Integration Technical Specifications

Intel 471 Malware Intelligence

Table of Contents

[Versioning 2](#_Toc25089534)

[Introduction 3](#_Toc25089535)

[Objective 3](#_Toc25089536)

[Contact 3](#_Toc25089537)

[Audience (internal) 3](#_Toc25089538)

[Audience (external under NDA) 3](#_Toc25089539)

[Overview 4](#_Toc25089540)

[User Story Definition 4](#_Toc25089541)

[Third Party Overview 5](#_Toc25089542)

[High Level Design and resources (Product Manager) 6](#_Toc25089543)

[Low Level Design and resources (development / QA teams) 7](#_Toc25089544)

[General specifications 7](#_Toc25089545)

[Assumptions 8](#_Toc25089546)

[Data Modelling 9](#_Toc25089547)

[Malware Intelligence Report and Indicator Feed 9](#_Toc25089548)

[Malware Intelligence YARA Feed 14](#_Toc25089549)

# Overview

## User Story Definition

|  |  |
| --- | --- |
| Extension Name | Intel 471 Malware Intelligence |
| Extension Description | The Intel 471 Malware intelligence extension is focused on the provision of high fidelity and timely indicators with rich context, TTP information and malware intelligence reports. |
| User Story | The malware intelligence feed provides the analyst with up to date indicators such as malware hashes, domains and IPs. These are provided with appropriate structure giving context around the malware indicator, helping to enable the analyst. For example, a malware hash will have a structure surrounding it that provides the analyst with the Malware Variant and its associated intel471 malware report. |
| Extension Type | INCOMING FEED |
| EDK Support | 0.x |

## 

## Third Party Overview

|  |  |
| --- | --- |
| Provider Name | Intel471 |
| Provider Description | Intel471 is a premier provider of cybercrime intelligence, providing adversary and malware centric intelligence. They deliver intelligence to leading security, fraud and intelligence organizations. Their team is comprised of intelligence operators and native speakers located where cybercriminals formerly operated with impunity and without consequence. |
| Product Name | Intel 471 Malware Intelligence |
| Product Description | Intel 471 Malware intelligence leverages their adversary intelligence and underground capabilities to provide timely data and context on malware and adversary infrastructure. |
| Company URL | https://intel471.com/ |
| Product URL | https://api.intel471.com/v1/ |
| Documentation URL | https://titan.intel471.com/api/docs/ |

# 

# Low Level Design and resources (development / QA teams)

## General specifications

|  |  |
| --- | --- |
| Transport type | REST |
| Content type | JSON / Form-Encoded |
| Expected processing time | N/A |
| 3rd party product API timeout | The API has a daily quota. This times the user out for a set period. See docs for more information |
| 3rd party product API specifics | Their default limit of returned entries is 10. This can be increased to a maximum of 100 using the count parameter. To return more data see the official documentation under the “Result paging, offset and count” section. |
| Integration platform configuration | N/A |
| How to check the integration is working (from the GUI) | N/A |

## Assumptions

* The user has obtained an API key for their own configuration.
* The user has obtained a username for their own configuration

# 

# Data Modelling

## Malware Intelligence Report and Indicator Feed

|  |  |
| --- | --- |
| Feed Name | Intel471 Malware Intelligence Indicator Feed |
| Feed Description | The Intel471 Malware Intelligence Feed provides the provision of timely indicators, with associated TTP information and malware intelligence reports in a structured format. |
| Feed Identifier | The “uid” field in the Malware Indicator endpoint |
| Feed Endpoints | Malware Intelligence Malware Reports Search by FamilyUID Endpoint   * https://api.intel471.com/v1/malwareReports?malwareFamilyProfileUid   =<malware\_family\_profile\_uid>  Malware Intelligence Indicator Search   * https://api.intel471.com/v1/indicators?indicator=\* |
| Technical Overview | |
| This feed will require multiple API calls to receive the relevant data to structure. Below gives a flow of the API calls:   * First call the Malware Intelligence Indicator Search endpoint using the URL above * This will return a list of indicators up to the limit * Map the feed using the structure below * Then call the Malware Intelligence Malware Reports Search endpoint using the URL above and the “malware\_family\_profile\_uid” field from the indicator endpoint to find the associated indicator and reports. | |
| Data Modelling Description | |
| Overview:   * Map entitles information source reference to their endpoint call + UID field   + E.g. Malware Indicator = https://api.intel471.com/v1/indicators?indicator= dce85f0c7a4b0a04d31f8c0e7e166ab6 * The producer / information source roles field should be set to “Initial Author”   Report:   * Create the report from the “title” field with “Intel 471 - <type>   + E.g. Intel 471 – Lokibot * The report Intents field should be set to “Malware Characterization” * See mapping below   TTP:   * A malware variant TTP will be created from the “family” field with a 6-digit UUID.   + E.g. Malware Variant: Lokibot f88ca2 * A malware family TTP will be created from the “family” field (if this doesn’t already exist in the platform).   + Malware: Lokibot * Both the malware variant and malware TTP entity should have their Characteristics à Behaviour à Malware à Names mapped to the “family” field * Call the associated malware report endpoint using the description above. * See mapping below   Indicator:   * An indicator will be created from the fields within the “indicator\_data” field. * Some URL indicators come with an IP address and port (e.g. [http://123.123.123.123:8080](http://123.123.123.123:8080/)). * When this occurs add a “/” to the end of the indicator title and URI observable. * Also, you will need to create the following. It will use the example above:   + Indicator Title = <http://123.123.123.123:8080/>   + URI observable = <http://123.123.123.123:8080/>   + IPv4 observable = 123.123.123.123   + Port observable = 8080 * The port observable will be safe. The others will use be mapped how every other observable maliciousness is mapped. * The indicator type will be determined from the “indicator\_type” field.   + File = File Hash Watchlist (md5 = md5 for example)   + For hashes there might be multiple indicators. Create an indicator from one then create the others as hash-type extracts (e.g. sha256 = 256 extract)   + IPv4 = IP Watchlist   + URL = URL Watchlist   + Domain = Domain Watchlist   + Indicator will need to take their tags from the report they are associated with. * Indicator extracts will be taken from the “indicator\_data” field (the same value as the indicator title). The extract confidence will be mapped to the data.confidence field * The extract type will be determined by the “indicator\_type” field:   + File = (relevant hash extract type)   + URL = Uri   + IPv4 = Ipv4   + Domain = Domain * If “command\_and\_control” in “mitre\_tactics” field, then add “C2” to IP, Domain and URL indicator types. * The “indicator\_data.file.type” field from the indicator json will be fomratted as “Type: <type>” in its associated indicators analysis section. * See mapping below   Relationships   * Indicator à Malware variant * Malware Variant à Malware * Malware à Report | |
| Response (Malware Intelligence Indicator) | |
| {  "indicatorTotalCount": 1,  "indicators": [{  "data": {  "confidence": "medium",  "expiration": 1560660937000,  "context": {  "description": "lokibot controller URL"  },  "threat": {  "uid": "22e7a5f41d4f3cc5c704758ffa505556",  "type": "malware",  "data": {  "family": "lokibot",  "malware\_family\_profile\_uid": "20eb1f82621001883ea0c2085aff5729",  "version": "1.8"  }  },  "mitre\_tactics": "command\_and\_control”  "intel\_requirements": ["1.1.5", "1.1.6"],  "indicator\_type": "url”,  "indicator\_data": {  "url": "http://alphastand.top/alien/fre.php”  }  },  "meta": {  "version": "0.1"  },  "last\_updated": 1558068945543,  "uid": "dce85f0c7a4b0a04d31f8c0e7e166ab6",  "activity": {  "first": 1533883250000,  "last": 1558068937000  }  }]  } | |
| Data Mapping (Malware Intelligence Indicator) | |
| {  “indicatorTotalCount”: 1,  “indicators”: [{  “data”: {  “confidence”: “<Indicator Confidence> <Indicator extract maliciousness>”,  “expiration”: <Indicator + Malware Variant Estimated Threat End Time>,  “context”: {  “description”: “<Indicator Description>”  },  “threat”: {  “uid”: “<Potentially use to stop duplication of entities>”,  “type”: “<Indicator + Malware Variant Tag>”,  “data”: {  “family”: “<Malware Family> <Malware Variant + 6-digit UUID><Malware Variant Characteristics Malware field> <Indicator Tag> <Malware Variant Tag>”,  “malware\_family\_profile\_uid”: “<Use to link to malware intelligence report>”,  “version”: “1.8”  }  },  “mitre\_tactics”: “<Indicator type watchlist (When it equals to “command and control”)>”  “intel\_requirements”: [“<Indicator + Malware Variant Tag (See Appendix A for mapping)>”, “<Indicator + Malware Variant Tag (See Appendix A for mapping)>”],  “indicator\_type”: “<Indicator Type Watchlist>”,  “indicator\_data”: {  “url”: “<Indicator Title> <Indicator extract title (Extract type depends on indicator type)>”  “type”: “<Indicator Analysis>”  “download\_url”: “<Indicator Producer References>”  }  },  “meta”: {  “version”: “0.1”  },  “last\_updated”: 1558068945543,  “uid”: “<Indicator Producer Reference> <Malware Variant Information Source Reference>”,  “activity”: {  “first”: <Indicator + Malware Variant Estimated Observed Time> <Indicator + Malware Variant Threat start time>,  “last”:  }  }]  } | |
| Response (Malware Intelligence Malware Report) | |
| {  "malwareReportTotalCount": 1,  "malwareReports": [{  "data": {  "threat": {  "uid": "20eb1f82621001883ea0c2085aff5729",  "type": "malware",  "data": {  "family": "lokibot",  "malware\_family\_profile\_uid": "20eb1f82621001883ea0c2085aff5729"  }  },  "malware\_report\_data": {  "text": "(loki pws.zip)</p>",  "released\_at": 1536246010000,  "title": "LokiBot"  }  },  "meta": {  "version": "0.1"  },  "last\_updated": 1555343290418,  "uid": "7b29fd15bab5b686e148728f5d01c2ec",  "activity": {  "first": 1555343290000,  "last": 1555343290000  }  }]  } | |
| Data Modelling (Malware Intelligence Malware Report) | |
| {  "malwareReportTotalCount": 1,  "malwareReports": [{  "data": {  "threat": {  "uid": "20eb1f82621001883ea0c2085aff5729",  "type": "<Report + Malware Family TTP tag> <Report title>",  "data": {  "family": "<Report + Malware Family TTP Tag>",  "malware\_family\_profile\_uid": "20eb1f82621001883ea0c2085aff5729"  }  },  "malware\_report\_data": {  "text": <Report Analysis>,  "released\_at": <Report Estimated Observed Time> <Malware Family TTP Estimated Observed Time>,  "title": "<Report Title>"  }  },  "meta": {  "version": "0.1"  },  "last\_updated": 1555343290418,  "uid": "<Report Information Source References> <Malware Family TTP Information Source References>",  "activity": {  "first": <Report Estimated Threat Start Time> <Malware Family TTP Estimated Threat Start TIme>,  "last":  }  }]  } | |
| Desired Graph Visualisation | |
| A close up of a map  Description automatically generated | |

## Malware Intelligence YARA Feed

|  |  |
| --- | --- |
| Feed Name | Malware Intelligence YARA |
| Feed Description | The Intel471 Malware Intelligence YARA feed provides the provision of timely rules, with associated TTP information and malware intelligence reports in a structured format. |
| Feed Identifier | The “uid” field |
| Feed Endpoints | Malware Intelligence Malware Reports Search by FamilyUID Endpoint   * <https://api.intel471.com/v1/malwareReports?malwareFamilyProfileUid>   =<malware\_family\_profile\_uid>  Malware Intelligence YARA search   * https://api.intel471.com/v1/yara?threatType=malware |
| Technical Overview | |
| This feed will require multiple API calls to receive the relevant data to structure. Below gives a flow of the API calls:   * First call the Malware Intelligence YARA Search endpoint using the URL above * This will return a list YARA rules up to the limit (see High Level Design and Resources section) * Loop through every entry within this endpoint, mapping the data using the structure below   Then call the Malware Intelligence Malware Reports Search endpoint using the URL above and the “malware\_family\_profile\_uid” field from the YARA endpoint to find the associated YARA rule and reports. | |
| Data Modelling Description | |
| Overview:   * Use the Malware Intelligence Reports Search endpoint with the “malware\_family\_profile\_uid” field to grab the correct report. * The producer / information source roles field should be set to “Initial Author” * Map entitles information source reference to their endpoint call with the “yara=” filter + threat UID field   + E.g. Malware Indicator = https://api.intel471.com/v1/yara?threatuid=45c17dfa1b60fb295f377836da5454c5   Report:   * Create the report from the “title” field with “Intel 471 - <type>   + E.g. Intel 471 – Lokibot * The report Intents field should be set to “Malware Characterization” * (Use the report mapping in the previous section)   TTP:   * A malware variant TTP will be created from the “family” field with a 6-digit UUID.   + E.g. Malware Variant: ZeusPanda f88ca2 * A malware family TTP will be created from the “family” field if this doesn’t already exist in the platform.   + Malware: ZeusPanda * Both the malware variant and malware TTP entity should have their Characteristics à Behaviour à Malware à Names mapped to the “family” field. * See mapping below   Indicator:   * An indicator will be created from the title field combined with “YARA Rule:”   + E.g. YARA Rule: ZeusPanda * The “signature” field will be mapped to the Characteristics à Test mechanism à Signature (rule) * The Type field in the Characteristics à Test mechanism à should also be set to YARA * Indicator Types field should be set to “Malware Artifacts” * See Appendix B to see the Characteristics  Test Mechanism Producer mapping   Relationships   * Indicator à Malware variant * Malware Variant à Malware * Malware à Report | |
| Response (Malware Intelligence YARA) | |
| {  "yaraTotalCount": 3,  "yaras": [{  "data": {  "confidence": "high",  "yara\_data": {  "title": "arkei",  "signature": "rule arkei\n{\n meta: \n author = \"Intel 471\"\n strings:\n $config = \"/server/grubConfig\" fullword ascii\n $gate = \"/server/gate\" fullword ascii\n $arkei = \"Arkei\"\n $filezilla1 = \"\\\\files\\\\filezilla\_recentservers.xml\" fullword\n $filezilla2 = \"\\\\files\\\\filezilla\_sitemanager.xml\" fullword\n $info\_log = \"files\\\\information.log\"\n $passwords\_log = \"files\\\\passwords.log\" fullword wide\n $stats1 = \"MachineID: %s\"\n $stats2 = \"Windows Username: %s\"\n $stats3 = \"Videocard: %s\" \n $desktop = \"Desktop.zip\"\n $ipgeo1 = \"http://ip-api.com/line/?fields=countryCode\" fullword wide\n $ipgeo2 = \"http://ip-api.com/line/?fields=query\" fullword wide\n\n condition:\n uint16(0) == 0x5a4d and (all of them)\n}\n"  },  "threat": {  "data": {  "family": "arkei",  "malware\_family\_profile\_uid": "45c17dfa1b60fb295f377836da5454c5"  },  "type": "malware",  "uid": "45c17dfa1b60fb295f377836da5454c5"  },  "intel\_requirements": ["1.1.5", "1.1.6"]  },  "meta": {  "version": "0.1"  },  "last\_updated": 1553964714670,  "uid": "048fe252afced217d487600349355bbc",  "activity": {  "first": 1550066320000,  "last": 1550066320000  } | |
| Data Mapping (Malware Intelligence YARA) | |
| {  "yaraTotalCount": 3,  "yaras": [{  "data": {  "confidence": "<Indicator Confidence>",  "yara\_data": {  "title": "<Indicator Title>",  "signature": "<Indicator Characteristics à Test mechanism à Signature (rule)>"  },  "threat": {  "data": {  "family": “<Malware Family> <Malware Variant + 6-digit UUID><Malware Variant Characteristics Malware field> <Indicator + Malware variant Tag>”,  "malware\_family\_profile\_uid": "<Use to link to malware intelligence report>”  },  "type": <Indicator + malware variant Tag>,  "uid": "45c17dfa1b60fb295f377836da5454c5"  },  "intel\_requirements": ["<Indicator + Malware Variant Tag (See Appendix A for mapping)>", " <Indicator + Malware Variant Tag (See Appendix A for mapping)> "]  },  "meta": {  "version": "0.1"  },  "last\_updated": 1553964714670,  "uid": "048fe252afced217d487600349355bbc",  "activity": {  "first": <Indicator + Malware Variant Estimated Observed Time> <Indicator + Malware Variant Estimated Threat Start Time>,  "last":  } | |
| Desired Graph Visualisation | |
| A picture containing text, map  Description automatically generated | |

# Appendix A – Intelligence Requirements Formatting

|  |  |
| --- | --- |
| **Value** | **Mapping** |
| 1.1.1 Ransomware malware | Intelligence Requirement - Ransomware malware |
| 1.1.2 Mobile malware | Intelligence Requirement - Mobile malware |
| 1.1.3 Remote Access Trojan (RAT) malware | Intelligence Requirement - Remote Access Trojan (RAT) malware |
| 1.1.4 Banking trojan malware | Intelligence Requirement - Banking trojan malware |
| 1.1.5 Information stealer malware | Intelligence Requirement - Information stealer malware |
| 1.1.6 Loader malware | Intelligence Requirement - Loader malware |
| 1.1.7 Botnet malware | Intelligence Requirement - Botnet malware |
| 1.1.8 Worm malware | Intelligence Requirement - Worm malware |
| 1.1.9 Point-Of-Sale (PoS) malware | Intelligence Requirement - Point-Of-Sale (PoS) malware |
| 1.1.10 ATM malware | Intelligence Requirement - ATM malware |
| 1.1.11 Internet of Things (IoT) malware | Intelligence Requirement - Internet of Things (IoT) malware |
| 1.1.12 Denial of Service (DoS) malware | Intelligence Requirement - Denial of Service (DoS) malware |
| 1.1.13 Proxy malware | Intelligence Requirement - Proxy malware |
| 1.1.14 Destructive malware | Intelligence Requirement - Destructive malware |
| 1.1.15 Cryptomining malware | Intelligence Requirement - Cryptomining malware |
| 1.1.16 Formgrabber, Web Inject, Automatic Transfer Systems (ATS) malware | Intelligence Requirement - Formgrabber, Web Inject, Automatic Transfer Systems (ATS) malware |
| 1.2.1 Multifunctional Malware-as-a-Service (MaaS) platforms | Intelligence Requirement - Multifunctional Malware-as-a-Service (MaaS) platforms |
| 1.2.2 Crypter/FUD services | Intelligence Requirement - Crypter/FUD services |
| 1.2.3 Anti/Counter-AV services | Intelligence Requirement - Anti/Counter-AV services |
| 1.2.4 Ransomware-as-a-Service (RaaS) | Intelligence Requirement - Ransomware-as-a-Service (RaaS) |
| 1.2.5 Spamming services | Intelligence Requirement - Spamming services |
| 1.2.6 DoS/booter/stresser services | Intelligence Requirement - DoS/booter/stresser services |
| 1.2.7 Rogue Code Signing certificate providers | Intelligence Requirement - Rogue Code Signing certificate providers |
| 1.2.8 Rogue Web certificate providers | Intelligence Requirement - Rogue Web certificate providers |
| 1.3.1 Malware install providers | Intelligence Requirement - Malware install providers |
| 1.3.2 Malvertising | Intelligence Requirement - Malvertising |
| 2.1.1 Operating System (OS) vulnerabilities | Intelligence Requirement - Operating System (OS) vulnerabilities |
| 2.1.1.1 Desktop/Server OS vulnerabilities | Intelligence Requirement - Desktop/Server OS vulnerabilities |
| 2.1.1.2 Mobile OS vulnerabilities | Intelligence Requirement - Mobile OS vulnerabilities |
| 2.1.2 Software and web application vulnerabilities | Intelligence Requirement - Software and web application vulnerabilities |
| 2.1.2.1 Web browser vulnerabilities | Intelligence Requirement - Web browser vulnerabilities |
| 2.1.2.2 Office / productivity software vulnerabilities | Intelligence Requirement - Office / productivity software vulnerabilities |
| 2.1.2.3 Open source software library vulnerabilities | Intelligence Requirement - Open source software library vulnerabilities |
| 2.1.3 Protocol vulnerabilities | Intelligence Requirement - Protocol vulnerabilities |
| 2.1.4 Server platform vulnerabilities | Intelligence Requirement - Server platform vulnerabilities |
| 2.1.4.1 Database server vulnerabilities | Intelligence Requirement - Database server vulnerabilities |
| 2.1.4.2 Web server vulnerabilities | Intelligence Requirement - Web server vulnerabilities |
| 2.1.4.3 Email server vulnerabilities | Intelligence Requirement - Email server vulnerabilities |
| 2.1.4.4 Content management server vulnerabilities | Intelligence Requirement - Content management server vulnerabilities |
| 2.1.5 Network appliance / endpoint vulnerabilities | Intelligence Requirement - Network appliance / endpoint vulnerabilities |
| 2.1.6 Cloud computing / storage vulnerabilities | Intelligence Requirement - Cloud computing / storage vulnerabilities |
| 2.1.7 Hardware vulnerabilities | Intelligence Requirement - Hardware vulnerabilities |
| 2.1.8 Other platform vulnerabilities | Intelligence Requirement - Other platform vulnerabilities |
| 2.1.8.1 Transportation controls vulnerabilities | Intelligence Requirement - Transportation controls vulnerabilities |
| 2.1.8.2 Industrial controls systems vulnerabilities | Intelligence Requirement - Industrial controls systems vulnerabilities |
| 2.1.8.3 IoT-related vulnerabilities | Intelligence Requirement - IoT-related vulnerabilities |
| 2.1.8.4 Healthcare systems related vulnerabilities | Intelligence Requirement - Healthcare systems related vulnerabilities |
| 2.2.1 Exploit Proof-of-concept (PoC) code | Intelligence Requirement - Exploit Proof-of-concept (PoC) code |
| 2.2.2 Exploit kits | Intelligence Requirement - Exploit kits |
| 3.1.1 Bulletproof Hosting (BPH) services | Intelligence Requirement - Bulletproof Hosting (BPH) services |
| 3.1.2 Proxy services | Intelligence Requirement - Proxy services |
| 3.1.3 Domain registrar services | Intelligence Requirement - Domain registrar services |
| 3.1.4 Botnet services | Intelligence Requirement - Botnet services |
| 4.1.1 Cash-out services | Intelligence Requirement - Cash-out services |
| 4.1.2 Money laundering and exchange services | Intelligence Requirement - Money laundering and exchange services |
| 4.1.3 Money mule accounts and networks | Intelligence Requirement - Money mule accounts and networks |
| 4.1.4 Bank account drops and fund transfers | Intelligence Requirement - Bank account drops and fund transfers |
| 4.1.5 Prepaid cards / gift cards | Intelligence Requirement - Prepaid cards / gift cards |
| 4.1.6 Travel fraud | Intelligence Requirement - Travel fraud |
| 4.1.7 Hospitality fraud | Intelligence Requirement - Hospitality fraud |
| 4.1.8 Tax fraud | Intelligence Requirement - Tax fraud |
| 4.1.9 CEO/CFO fraud / Business Email Compromise (BEC) | Intelligence Requirement - CEO/CFO fraud / Business Email Compromise (BEC) |
| 4.1.10 Documentation fraud | Intelligence Requirement - Documentation fraud |
| 4.1.11 Insurance fraud | Intelligence Requirement - Insurance fraud |
| 4.2.1 Compromised payment cards (CVVs, fullz, dumps) | Intelligence Requirement - Compromised payment cards (CVVs, fullz, dumps) |
| 4.2.2 Compromised account credentials | Intelligence Requirement - Compromised account credentials |
| 4.2.3 Compromised Personally Identifiable Information (PII) | Intelligence Requirement - Compromised Personally Identifiable Information (PII) |
| 4.2.4 Compromised Intellectual Property (IP) | Intelligence Requirement - Compromised Intellectual Property (IP) |
| 4.3.1 Call center services | Intelligence Requirement - Call center services |
| 4.3.2 Account checking services | Intelligence Requirement - Account checking services |
| 4.3.3 Brute force tools | Intelligence Requirement - Brute force tools |
| 4.3.3.1 Credential stuffing | Intelligence Requirement - Credential stuffing |
| 4.4.1 Phishing | Intelligence Requirement - Phishing |
| 4.4.2 Spearphishing | Intelligence Requirement - Spearphishing |
| 4.4.3 Vishing | Intelligence Requirement - Vishing |
| 4.4.4 Social media scams | Intelligence Requirement - Social media scams |
| 4.4.5 Smishing | Intelligence Requirement - Smishing |
| 5.1.1 Reconaissance & information gathering (Att&ck) | Intelligence Requirement - Reconaissance & information gathering (Att&ck) |
| 5.1.2 Weaponization (Att&ck) | Intelligence Requirement - Weaponization (Att&ck) |
| 5.1.3 Delivery (Att&ck) | Intelligence Requirement - Delivery (Att&ck) |
| 5.2.1 Initial Access (Att&ck) | Intelligence Requirement - Initial Access (Att&ck) |
| 5.2.2 Execution (Att&ck) | Intelligence Requirement - Execution (Att&ck) |
| 5.2.3 Persistence (Att&ck) | Intelligence Requirement - Persistence (Att&ck) |
| 5.2.4 Privilege Escalation (Att&ck) | Intelligence Requirement - Privilege Escalation (Att&ck) |
| 5.2.5 Defense Evasion (Att&ck) | Intelligence Requirement - Defense Evasion (Att&ck) |
| 5.2.6 Credential Access (Att&ck) | Intelligence Requirement - Credential Access (Att&ck) |
| 5.2.7 Discovery (Att&ck) | Intelligence Requirement - Discovery (Att&ck) |
| 5.2.8 Lateral Movement (Att&ck) | Intelligence Requirement - Lateral Movement (Att&ck) |
| 5.2.9 Collection (Att&ck) | Intelligence Requirement - Collection (Att&ck) |
| 5.2.10 Exfiltration (Att&ck) | Intelligence Requirement - Exfiltration (Att&ck) |
| 5.2.11 Command and Control (Att&ck) | Intelligence Requirement - Command and Control (Att&ck) |
| 5.3.1 Denial of Service (DoS) attacks | Intelligence Requirement - Denial of Service (DoS) attacks |
| 5.3.2 Injection attacks | Intelligence Requirement - Injection attacks |
| 5.3.3 Website defacements | Intelligence Requirement - Website defacements |
| 5.3.4 Brute Force Attacks | Intelligence Requirement - Brute Force Attacks |
| 5.4.1 ATM attacks: skimming, shimming, jackpotting | Intelligence Requirement - ATM attacks: skimming, shimming, jackpotting |
| 5.4.2 PoS attacks: skimming | Intelligence Requirement - PoS attacks: skimming |
| 5.4.3 Physical sabotage of network / system | Intelligence Requirement - Physical sabotage of network / system |
| 5.5 Insider threats | Intelligence Requirement - Insider threats |
| 5.6.1 Espionage | Intelligence Requirement - Espionage |
| 5.6.2 Outsider trading | Intelligence Requirement - Outsider trading |
| 5.6.3 Information or data breach | Intelligence Requirement - Information or data breach |
| 6.1.1 Consumer & Industrial Products | Intelligence Requirement - Consumer & Industrial Products |
| 6.1.1.1 Consumer Business | Intelligence Requirement - Consumer Business |
| 6.1.1.2 Aviation & Transportation | Intelligence Requirement - Aviation & Transportation |
| 6.1.1.3 Consumer Products | Intelligence Requirement - Consumer Products |
| 6.1.1.4 Sports & Leisure | Intelligence Requirement - Sports & Leisure |
| 6.1.1.5 Hospitality | Intelligence Requirement - Hospitality |
| 6.1.1.6 Restaurants & Food Service | Intelligence Requirement - Restaurants & Food Service |
| 6.1.1.7 Retail, Wholesale & Distribution | Intelligence Requirement - Retail, Wholesale & Distribution |
| 6.1.2 Energy & Resources | Intelligence Requirement - Energy & Resources |
| 6.1.2.1 Oil. Gas, and Consumable Fuels | Intelligence Requirement - Oil. Gas, and Consumable Fuels |
| 6.1.2.2 Power & Utilities | Intelligence Requirement - Power & Utilities |
| 6.1.2.3 Shipping & Ports | Intelligence Requirement - Shipping & Ports |
| 6.1.2.4 Water | Intelligence Requirement - Water |
| 6.1.3 Financial Services | Intelligence Requirement - Financial Services |
| 6.1.3.1 Banking & Securities | Intelligence Requirement - Banking & Securities |
| 6.1.3.2 Insurance | Intelligence Requirement - Insurance |
| 6.1.3.3 Investment Management | Intelligence Requirement - Investment Management |
| 6.1.4 Life Sciences & Health Care | Intelligence Requirement - Life Sciences & Health Care |
| 6.1.4.1 Health Care Providers and Services | Intelligence Requirement - Health Care Providers and Services |
| 6.1.4.2 Health Care Equipment and Technology | Intelligence Requirement - Health Care Equipment and Technology |
| 6.1.4.3 Pharmaceuticals, Biotechnology and Life Sciences | Intelligence Requirement - Pharmaceuticals, Biotechnology and Life Sciences |
| 6.1.5 Manufacturing | Intelligence Requirement - Manufacturing |
| 6.1.5.1 Aerospace & Defense | Intelligence Requirement - Aerospace & Defense |
| 6.1.5.2 Automotive | Intelligence Requirement - Automotive |
| 6.1.5.3 Industrial Products & Services | Intelligence Requirement - Industrial Products & Services |
| 6.1.5.4 Chemicals & Specialty Materials | Intelligence Requirement - Chemicals & Specialty Materials |
| 6.1.6 Public Sector | Intelligence Requirement - Public Sector |
| 6.1.6.1 International Government | Intelligence Requirement - International Government |
| 6.1.6.2 National Government | Intelligence Requirement - National Government |
| 6.1.6.3 Regional Government | Intelligence Requirement - Regional Government |
| 6.1.6.4 Education | Intelligence Requirement - Education |
| 6.1.6.5 Public Safety | Intelligence Requirement - Public Safety |
| 6.1.6.6 Military and Defense | Intelligence Requirement - Military and Defense |
| 6.1.7 Real Estate | Intelligence Requirement - Real Estate |
| 6.1.7.1 Engineering and Construction Industry | Intelligence Requirement - Engineering and Construction Industry |
| 6.1.7.2 Real Estate Fund and Investor | Intelligence Requirement - Real Estate Fund and Investor |
| 6.1.7.3 REIT and Property Company | Intelligence Requirement - REIT and Property Company |
| 6.1.7.4 Real Estate Management, Brokerage, and Service Provider | Intelligence Requirement - Real Estate Management, Brokerage, and Service Provider |
| 6.1.7.5 Tenants and Occupiers | Intelligence Requirement - Tenants and Occupiers |
| 6.1.8 Technology, Media & Telecommunications | Intelligence Requirement - Technology, Media & Telecommunications |
| 6.1.8.1 Technology | Intelligence Requirement - Technology |
| 6.1.8.2 Media & Entertainment | Intelligence Requirement - Media & Entertainment |
| 6.1.8.3 Communications | Intelligence Requirement - Communications |
| 6.1.8.4 Internet of Things | Intelligence Requirement - Internet of Things |
| 6.1.9 Professional Services & Consulting | Intelligence Requirement - Professional Services & Consulting |
| 6.1.9.1 IT/Technology Consulting | Intelligence Requirement - IT/Technology Consulting |
| 6.1.9.2 Management & Operations Consulting | Intelligence Requirement - Management & Operations Consulting |
| 6.1.9.3 Financial & Investment Consulting | Intelligence Requirement - Financial & Investment Consulting |
| 6.1.9.4 Human Resources Consulting | Intelligence Requirement - Human Resources Consulting |
| 6.1.9.5 Marketing & Sales Consulting | Intelligence Requirement - Marketing & Sales Consulting |
| 6.1.9.6 Law Services & Consulting | Intelligence Requirement - Law Services & Consulting |
| 6.1.9.7 Political Consulting | Intelligence Requirement - Political Consulting |
| 6.1.9.8 Physical Security Consulting | Intelligence Requirement - Physical Security Consulting |
| 6.2.1 Africa | Intelligence Requirement - Africa |
| 6.2.2 Asia | Intelligence Requirement - Asia |
| 6.2.3 Central America | Intelligence Requirement - Central America |
| 6.2.4 Europe | Intelligence Requirement - Europe |
| 6.2.5 European Union | Intelligence Requirement - European Union |
| 6.2.6 Middle East | Intelligence Requirement - Middle East |
| 6.2.7 North America | Intelligence Requirement - North America |
| 6.2.8 Oceania | Intelligence Requirement - Oceania |
| 6.2.9 South America | Intelligence Requirement - South America |
| 6.2.10 The Caribbean | Intelligence Requirement - The Caribbean |

# Appendix B – YARA Rule Indicator Characteristics / Test Mechanism / Producer mapping

