمتحملا عوفدل او، اهب ةطبترملا تءارجلاو تاعومجم وأ ديدهتلا تاعامج ىلى ةراشلا تاعامج اضيا مضي "هيك دنآ رتيم" لمع راطا نا امك تاكيكتلا نم ةعومجم ىلى اذانتسا ديدهتلا لاجم يف ةلعافلا تاهجلا وأ عطشنألا فينصت ىلع لمعل راطا دعاسي، تاعومجملا مادختساب. اهمدختست يتلا تاي نقتلاو تادنتستلا تايكولس.

لمع راطا ضرعلا ىلى <https://attack.mitre.org> عوجرلا ىجرى، Miter لوح تامولعمل نم ديزم

## ةيساسا اناابلطتلا

## تاب لطلت مل

ةة لالتل عيضاوم لابل ةفرعم كيدل نوكت نأب Cisco ي صوت

- ريخشلا ةفرعم
- نم آ FMC
- ةيامحلل ةوق ديهت نع نم آلا عافدل

## ةمدختس مل تانوك مل

ةة لالتل ةيدامل تانوك مل او جم اربل اارااصل اىل دنن تسمل اذف ةدراول تامولعمل دنن تست

- Firepower تاصلنم عيجم اىل دنن تسمل اذف قبطني
- 7.3.0 رادصلال، هليغشت يراجلال Secure FTD جم انرب
- نم 7.3.0 رادصلال لغشي يذل Secure Firepower Management Center Virtual (FMC) جم انربل

ةصاخ ةيلمعم ةئيبي ف ةدوومل ةزهجال نم دنن تسمل اذف ةدراول تامولعمل عاشن ا مت تناك اذف. (يضا رتفا) حوسمم نيوكتب دنن تسمل اذف ةمدختس مل ةزهجال عيجم اءب رمأ اىل لم تحملل ريثا لىل كمهف نم دكا ف، ليغشتل دي قكتكبش

## رتيم لمع راطل اءاوف

- نكمت يىلل للستل اءا ح اىل انا يابل لىل قن اءارج او انا نقتو تاكي تكت ةفاضا متت فراعمل او مصلل تاكي تكت (MITER ATT&CK لمع راطل اىل عانبل لمعمل نم ني لوؤس مل ةيلباقل نم ديزمب اهتجال عم و رورمل ةكرح ضرع نم ني لوؤس مل نكمي اذو. (ةعئاشل ةئف و اءهال ماظنل و اءارغثلل عون بسح ءعاوقل عيجمت مهنكمي امك، ليءعثلل ديهتل
- كل حمسي اذو. "هيك دنأ يىل اءي رتيم" لمع راطل اىل اق فو لفلطلل ءعاوق ميظنت كنكمي ةنيعم نيجماهم تاينقتو تاكي تكتل اق فو تاسايسل لصي صخبت

## للىستل اءه ن ف MITER لمع راطل اءه

ةئف ءرجم وه رتيمو. كب ةصاخل لفلطلل ءعاوق لالخال لىل قننل نم MITER لمع راطل اءه كنكمي نم تاينوتسم ءءل ءعاوقل لىل قنن. Talos ءعاوق تاعومجم نم عىج وه ءعاوقل تاعومجم نم رىخا ءعاوقل لىل قننم عيجمتو ربكأ ءنورم رفوي امم موعءم ءعاوقل تاعومجم

1. Policies > Intrusion رتخا.
2. بىوبتلل ءمالع Intrusion Policies رايءخا نم دكا.
3. ءعاسم لىل قننل اءررحت و اءضرع ءيرت يىلل لفلطلل ءسايس راولب Snort 3 Version رقنا.
4. ءقوبطلل Group Overrides قوف رقنا.

ةوعومجم لىل قننل اءه كنكمي. يمره لىل قننل ءعاوقل تاعومجم تائف لك ءقوبطلل Group Overrides ءرست ءعاوقل ءوعومجم لك ف ءقرولا ءرطس مل ءريخا



Base Policy: Balanced Security and Connectivity Mode: Prevention

Description test\_policy

Base Policy → Group Overrides → Recommendations Not in use → Rule Overrides Summary Page 3

Group Overrides ?

101 items All x v +

Search through all Rule Groups

MITRE (1 group)

ATT&CK Framework (1 group)

Enterprise (13 groups)

MITRE / ATT&CK Framework 1 Groups

Group Name Security Level

9. هديدمتل "ةسسؤم" قوف رقنا ، ATT&CK Framework تحت 9.

Base Policy: Balanced Security and Connectivity Mode: Prevention

Description test\_policy Page 3

Base Policy → Group Overrides → Recommendations Not in use → Rule Overrides

Group Overrides ?

101 items All x v +

Search through all Rule Groups

MITRE (1 group)

ATT&CK Framework (1 group)

Enterprise (13 groups)

MITRE / ATT&CK Framework / Enterprise 13 Groups

Group Name

10. يوتسم يلع ةريبك تاريخيغت ءارجال دعاوقلا ةعومجمل نامألا يوتسم راجب ( ) Edit رقنا 10. دعاوقلا ةعومجم ةئف Enterprise نمض ةنرتقملا دعاوقلا ءاعومجم ةفاكل نامألا

Base Policy → Group Overrides → Recommendations Not in use → Rule Overrides Summary

Group Overrides ?

101 items All x v +

Search through all Rule Groups

MITRE / ATT&CK Framework / Enterprise / Collection (TA0009) 1 Groups

Security Level

Group Name	Security Level	Override	Rule Count
Input Capture (T1056) Adversaries may use methods of capturing user input to obtain credentials or collect inf...	Security Level	Override	256 Include

نامألا دعاوق ةعومجم ريرحت

11. Save. رقنا وراطال Edit Security Level ي 3 نامألا يوتسم رتخأ ، لاثملا لابس يلع 11.

# Edit Security Level



Higher security with more detections for administrators who are willing to tolerate some network latency and low level of false positives, in an effort to catch more attacks.

← Revert to default

Cancel

Save

نام ألي يوتسم

12. هق اطن عي سوت ل Initial Access رقنا ، Enterprise تحت .

13. تاح فصل ال نم ة ري خأ ال ة وم جم ال يه يت ل او ، Exploit Public-Facing Application رقنا ، Initial Access تحت .

Base Policy → Group Overrides → Recommendations Not in use → Rule Overrides → Summary

Group Overrides 101 items

Search through all Rule Groups

MITRE / ATT&CK Framework / Enterprise / Initial Access (TA0001) 5 Groups Security Level

Group Name	Security Level	Override	Rule Count	
Drive-by Compromise (T1189) Adversaries may gain access to a system through a user visiting a website over the nor...	○○○○	⊖	8783	Include
Exploit Public-Facing Application (T1190) Adversaries may attempt to take advantage of a weakness in an Internet-facing comput...	○○○○	⊖	11976	Include
External Remote Services (T1133) Adversaries may leverage external-facing remote services to initially access and/or per...	○○○○	⊖	443	Include
Phishing (T1566) Adversaries may send phishing messages to gain access to victim systems. All forms o...	○○○○	⊖	304	Include
Valid Accounts (T1078) Adversaries may obtain and abuse credentials of existing accounts as a means of gaini...	○○○○			

ة ل و أ ال ل و ص و ال ة وم جم

14. تاءارج ، ة دع اقل ال لي صافات ، ة فل تخم ال دع او قل ضرع ل رز View Rules in Rule Overrides قوف رقنا .  
ة فل تخم ال دع او قل ل اذك هو ، ة دع اقل ال

This group does not contain any children.

0 Groups / Group contains 8783 rules

[View Rules in Rule Overrides](#)

دعاوقلا تازواجت في دعاوقلا

Cisco. اھب ې صوت ېتلا دعاوقلا مادختسا ادبلا Start رقنا مٲ ةقبط Recommendations قوف رقنا 15. لوصأب ةطبرملا فعضل طاقن فادهتسال لفطتلا دعاوق تايصوت مادختسا كنكمي تامولعمل نم ديزملا ىلع لوصحلل. ةكبشلا في اهنع فشكلا متي تلا فيضملا

Base Policy → Group Overrides → **Recommendations** Not in use → Rule Overrides | Summary

Cisco Recommended Rules ⓘ

**Start using recommendations**

You can use Cisco Recommended Rules to target vulnerabilities associated with host assets detected in the network

[Start](#)

تايصوت

# Cisco Recommended Rules



Security Level (Click to select)

Accept Recommendation to Disable Rules i

**Higher Efficiency**– Keeps existing rules that match potential vulnerabilities on discovered hosts and disables rules for vulnerabilities not found on the network.

Protected Networks i

Add +

Cancel

Generate

Generate and Apply

ضرع كنكمي. ةسايسلا لىل ةيلال تاريغت لل لماش ضرل ةقبط Summary قوف رونا 16. كلذ لىل امو دع او قل تاي طختو ةوم جم ل تاي طختو ةدع اق ةيزوت

Base Policy → Group Overrides → Recommendations **Not in use** → Rule Overrides Summary

### Summary

**Rule Distribution**

Alert	645
Block	10879
Disabled	33478
Others	5067

**Active Rules** 16591  
**Overridden Rules** 4 View Effective Policy  
**Disabled Rules** 33478  
**Total Rules** 50069

**Report and Exporting**

Generate Report

Export Policy

**Base Configuration**

Base Policy: Balanced Security and Connectivity

**Recommendations**

Usage: **Not in use** Turn on recommendations

**Group Overrides**

Total 2 group overrides

- Non-Application Layer Protocol
- Malicious File

**Rule Overrides**

Total 4 rule overrides

1:62647	Block	→	Alert
1:61683	Drop	→	Alert
1:61681	Drop	→	Block
1:61684	Drop	→	Drop

جهنال صخلم

## لفطتال شادحاً ضرع

شادحاً ال ضرع في لفظتال شادحاً في دع او قل تاعوم جم و Miter ATT&CK تاي نقت ضرع كنكمي لىل snort (GID:SID) دع او قل نم تاني عي Talos رفوي. دحوم ل شادحاً ال ضرع و يكي سالا ل نام ال ةمزح نم عزجك تاني عي ال هذه تي ثت م تي. دع او قل تاعوم جم و Miter ATT&CK تاي نقت





Views... Rule Group Protocol Select...

Showing all 501 events (501) 2022-07-19 10:19:09 EDT → 2022-07-19 11:19:09 EDT 1h

Time	Event Type	Device	MITRE ATT&CK	Rule Group	Snort ID
2022-07-19 11:19:08	Intrusion	snort: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:07	Intrusion	snort: 192.168.7.115		Protocol • DNS	1:254:16
2022-07-19 11:19:03	Intrusion	snort: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:02	Intrusion	snort: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:59	Intrusion	snort: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:38	Intrusion	snort: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:35	Intrusion	snort: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:31	Intrusion	snort: 192.168.7.115		1 Group	1:254:16

دعاوقلا ةومجم لوكوتورب

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل