Mandiant® Advantage Threat Intelligence Engine Integration Configuration Guide

Software Version 1.0

Integration Guide

April 21, 2023

30002-06 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 I F: 703.229.4489
www.ThreatConnect.com

Table of Contents

Overview

The Mandiant Advantage Threat Intelligence Engine Integration with ThreatConnect® allows customers to ingest Mandiant Advantage Threat Intelligence Reports, Indicators, Campaigns, Actors, Malware, Attack Patterns, and Vulnerabilities into ThreatConnect seamlessly.

Dependencies

ThreatConnect Dependencies

- Active ThreatConnect Application Programming Interface (API) key

Note: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Customers on Dedicated Cloud and On-Premises instances can enable these settings on the **Account Settings** screen within their ThreatConnect instance.

Mandiant Dependencies

- Active Mandiant Advantage Threat Intelligence subscription that provides access to an API key

Application Setup and Configuration

1. Install the **Mandiant Advantage Threat Intelligence Engine** App via TC Exchange™.
2. Use the ThreatConnect Feed Deployer to set up and configure the **Mandiant Advantage Threat Intelligence Engine** App.

Configuration Parameters

Parameter Definitions

The parameters defined in Table 1 apply to the configuration parameters available when using the Feed Deployer to configure the App.

Table 1

Name	Description	Required?
Source to Create	The name of the Source to be created in ThreatConnect.	Yes
Owner	The Organization in which the Source will be created in ThreatConnect.	Yes
Activate Deprecation	Select this checkbox to allow the creation of depreciation rules for Indicators in the Source.	No
Create Attributes	Select this checkbox to allow the creation of custom Attribute Types in the Source.	No
Launch Server	Select the server on which the Service corresponding to the Feed API Service App will launch. It is recommended to select **tc-job**.	Yes
Mandiant Indicator Types	Select the Indicator type(s) to import from Mandiant.	Yes
Mandiant Group Types	Select the Group type(s) to import from Mandiant.	Yes
Mandiant Report Types	Select the Report type(s) to import from Mandiant.	Yes
Minimum Mscore Filter	The minimum Mandiant Indicator Confidence score (Mscore) that Indicators in Mandiant	Yes

	must have in order to be imported into ThreatConnect. The default value is **80**.	
Exclude OSINT	Select this checkbox to prevent open-source intelligence (OSINT) from being imported into ThreatConnect. The default value is **True**.	Yes
Mandiant Advantage API Public Key	The Mandiant Advantage Threat Intelligence ID.	Yes
Mandiant Advantage API Secret Key	The Mandiant Advantage Threat Intelligence API secret key.	Yes

Data Mappings

The data mappings in Table 2 through Table 15 illustrate how data are mapped from Mandiant Advantage Threat Intelligence API endpoints into ThreatConnect's data model.

Reports

ThreatConnect object type: Report Group

Table 2

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
reportId	Attribute: "Report ID"
title	Attribute: "Report Title"
ThreatScape	Tag
audience	Tag
publish_date	Attribute: "Report Publish Date"
version	Attribute: "Version"
version_one_publish_date	Attribute: "Report Version 1 Publish Date"
intelligence_type	N/A
report_type	Attribute: "Report Type"
report_link	N/A
threat_description	Attribute: "Description"

cve_ids	Tag
tags[*].actors.id	N/A
tags[*].actors.name	Tag
tags[*].affected_industries	Attribute: "Targeted Industry Sector"
tags[*].intended_effects	Attribute: "Intended Effects"
tags[*].motivations	Attribute: "Adversary Motivation Type"
tags[*].malware_families	N/A
tags[*].operating_systems	Attribute: "Operating System"
tags[*].ttps	N/A
tags[*].target_geographies	Attribute: "Target Country"
tags[*].affected_systems	Attribute: "Affected Systems"
tags[*].source_geographies	Attribute: "Adversary Origin & Source"
tags[*].targeted_informations	Attribute: "Targeted Information"

Vulnerability Reports

ThreatConnect object type: Report Group

Table 3

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
reportId	Attribute: "Report ID"
title	Attribute: "Report Title"
ThreatScape	Tag
audience	Tag
publish_date	Attribute: "Report Publish Date"
version	Attribute: "Version"
version_one_publish_date	Attribute: "Report Version 1 Publish Date"
intelligence_type	N/A
report_type	Attribute: "Report Type"
report_link	N/A
cve_ids	Tag: " %cve_id%"
risk_rating	Tag: "Risk Rating: %risk_rating%"
summary	Attribute: "Description"

vendor_fixes.name	Attribute: "Vendor Fix URL" (one concatenated Attribute per grouping) (Vendor Name: %name% Vendor URL: %url%)
vendor_fixes.url	
exploitation_consequence	Attribute: "Exploitation Consequence"
exploit_rating	N/A
mitigations	Attribute: "Mitigations"
cvss_base_score	Attribute: "CVSS Base Score"
cvss_temporal_score	Attribute: "CVSS Temporal Score"
source.date	Attribute: "Source" (one concatenated Attribute per grouping) (Date: %date% </br> Description: %description% </br> Title: %title% </br> Urls: %urls% </br>)
source.title	
source.urls	
source.description	
previous_version.version_number	Attribute: "Previous Attributes" (one concatenated Attribute per grouping) (Version Number: %version_number% </br>
previous_versions.title	

previous_versions.publish_date	title: %title% </br> Publish Date: %publish_date% </br>)
technologies.vendor	Attribute: "Vulnerable CPE" (one concatenated Attribute per grouping) (Affected Vendor: %vendor% </br> Affected Technology: %technology_name% </br> Affected CPE Title: %cpe_title%</br> Affected CPE: %cpe%</br>)
technologies.cpe_title	
technologies.technology_name	
technologies.cpe	
vendor_fix_text	Attribute: "Vendor Fix"
executive_summary	N/A
attacking_ease	Tag: "Attacking Ease: %attacking_ease%"
exploitation_vectors	Attribute: "Exploitation Vector"
vulnerability_type	Attribute: "Vulnerability Type"
exploits.exploitUrl	Attribute: "Exploits" (one concatenated Attribute per grouping) (Description: %description% </br> Exploit URL: %exploit_url% </br> File Size: %file_size% </br>
exploits.description	
exploits.name	
exploits.releaseDate	

exploits.reliability	md5: %md5% </br> name: %name% </br> Release Date: %release_date% </br> Reliability: %reliability% </br>)
exploits.fileSize	
exploits.md5	
date_of_disclosure	Attribute: "Date of Disclosure"
access_vectors	Tag: "Access Vector: %access_vectors%"
access_complexity	Tag: "Access Complexity: %access_complexity%"
authentication	Tag: "Authentication: %authentication%"
confidentiality_impact	Tag: "Confidentiality Impact: %confidentiality_impact%"
integrity_impact	Tag: "Integrity Impact: %integrity_impact%"
availability_impact	Tag: "Availability Impact: %availability_impact%"
exploitability	Tag: "Exploitability: %exploitability%"
remediation	Tag: "Remediation: %remediation%"
report_confidence	Tag: "Report Confidence: %report_confidence%"
mitigation_details	Attribute: "Mitigation Details"

Vulnerabilities

ThreatConnect object type: Vulnerability Group

Table 4

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
name	Name/Summary
id	Attribute: "External ID"
description	Attribute: "Description"
title	Attribute: "Report Title"
risk_rating	Tag: "Risk Rating: %risk_rating%"
analysis	N/A
executive_summary	N/A
exploitation_vectors/{index}	Attribute: "Exploitation Vector"
exploitation_consequence	Attribute: "Exploitation Consequence"
exploitation_state	Tag: "Exploitation State: %exploitation_state%"
cwe	Tag: "CWE: %cwe%"
cve_id	Tag: "%cve_id%"
vulnerable_products	Attribute: "Vulnerable Products"

vendor_fix_references/{index}/url	Attribute: "Vendor Fix URL" (one concatenated Attribute per grouping) (Vendor: %name% </br> Fix URL: %url% </br></br>)
vendor_fix_references/{index}/name	
date_of_disclosure	Attribute: "Date of Disclosure"
observed_in_the_wild	Attribute: "Observe in Wild"
was_zero_day	N/A
last_modified_date	Attribute: "External Date Last Modified"
workarounds	N/A
publish_date	Attribute: "Report Publish Date"
available_mitigation/{index}	Attribute: "Mitigations"
sources/{index}/source_name	Attribute: "Source" (one concatenated Attribute per grouping) (Date: %date% </br> Description: %source_description% </br> Name: %source_name% </br> URL: %url% </br>)
sources/{index}/source_description	
sources/{index}/date	
sources/{index}/url	
exploits/{index}	Attribute: "Exploits" (

	Description: %description% </br> Exploit URL: %exploit_url% </br> File Size: %file_size% </br> md5: %md5% </br> name: %name% </br> Release Date: %release_date% </br> Reliability: %reliability% </br> Replication URLs:%replication_urls% </br>)
associated_actors/{index}	Actor Association **Note**: Actor Association refers to the association between the Vulnerability Group object and the Intrusion Set Group object. Customers should expect to see the Actor information as a Group association on the Vulnerability Group's **Details** screen.
associated_malware/{index}	Malware Association **Note**: Malware Association refers to the association between the Vulnerability Group object and the Malware Group object. Customers should expect to see the Malware information as a Group association on the Vulnerability Group's **Details** screen.
associated_Reports/{index}	Reports Association **Note**: Reports Association refers to the association between the Vulnerability Group object and the Report Group object. Customers should expect to see the Report information as a Group association on the Vulnerability Group's **Details** screen.

vulnerable_cpes/{index}/vendor_name	Attribute: "Vulnerable CPE" (one concatenated Attribute per grouping) (Affected Vendor: %vendor_name% </br> Affected Product: %technology_name% </br> Affected CPE: %cpe% </br> Affected CPE Title: %cpe_title% </br>) Tag: "Affected Product: %technology_name%"
vulnerable_cpes/{index}/technology_name	
vulnerable_cpes/{index}/cpe	
vulnerable_cpes/{index}/cpe_title	
common_vulnerability_scores	N/A
common_vulnerability_scores/v2.0/attack_complexity	Tag: "Attack Complexity v2: %attack_complexity%"
common_vulnerability_scores/v2.0/base_score	Attribute: "CVSS Score v2": %base_score% Tag: "CVSS Score v2: %base_score%"
common_vulnerability_scores/v2.0/vector_string	Tag: "Vector String v2: %vector_string%"
common_vulnerability_scores/v2.0/integrity_impact	Tag: "Integrity Impact v2: %integrity_impact%"
common_vulnerability_scores/v2.0/report_confidence	Tag: "Report Confidence v2: %report_confidence%"
common_vulnerability_scores/v2.0/attack_vector	Tag: "Attack Vector v2: %attack_vector%"
common_vulnerability_scores/v2.0/privileges_required	Tag: "Privileges Required v2: %privileges_required%"

common_vulnerability_scores/v2.0/availability_impact	Tag: "Availability Impact v2: %availability_impact%"
common_vulnerability_scores/v2.0/temporal_score	Attribute: "CVSS v2 Temporal Score": %temporal_score% Tag: "CVSS Temporal Score v2: %temporal_score%"
common_vulnerability_scores/v2.0/exploit_code_maturity	Tag: "Exploit Code Maturity v2: %exploit_code_maturity%"
common_vulnerability_scores/v2.0/user_interaction	Tag: "User Interaction v2: %user_interaction%"
common_vulnerability_scores/v2.0/scope	Tag: "Scope v2: %scope%"
common_vulnerability_scores/v2.0/confidentiality_impact	Tag: "Confidentiality Impact v2: %confidentiality_impact%"
common_vulnerability_scores/v2.0/remediation_level	Tag: "Remediation Level v2: %remediation_level%"
common_vulnerability_scores/v3	N/A
common_vulnerability_scores/v3.1/attack_complexity	Tag: "Attack Complexity v3: %attack_complexity%"
common_vulnerability_scores/v3.1/base_score	Attribute: "CVSS Score v3": %base_score% Tag: "CVSS Score v3: %base_score%"
common_vulnerability_scores/v3.1/vector_string	Tag: "Vector String v3: %vector_string%"
common_vulnerability_scores/v3.1/integrity_impact	Tag: "Integrity Impact v3: %integrity_impact%"

common_vulnerability_scores/v3.1/report_confidence	Tag: "Report Confidence v3: %report_confidence%"
common_vulnerability_scores/v3.1/attack_vector	Tag: "Attack Vector v3: %attack_vector%"
common_vulnerability_scores/v3.1/privileges_required	Tag: "Privileges Required v3: %privileges_required%"
common_vulnerability_scores/v3.1/availability_impact	Tag: "Availability Impact v3: %availability_impact%"
common_vulnerability_scores/v3.1/temporal_score	Attribute: "CVSS v3 Temporal Score": %temporal_score% Tag: "CVSS Temporal Score v3: %temporal_score%"
common_vulnerability_scores/v3.1/exploit_code_maturity	Tag: "Exploit Code Maturity v3: %exploit-code_maturity%"
common_vulnerability_scores/v3.1/user_interaction	Tag: "User Interaction v3: %user_interaction%"
common_vulnerability_scores/v3.1/scope	Tag: "Scope v3: %scope%"
common_vulnerability_scores/v3.1/confidentiality_impact	Tag: "Confidentiality Impact v3: %confidentiality_impact%"
common_vulnerability_scores/v3.1/remediation_level	Tag: "Remediation Level v3: %remediation_level%"

Actors

ThreatConnect object type: Intrusion Set Group

Table 5

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
name	Name/Summary
description	Attribute: "Description"
id	Attribute: "External ID"
intel_free	N/A
aliases[*].name	Attribute: "Aliases"
aliases[*].attribution_scope	N/A
last_updated	Attribute: "External Date Last Modified"
motivations[*].id	N/A
motivations[*].name	Attribute: "Adversary Motivation Type"
motivations[*].attribution_scope	N/A
industries[*].id	N/A
industries[*].name	Attribute: "Targeted Industry Sector"
industries[*].attribution_scope	N/A
observed[*].earliest	Attribute: "First Seen"

observed[*].recent	Attribute: "Last Seen"
observed[*].attribution_scope	N/A
malware[*].id	Attribute: "External ID" (Malware Association) **Note**: Malware Association refers to the association between the Intrusion Set Group object and the Malware Group object. Customers should expect to see the Malware information as a Group association on the Intrusion Set Group's **Details** screen.
malware[*].name	N/A
malware[*].attribution_scope	N/A
locations.source.region.id	N/A
locations.source.region.name	Attribute: "Source Location" (concatenated) (%region.name%.%sub_region.name%)
locations.source.region.attribution_scope	N/A
locations.source.sub_region.id	N/A
locations.source.sub_region.name	N/A
locations.source.sub_region.attribution_scope	N/A

location.source.country.id	N/A
location.source.country.name	Attribute: "Origin Country"
location.source.country.iso2	N/A
location.source.country.attribution_scope	N/A
locations.target[*].id	N/A
locations.target[*].name	Attribute: "Target Country"
locations.target[*].iso2	N/A
locations.target[*].attribution_scope	N/A
cve[*].id	N/A (Vulnerability Association) **Note**: Vulnerability Association refers to the association between the Intrusion Set Group object and the Vulnerability Group object. Customers should expect to see the Vulnerability information as a Group association on the Intrusion Set Group's **Details** screen.
cve[*].name	Tag
cve[*].attribution_scope	N/A
associated_uncs[*].id	N/A
associated_uncs[*].name	Attribute: "Additional Analysis & Context"
associated_uncs[*].attribution_scope	Associated UNCs: %s: %s (name, attribution_scope)

last_activity_time	Attribute: "Last Seen"
audience[?(@.name=='tlp_marking')].license	Security Label
audience[*].name	N/A
audience[*].license	N/A
counts.reports	N/A
counts.malware	N/A
counts.cve	N/A
counts.associated_uncs	N/A
counts.aliases	N/A
counts.industries	N/A

Malware

ThreatConnect object type: Malware Group

Table 6

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
malware[*].name	Name/Summary
malware[*].description	Attribute: "Description"
malware[*].id	Attribute: "External ID"
malware[*].intel_free	N/A

malware[*].aliases[*].name	Attribute: "Aliases"
malware[*].last_updated	Attribute: "External Date Last Modified"
malware[*].has_yara	N/A
malware[*].roles	N/A

Malware Details

ThreatConnect object type: Malware Group

Table 7

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
id	Attribute: "External ID"
name	Name/Summary
description	Attribute: "Description"
intel_free	N/A
last_updated	Attribute: "External Date Last Modified"
operating_systems/{index}	Attribute: "Operating System"
inherently_malicious	N/A
aliases[*].name	Attribute: "Aliases" (comma delimited)
capabilities/{index}	Attribute: "Capabilities"
industries[*].name	Attribute: "Targeted Industry Sector"

industries[*].id	N/A
detections/{index}	Attribute: "Detections"
roles/{index}	Attribute: "Roles"
actors/{index}/id	N/A
actors/{index}/name	Tag: "%name%"
actors/{index}/country_name	N/A
actors/{index}/iso2	N/A
cve	Tag: "%cve%"
yara.id	Attribute: "Yara" (one concatenated Attribute per grouping) (ID: %id% </br> Name: %name% </br>) Tag: "Yara:%name%"
yara.name	
audience/{index}/name	N/A
audience/{index}/license	N/A
counts/{index}/reports	N/A
counts/{index}/malware	N/A
counts/{index}/cve	N/A

counts/{index}/associated_uncs	N/A
counts/{index}/aliases	N/A
counts/{index}/industries	N/A

Malware Families

ThreatConnect object type: Malware Group

Table 8

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
malware/{index}/id	N/A
malware/{index}/name	Name/Summary; Tag
malware/{index}/attribution_scope	N/A

Attack Patterns

ThreatConnect object type: Attack Pattern Group

Table 9

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
attack-pattern[*].name	Name/Summary
attack-pattern[*].description	Attribute: "Description"
attack-pattern[*].id	Attribute: "External ID"
attack-pattern[*].intel_free	N/A

attack-pattern[*].attack_pattern_identifier	Attribute: "Attack Pattern Identifier"
attack-pattern[*].last_updated	Attribute: "External Date Last Modified"
attack-pattern[*].tactic_name	Attribute: "Tactic Name"

Attack Pattern Details

ThreatConnect object type: Attack Pattern Group

Table 10

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
created	N/A
name	Name/Summary
attack_pattern_identifier	Attribute: "Attack Pattern Identifier"
description	Attribute: "Description"
id	Attribute: "External ID"

Indicators

ThreatConnect object type: Indicators (all types)

Table 11

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
id	Attribute: "External ID"
name	Name/Summary
indicators[*].last_updated	Attribute: "External Date Last Modified"
indicators[*].first _seen	Attribute: "First Seen"
indicators[*].last_seen	Attribute: "Last Seen"
indicators[*].sources.first_seen	Attribute: "Source" (one concatenated Attribute per grouping) (First Seen: %first_seen% </br> Last Seen: %last_seen% </br> Osint: %osint% </br> Category: %category% </br> Source Name: %source_name% </br>)
indicators[*].sources.last_seen	
indicators[*].sources.osint	
indicators[*].sources.category	
indicators[*].sources.source_name	
indicators[*].mscore	Confidence Rating **Note**: See the "Mandiant Indicator Confidence Score (Mscore) Mappings" section for more information on how the Mandiant Indicator Confidence score

	(Mscore) is mapped to Threat and Confidence Ratings in ThreatConnect.
indicators[*].attributed_associations.id	N/A
indicators[*].attributed_associations.name	N/A (Malware and Actor Group Association) **Note**: Malware and Actor Group Association refers to the association between the Indicator object and the Malware and Intrusion Set Group objects. Customers should expect to see the Malware and Intrusion Set information as Group associations on the Indicator's **Details** screen.
indicators[*].attributed_associations.type	N/A
indicators[*].id	N/A
indicators[*].type	Indicator Type
indicators[*].value	Attribute: "Indicator"
indicators[*].associated_hashes	N/A
reports/reports_id	Report Association **Note**: Report Association refers to the association between the Indicator object and the Report Group object. Customers should expect to see the Report information as Group associations on the Indicator's **Details** screen.

campaign/id	Campaign Association **Note**: Campaign Association refers to the association between the Indicator object and the Campaign Group object. Customers should expect to see the Campaign information as Group associations on the Indicator's **Details** screen.

Campaign

ThreatConnect object type: Campaign Group

Table 12

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
campaign.id	Attribute: "External ID"
campaign.name	Name/Summary
campaign.short_name	Tag: "%short_name%"

Campaign Details

ThreatConnect object type: Campaign Group

Table 13

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
campaign.id	Attribute: "External ID"
campaign.name	Name/Summary
campaign.description	Attribute: "Description"

campaign.campaign_type	Attribute: "Campaign Type"
campaign.short_name	Tag: "%short_name%"
campaign.last_activity_time	Attribute: "External Date Last Modified"
campaign.audience[?(@.name=='tlp_marking')].license	Security Label
campaign.timeline.name	Attribute: "Timeline" (one concatenated Attribute per grouping) (Name: %name% Description: %description% Event Type: %event_type% Timestamp: %timestamp%)
campaign.timeline.description	
campaign.timeline.releasable	
campaign.timeline.event_type	
campaign.aliases.actor	Attribute: "Aliases " (one concatenated Attribute per grouping) (id: %name% Name: %description% Source: %event_type% Resource:%source% (i.e., the source from which the aliases originated))
campaign.aliases.malware	
campaign.aliases.campaign	
campaign.malware.id	Malware Association **Note**: Malware Association refers to the association between the Campaign Group object and the Malware Group

	object. Customers should expect to see the Malware information as a Group association on the Campaign Group's **Details** screen.
campaign.vulnerabilities.id	Tag: "%cve_id%" Vulnerabilities Association **Note**: Vulnerabilities Association refers to the association between the Campaign Group object and the Vulnerability Group object. Customers should expect to see the Vulnerability information as a Group association on the Campaign Group's **Details** screen.
campaign.industries.name	Attribute: "Target Industry Sector"
campaign.target_locations.countries.name	Attribute: "Target Country"
campaigns.target_locations.regions_name	Attribute: "Region"
campaign.target_locations.sub_regions_name	Attribute: "Sub-Region"

Campaign Reports

ThreatConnect object type: Report Group

Table 14

Mandiant Advantage Threat Intelligence API Field	ThreatConnect Field
reports.id	Attribute: "External ID" Report to Campaign Association **Note**: Report to Campaign Association refers to the association between the Report Group object and the Campaign Group object. Customers should expect to see the Campaign information as a Group association on the Report Group's **Details** screen.
reports.report_id	Attribute: "Report Id"
reports.title	Attribute: "Report Title"
reports.published_date	Attribute: "Report Published Date"
reports.report_type	Attribute: "Report Type"
reports.version	Attribute: "Version"
reports.audience_name	Tag: "Audience: %name%"

Mandiant Indicator Confidence Score (Mscore) Mappings

The Mandiant Indicator Confidence score (Mscore) conveys the confidence in the Indicator being benign or malicious. This score ranges from 0 to 100, where 0 indicates high confidence in the Indicator being benign and 100 indicates high confidence in the Indicator being malicious. In ThreatConnect, Mscore is mapped to an Indicator's Threat and Confidence Ratings.

Table 15

Mandiant Mscore	ThreatConnect Threat Rating	ThreatConnect Confidence Rating
0	0	100
1	0	98
2	0	96
3	0	94
4	0	92
5	0	90
6	0	88
7	0	86
8	0	84
9	0	82
10	0	80

11	0	78
12	0	76
13	0	74
14	0	72
15	0	70
16	0	68
17	0	66
18	0	64
19	0	62
20	0	60
21	0	58
22	0	56
23	0	54
24	0	52
25	0	50
26	0	48
27	0	46
28	0	44

29	0	42
30	0	40
31	0	38
32	0	36
33	0	34
34	0	32
35	0	30
36	0	28
37	0	26
38	0	24
39	0	22
40	0	20
41	0	18
42	0	16
43	0	14
44	0	12
45	0	10
46	0	8

47	0	6
48	0	4
49	0	2
50	0	0
51	2	2
52	2	4
53	2	6
54	2	8
55	2	10
56	2	12
57	2	14
58	2	16
59	2	18
60	3	20
61	3	22
62	3	24
63	3	26
64	3	28

65	3	30
66	3	32
67	3	34
68	3	36
69	3	38
70	3	40
71	3	42
72	3	44
73	3	46
74	3	48
75	3	50
76	3	52
77	3	54
78	3	56
79	3	58
80	4	80
81	4	81
82	4	82

83	4	83
84	4	84
85	4	85
86	4	86
87	4	87
88	4	88
89	4	89
90	5	90
91	5	91
92	5	92
93	5	93
94	5	94
95	5	95
96	5	96
97	5	97
98	5	98
99	5	99
100	5	100