# Analytical Results of a Cyber Threat Intelligence Survey

Ryan Trost

THREATQUOTIENT

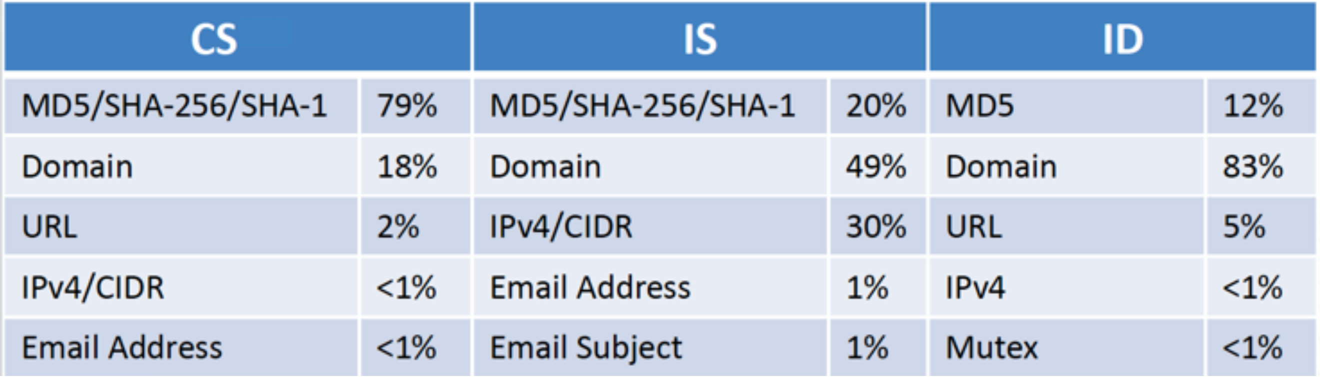
# whoami()

- Ryan Trost, Co-Founder of ThreatQuotient
- "…career SOC-dweller" - sysAdmin > security analyst > IR > SOC Mgr
- SOC Ops Manager - General Dynamics & several USG
- *Author of "Practical Intrusion Analysis"  © 2009*
- Developed a geospatial intrusion detection model
- Security Conference lectures include
  - DEFCON16, SANS, BlackHat 2014, ISACA ISRM, InfoSec World
- Chairman, Technical Advisory Board – Cyber Security AAS Collegiate program

# DISCLAIMER

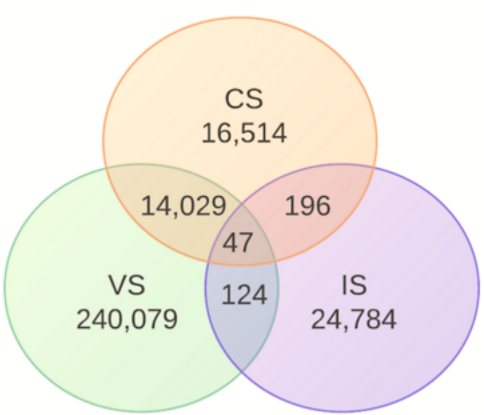
The views and opinions expressed in this presentation are those of the author and not of my Employer.

# Early vendor comparison triggered my fascination…

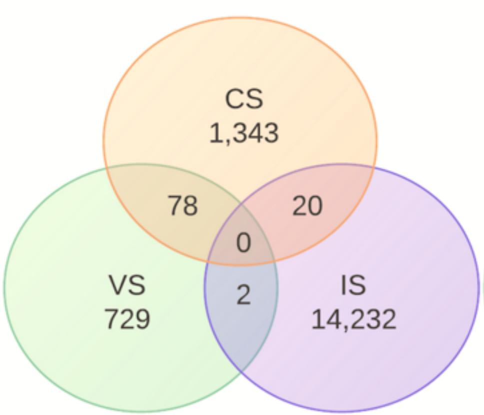


| CS | | IS | | ID | |
|---|---|---|---|---|---|
| MD5/SHA-256/SHA-1 | 79% | MD5/SHA-256/SHA-1 | 20% | MD5 | 12% |
| Domain | 18% | Domain | 49% | Domain | 83% |
| URL | 2% | IPv4/CIDR | 30% | URL | 5% |
| IPv4/CIDR | <1% | Email Address | 1% | IPv4 | <1% |
| Email Address | <1% | Email Subject | 1% | Mutex | <1% |

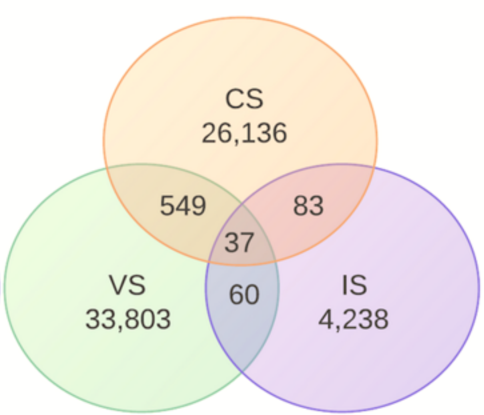
Domains



IP Address



MD5



Cite: Trost, Ryan: US Blackhat 2014

# Survey Purpose

Commercial Intel Providers lean on various requirements before publishing datapoints – what dictates those requirements?

- DEADEND question as commercial providers won't tell you

Flip the curiosity on its head by posing the question to the industry

- What IOC Types and supporting Attributes pose the most value/benefit?

# Methodology

- Identify the top ~20 IOC Types across intel providers

| | | | | |
|---|---|---|---|---|
| CIDR | FQDN | MD5 Hash | SHA-512 Hash | User-Agent |
| Email Address | Fuzzy Hash | Service Name | Registry Key | X.509 S/N |
| Email Subject | IP Address | SHA-1 Hash | URL | X.509 Subject |
| Filename | Mutex | SHA-256 Hash | URL Path | |

- Identify the top 35 TTPs [read: attributes] across intel providers

| | | | | | |
|---|---|---|---|---|---|
| ASN | Role | Compile Time | Motivation | Targeted Industry | CNC Name |
| File Size | First Seen | Domain Type | Intent | Targeted Geography | Malware Name |
| Packer | Last Seen | Email Address Type | Langauge | Malware Family | Malware Category |
| Port | Source of Information | IP Address Type | Adversary Group | Vector | Geolocation |
| Protocol | Confidence | Status | CVE | Attack Category | CVSS |
| Attack Country Origin | Threat/Risk Score | Severity | Impact | BotName | |

- Design a questionnaire long enough to have stability but short enough where swamped analysts will actually complete it…and speak to you again!

# Rating Scale – IOC TYPE

- Evaluate each IOC Type based on 3 characteristics
  - Strength – can it stand alone?
  - Deployment Versatility – how many detection technologies can it be deployed?
  - Burnability – how easy is it for the adversary to replenish/re-create?
- Scale 1-5 (5 = most valuable)
- 19 IOC Types * 3 scores = 57 answers…***a big ask of the participant***

***Calculate AVERAGES and results in a fascinating multi-tier prioritization***

# Rating Scale - TTP

- TTP needed to be easier/faster – in fear the analyst wouldn’t finish the survey!
- Assess each TTP
  1. No Value
  2. Poor Value
  3. Good Value
  4. Great Value
- A 4-option scale was strategic so participants could NOT be indifferent – and select the ‘middle’ option

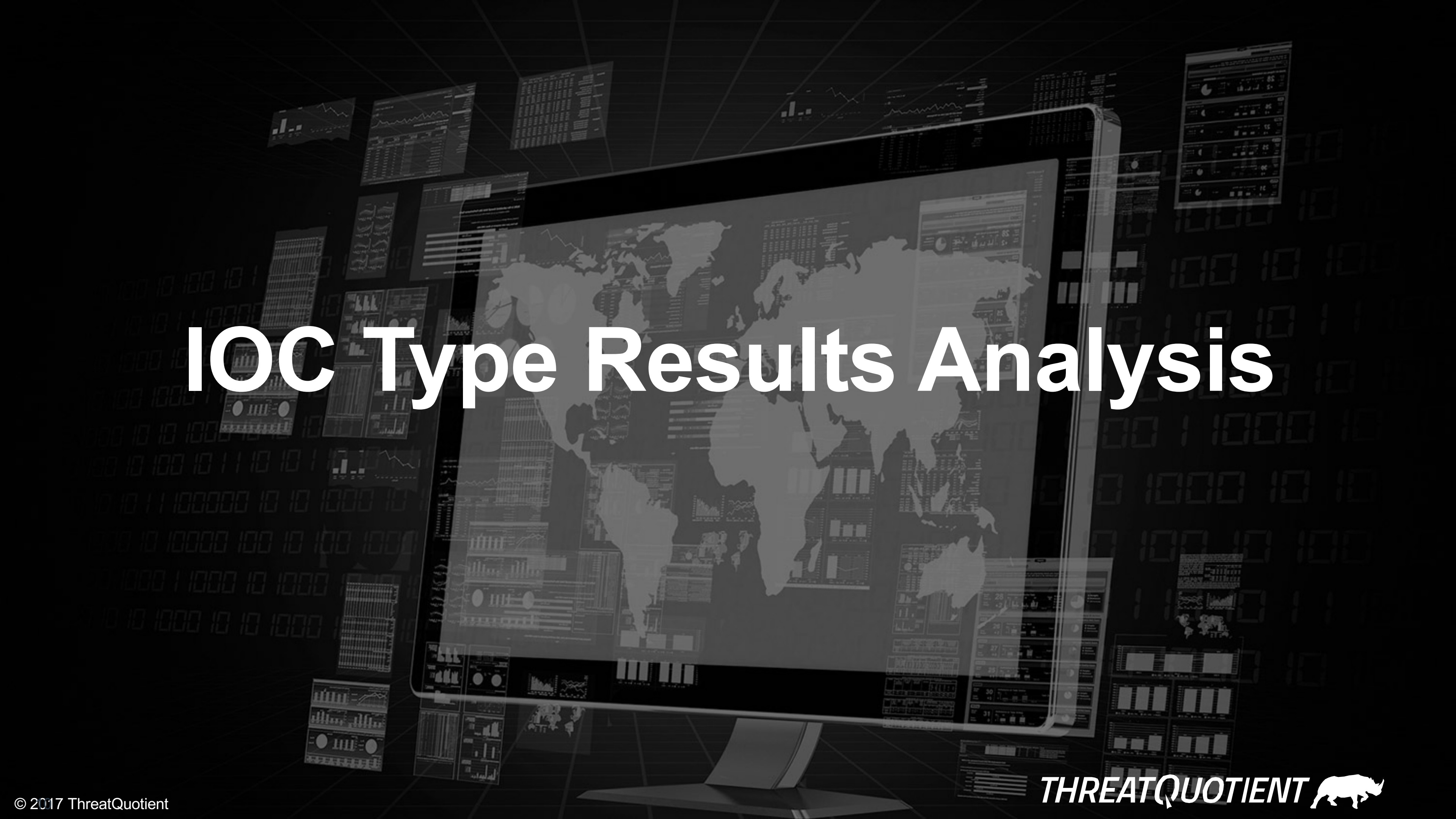
# Participant Breakdown

…by the numbers

| | | | |
|---|---|---|---|
| Security Analyst | 258 | Hunter | 36 |
| Incident Response | 124 | Malware | 34 |
| Intelligence Analyst | 94 | Other | 19 |

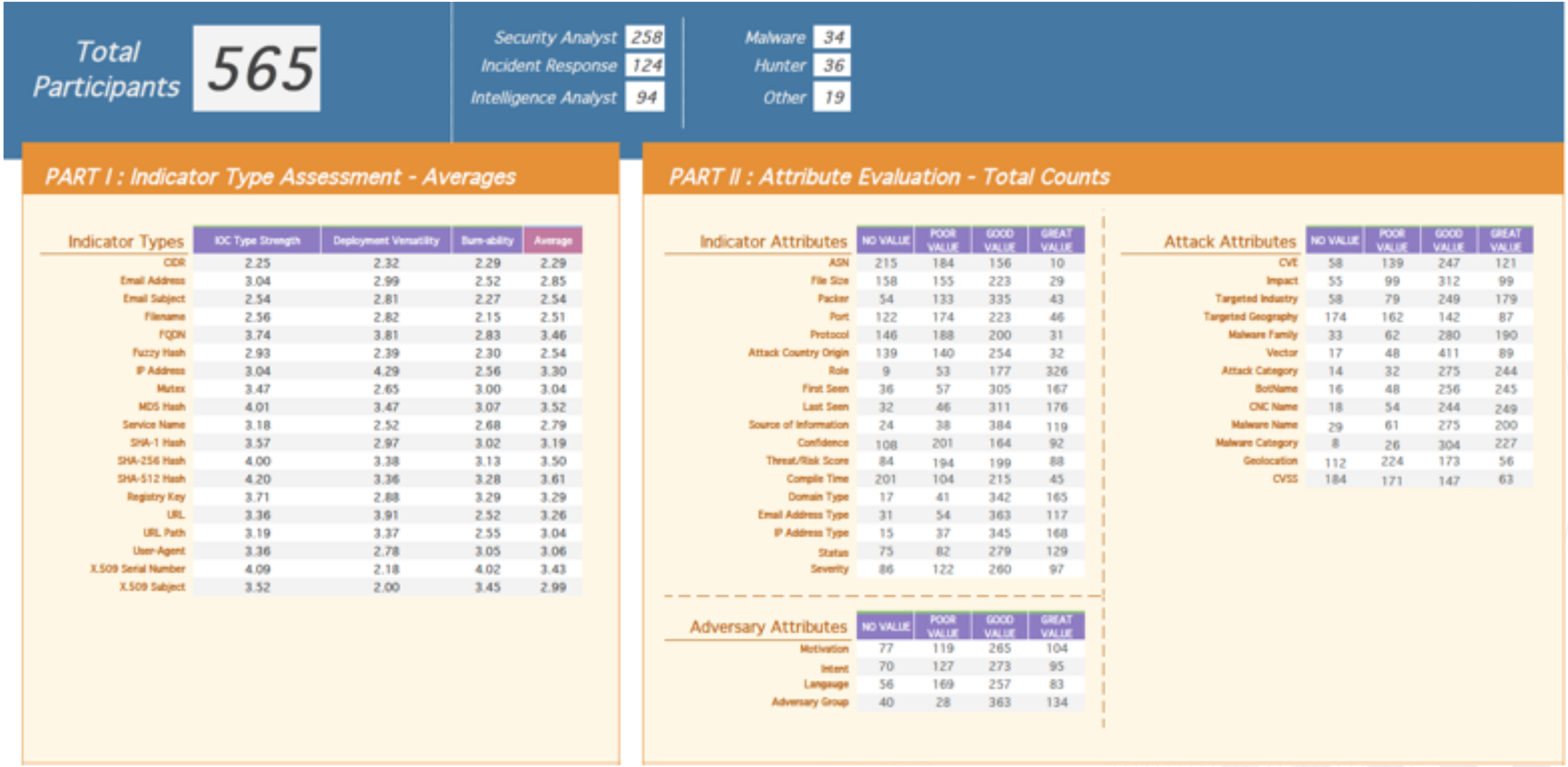
…by the percentage

| | | | |
|---|---|---|---|
| Security Analyst | 46% | Hunter | 6% |
| Incident Response | 22% | Malware | 6% |
| Intelligence Analyst | 17% | Other | 3% |



# IOC Type Results Analysis

# Overall Results



Total Participants **565**

| | |
|---|---|
| Security Analyst | 258 |
| Incident Response | 124 |
| Intelligence Analyst | 94 |
| Malware | 34 |
| Hunter | 36 |
| Other | 19 |

## PART I : Indicator Type Assessment - Averages

| Indicator Types | IOC Type Strength | Deployment Versatility | Burn-ability | Average |
|---|---|---|---|---|
| CIDR | 2.25 | 2.32 | 2.29 | 2.29 |
| Email Address | 3.04 | 2.99 | 2.52 | 2.85 |
| Email Subject | 2.54 | 2.81 | 2.27 | 2.54 |
| Filename | 2.56 | 2.82 | 2.15 | 2.51 |
| FQDN | 3.74 | 3.81 | 2.83 | 3.46 |
| Fuzzy Hash | 2.93 | 2.39 | 2.30 | 2.54 |
| IP Address | 3.04 | 4.29 | 2.56 | 3.30 |
| Mutex | 3.47 | 2.65 | 3.00 | 3.04 |
| MD5 Hash | 4.01 | 3.47 | 3.07 | 3.52 |
| Service Name | 3.18 | 2.52 | 2.68 | 2.79 |
| SHA-1 Hash | 3.57 | 2.97 | 3.02 | 3.19 |
| SHA-256 Hash | 4.00 | 3.38 | 3.13 | 3.50 |
| SHA-512 Hash | 4.20 | 3.36 | 3.28 | 3.61 |
| Registry Key | 3.71 | 2.88 | 3.29 | 3.29 |
| URL | 3.36 | 3.91 | 2.52 | 3.26 |
| URL Path | 3.19 | 3.37 | 2.55 | 3.04 |
| User-Agent | 3.36 | 2.78 | 3.05 | 3.06 |
| X.509 Serial Number | 4.09 | 2.18 | 4.02 | 3.43 |
| X.509 Subject | 3.52 | 2.00 | 3.45 | 2.99 |

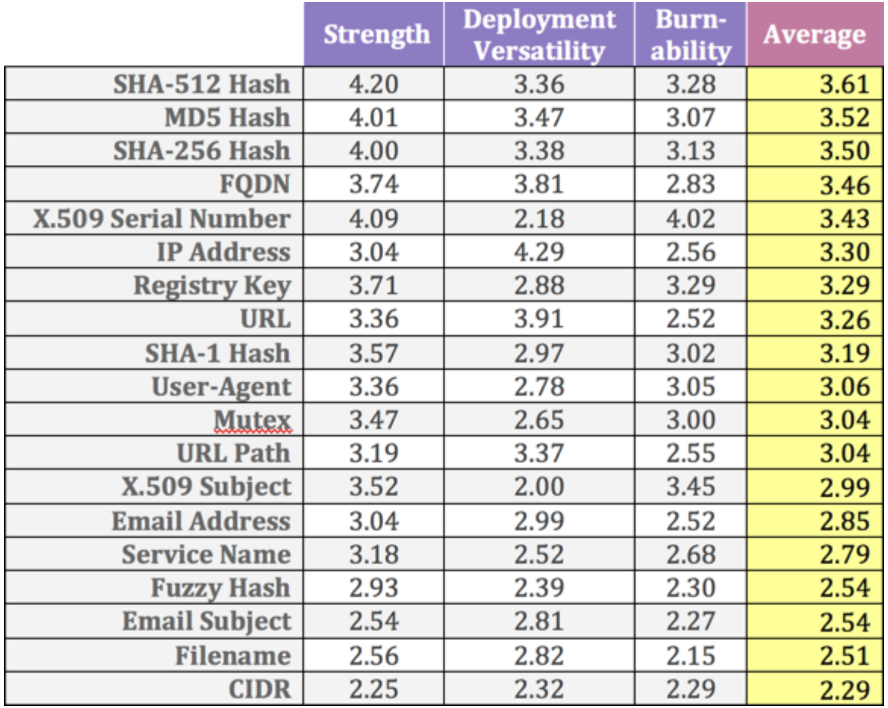
## PART II : Attribute Evaluation - Total Counts

| Indicator Attributes | NO VALUE | POOR VALUE | GOOD VALUE | GREAT VALUE |
|---|---|---|---|---|
| ASN | 215 | 184 | 156 | 10 |
| File Size | 158 | 155 | 223 | 29 |
| Packer | 54 | 133 | 335 | 43 |
| Port | 122 | 174 | 223 | 46 |
| Protocol | 146 | 188 | 200 | 31 |
| Attack Country Origin | 139 | 140 | 254 | 32 |
| Role | 9 | 53 | 177 | 326 |
| First Seen | 36 | 57 | 305 | 167 |
| Last Seen | 32 | 46 | 311 | 176 |
| Source of Information | 24 | 38 | 384 | 119 |
| Confidence | 108 | 201 | 164 | 92 |
| Threat/Risk Score | 84 | 194 | 199 | 88 |
| Compile Time | 201 | 104 | 215 | 45 |
| Domain Type | 17 | 41 | 342 | 165 |
| Email Address Type | 31 | 54 | 363 | 117 |
| IP Address Type | 15 | 37 | 345 | 168 |
| Status | 75 | 82 | 279 | 129 |
| Severity | 86 | 122 | 260 | 97 |

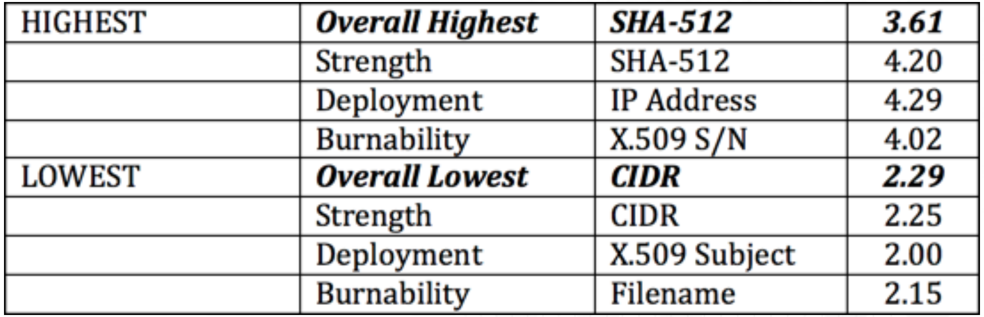
| Adversary Attributes | NO VALUE | POOR VALUE | GOOD VALUE | GREAT VALUE |
|---|---|---|---|---|
| Motivation | 77 | 119 | 265 | 104 |
| Intent | 70 | 127 | 273 | 95 |
| Language | 56 | 169 | 257 | 83 |
| Adversary Group | 40 | 28 | 363 | 134 |

| Attack Attributes | NO VALUE | POOR VALUE | GOOD VALUE | GREAT VALUE |
|---|---|---|---|---|
| CVE | 58 | 139 | 247 | 121 |
| Impact | 55 | 99 | 312 | 99 |
| Targeted Industry | 58 | 79 | 249 | 179 |
| Targeted Geography | 174 | 162 | 142 | 87 |
| Malware Family | 33 | 62 | 280 | 190 |
| Vector | 17 | 48 | 411 | 89 |
| Attack Category | 14 | 32 | 275 | 244 |
| BotName | 16 | 48 | 256 | 245 |
| CNC Name | 18 | 54 | 244 | 249 |
| Malware Name | 29 | 61 | 275 | 200 |
| Malware Category | 8 | 26 | 304 | 227 |
| Geolocation | 112 | 224 | 173 | 56 |
| CVSS | 184 | 171 | 147 | 63 |

# IOC Type Results - Overall



| | Strength | Deployment Versatility | Burn-ability | Average |
|---|---|---|---|---|
| SHA-512 Hash | 4.20 | 3.36 | 3.28 | 3.61 |
| MD5 Hash | 4.01 | 3.47 | 3.07 | 3.52 |
| SHA-256 Hash | 4.00 | 3.38 | 3.13 | 3.50 |
| FQDN | 3.74 | 3.81 | 2.83 | 3.46 |
| X.509 Serial Number | 4.09 | 2.18 | 4.02 | 3.43 |
| IP Address | 3.04 | 4.29 | 2.56 | 3.30 |
| Registry Key | 3.71 | 2.88 | 3.29 | 3.29 |
| URL | 3.36 | 3.91 | 2.52 | 3.26 |
| SHA-1 Hash | 3.57 | 2.97 | 3.02 | 3.19 |
| User-Agent | 3.36 | 2.78 | 3.05 | 3.06 |
| Mutex | 3.47 | 2.65 | 3.00 | 3.04 |
| URL Path | 3.19 | 3.37 | 2.55 | 3.04 |
| X.509 Subject | 3.52 | 2.00 | 3.45 | 2.99 |
| Email Address | 3.04 | 2.99 | 2.52 | 2.85 |
| Service Name | 3.18 | 2.52 | 2.68 | 2.79 |
| Fuzzy Hash | 2.93 | 2.39 | 2.30 | 2.54 |
| Email Subject | 2.54 | 2.81 | 2.27 | 2.54 |
| Filename | 2.56 | 2.82 | 2.15 | 2.51 |
| CIDR | 2.25 | 2.32 | 2.29 | 2.29 |



| | | | |
|---|---|---|---|
| HIGHEST | ***Overall Highest*** | ***SHA-512*** | ***3.61*** |
| | Strength | SHA-512 | 4.20 |
| | Deployment | IP Address | 4.29 |
| | Burnability | X.509 S/N | 4.02 |
| LOWEST | ***Overall Lowest*** | ***CIDR*** | ***2.29*** |
| | Strength | CIDR | 2.25 |
| | Deployment | X.509 Subject | 2.00 |
| | Burnability | Filename | 2.15 |

# IOC Type Result by Category

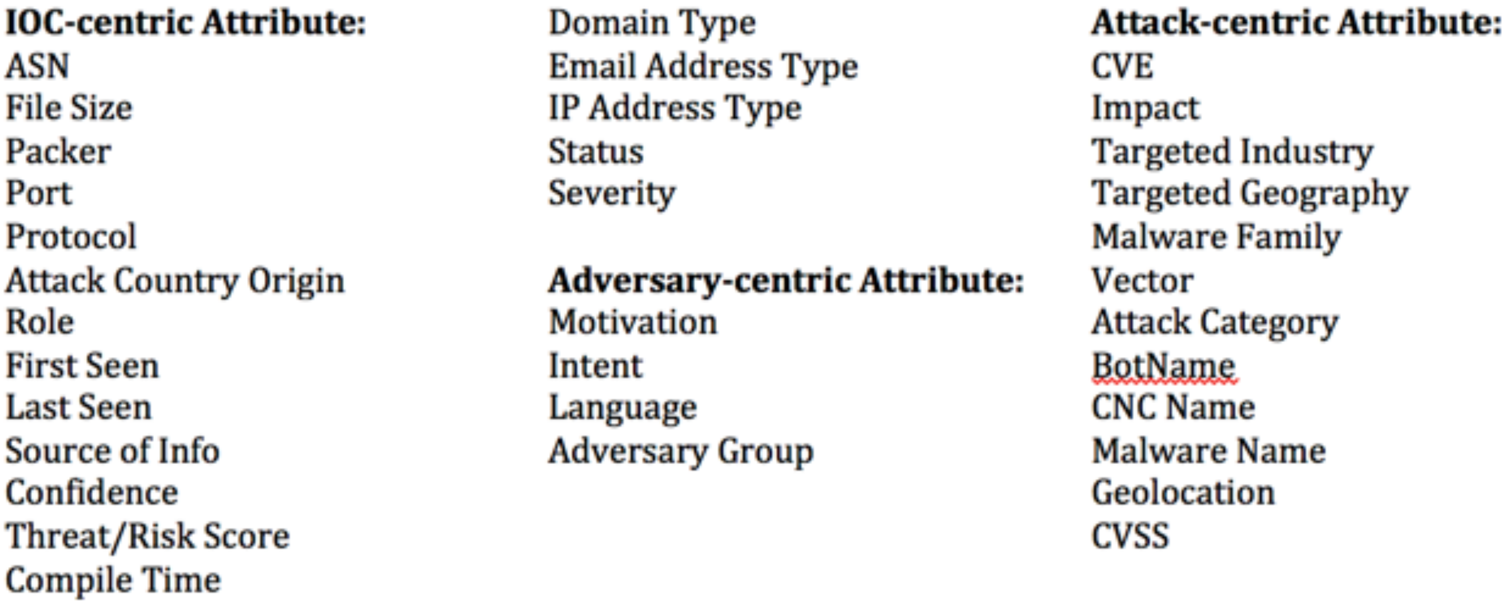
| IOC Type Strength Order | IOC Type Strength |
|---|---|
| SHA-512 Hash | 4.20 |
| X.509 Serial Number | 4.09 |
| MD5 Hash | 4.01 |
| SHA-256 Hash | 4.00 |
| FQDN | 3.74 |
| Registry Key | 3.71 |
| SHA-1 Hash | 3.57 |
| X.509 Subject | 3.52 |
| Mutex | 3.47 |
| URL | 3.36 |
| User-Agent | 3.36 |
| URL Path | 3.19 |
| Service Name | 3.18 |
| IP Address | 3.04 |
| Email Address | 3.04 |
| Fuzzy Hash | 2.93 |
| Filename | 2.56 |
| Email Subject | 2.54 |
| CIDR | 2.25 |

| Deployment Order | Deployment Versatility |
|---|---|
| IP Address | 4.29 |
| URL | 3.91 |
| FQDN | 3.81 |
| MD5 Hash | 3.47 |
| SHA-256 Hash | 3.38 |
| URL Path | 3.37 |
| SHA-512 Hash | 3.36 |
| Email Address | 2.99 |
| SHA-1 Hash | 2.97 |
| Registry Key | 2.88 |
| Filename | 2.82 |
| Email Subject | 2.81 |
| User-Agent | 2.78 |
| Mutex | 2.65 |
| Service Name | 2.52 |
| Fuzzy Hash | 2.39 |
| CIDR | 2.32 |
| X.509 Serial Number | 2.18 |
| X.509 Subject | 2.00 |

| Burnability Order | Burnability |
|---|---|
| X.509 Serial Number | 4.02 |
| X.509 Subject | 3.45 |
| Registry Key | 3.29 |
| SHA-512 Hash | 3.28 |
| SHA-256 Hash | 3.13 |
| MD5 Hash | 3.07 |
| User-Agent | 3.05 |
| SHA-1 Hash | 3.02 |
| Mutex | 3.00 |
| FQDN | 2.83 |
| Service Name | 2.68 |
| IP Address | 2.56 |
| URL Path | 2.55 |
| URL | 2.52 |
| Email Address | 2.52 |
| Fuzzy Hash | 2.30 |
| CIDR | 2.29 |
| Email Subject | 2.27 |
| Filename | 2.15 |

# Attribute Results Analysis

# List of TTPs/Attributes

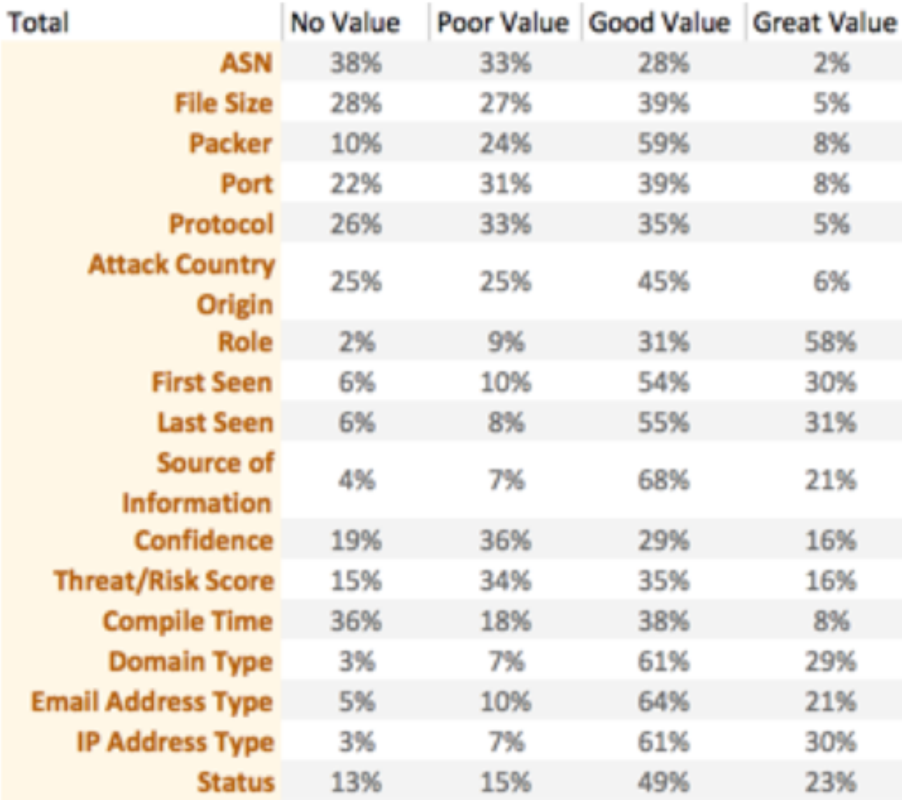


**IOC-centric Attribute:**
ASN
File Size
Packer
Port
Protocol
Attack Country Origin
Role
First Seen
Last Seen
Source of Info
Confidence
Threat/Risk Score
Compile Time
Domain Type
Email Address Type
IP Address Type
Status
Severity

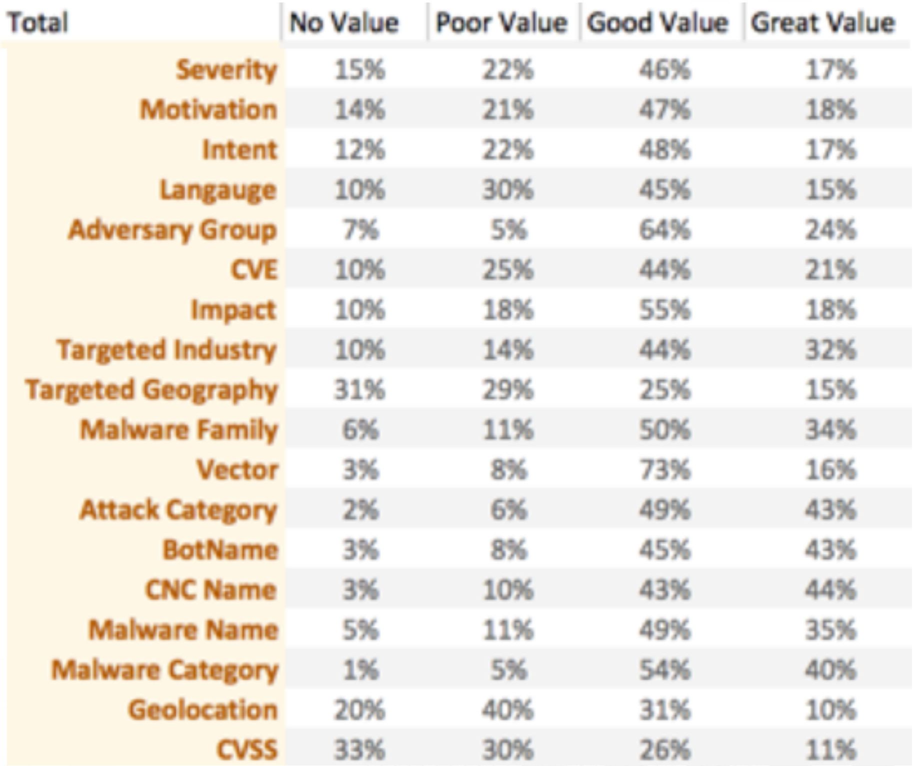
**Adversary-centric Attribute:**
Motivation
Intent
Language
Adversary Group

**Attack-centric Attribute:**
CVE
Impact
Targeted Industry
Targeted Geography
Malware Family
Vector
Attack Category
BotName
CNC Name
Malware Name
Geolocation
CVSS

# Attributes Results



| Total | No Value | Poor Value | Good Value | Great Value |
|---|---|---|---|---|
| ASN | 38% | 33% | 28% | 2% |
| File Size | 28% | 27% | 39% | 5% |
| Packer | 10% | 24% | 59% | 8% |
| Port | 22% | 31% | 39% | 8% |
| Protocol | 26% | 33% | 35% | 5% |
| Attack Country Origin | 25% | 25% | 45% | 6% |
| Role | 2% | 9% | 31% | 58% |
| First Seen | 6% | 10% | 54% | 30% |
| Last Seen | 6% | 8% | 55% | 31% |
| Source of Information | 4% | 7% | 68% | 21% |
| Confidence | 19% | 36% | 29% | 16% |
| Threat/Risk Score | 15% | 34% | 35% | 16% |
| Compile Time | 36% | 18% | 38% | 8% |
| Domain Type | 3% | 7% | 61% | 29% |
| Email Address Type | 5% | 10% | 64% | 21% |
| IP Address Type | 3% | 7% | 61% | 30% |
| Status | 13% | 15% | 49% | 23% |



| Total | No Value | Poor Value | Good Value | Great Value |
|---|---|---|---|---|
| Severity | 15% | 22% | 46% | 17% |
| Motivation | 14% | 21% | 47% | 18% |
| Intent | 12% | 22% | 48% | 17% |
| Langauge | 10% | 30% | 45% | 15% |
| Adversary Group | 7% | 5% | 64% | 24% |
| CVE | 10% | 25% | 44% | 21% |
| Impact | 10% | 18% | 55% | 18% |
| Targeted Industry | 10% | 14% | 44% | 32% |
| Targeted Geography | 31% | 29% | 25% | 15% |
| Malware Family | 6% | 11% | 50% | 34% |
| Vector | 3% | 8% | 73% | 16% |
| Attack Category | 2% | 6% | 49% | 43% |
| BotName | 3% | 8% | 45% | 43% |
| CNC Name | 3% | 10% | 43% | 44% |
| Malware Name | 5% | 11% | 49% | 35% |
| Malware Category | 1% | 5% | 54% | 40% |
| Geolocation | 20% | 40% | 31% | 10% |
| CVSS | 33% | 30% | 26% | 11% |

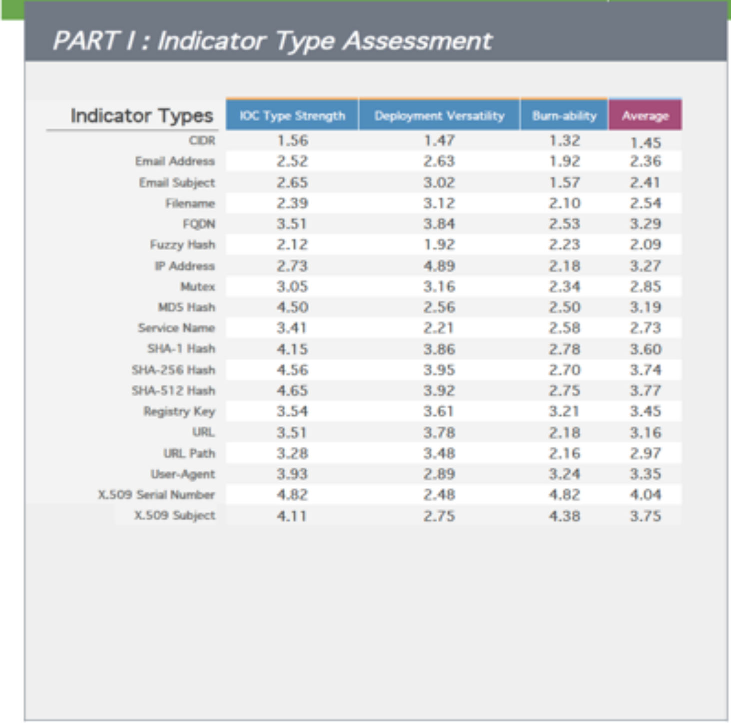
# Security Analyst Results Breakdown

# Security Analyst Results

*Role Summary*

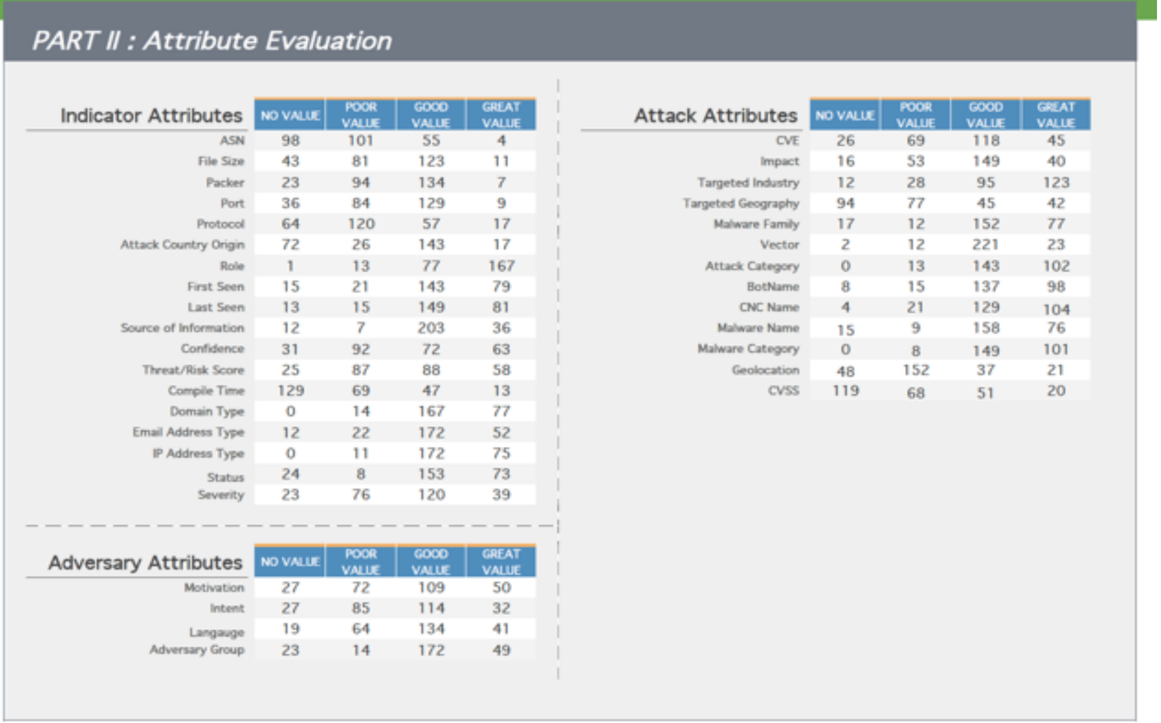
*Security Analyst*

*45.7 %* of partcipants



## *PART I : Indicator Type Assessment*

| Indicator Types | IOC Type Strength | Deployment Versatility | Burn-ability | Average |
|---|---|---|---|---|
| CIDR | 1.56 | 1.47 | 1.32 | 1.45 |
| Email Address | 2.52 | 2.63 | 1.92 | 2.36 |
| Email Subject | 2.65 | 3.02 | 1.57 | 2.41 |
| Filename | 2.39 | 3.12 | 2.10 | 2.54 |
| FQDN | 3.51 | 3.84 | 2.53 | 3.29 |
| Fuzzy Hash | 2.12 | 1.92 | 2.23 | 2.09 |
| IP Address | 2.73 | 4.89 | 2.18 | 3.27 |
| Mutex | 3.05 | 3.16 | 2.34 | 2.85 |
| MD5 Hash | 4.50 | 2.56 | 2.50 | 3.19 |
| Service Name | 3.41 | 2.21 | 2.58 | 2.73 |
| SHA-1 Hash | 4.15 | 3.86 | 2.78 | 3.60 |
| SHA-256 Hash | 4.56 | 3.95 | 2.70 | 3.74 |
| SHA-512 Hash | 4.65 | 3.92 | 2.75 | 3.77 |
| Registry Key | 3.54 | 3.61 | 3.21 | 3.45 |
| URL | 3.51 | 3.78 | 2.18 | 3.16 |
| URL Path | 3.28 | 3.48 | 2.16 | 2.97 |
| User-Agent | 3.93 | 2.89 | 3.24 | 3.35 |
| X.509 Serial Number | 4.82 | 2.48 | 4.82 | 4.04 |
| X.509 Subject | 4.11 | 2.75 | 4.38 | 3.75 |



## *PART II : Attribute Evaluation*

| Indicator Attributes | NO VALUE | POOR VALUE | GOOD VALUE | GREAT VALUE |
|---|---|---|---|---|
| ASN | 98 | 101 | 55 | 4 |
| File Size | 43 | 81 | 123 | 11 |
| Packer | 23 | 94 | 134 | 7 |
| Port | 36 | 84 | 129 | 9 |
| Protocol | 64 | 120 | 57 | 17 |
| Attack Country Origin | 72 | 26 | 143 | 17 |
| Role | 1 | 13 | 77 | 167 |
| First Seen | 15 | 21 | 143 | 79 |
| Last Seen | 13 | 15 | 149 | 81 |
| Source of Information | 12 | 7 | 203 | 36 |
| Confidence | 31 | 92 | 72 | 63 |
| Threat/Risk Score | 25 | 87 | 88 | 58 |
| Compile Time | 129 | 69 | 47 | 13 |
| Domain Type | 0 | 14 | 167 | 77 |
| Email Address Type | 12 | 22 | 172 | 52 |
| IP Address Type | 0 | 11 | 172 | 75 |
| Status | 24 | 8 | 153 | 73 |
| Severity | 23 | 76 | 120 | 39 |

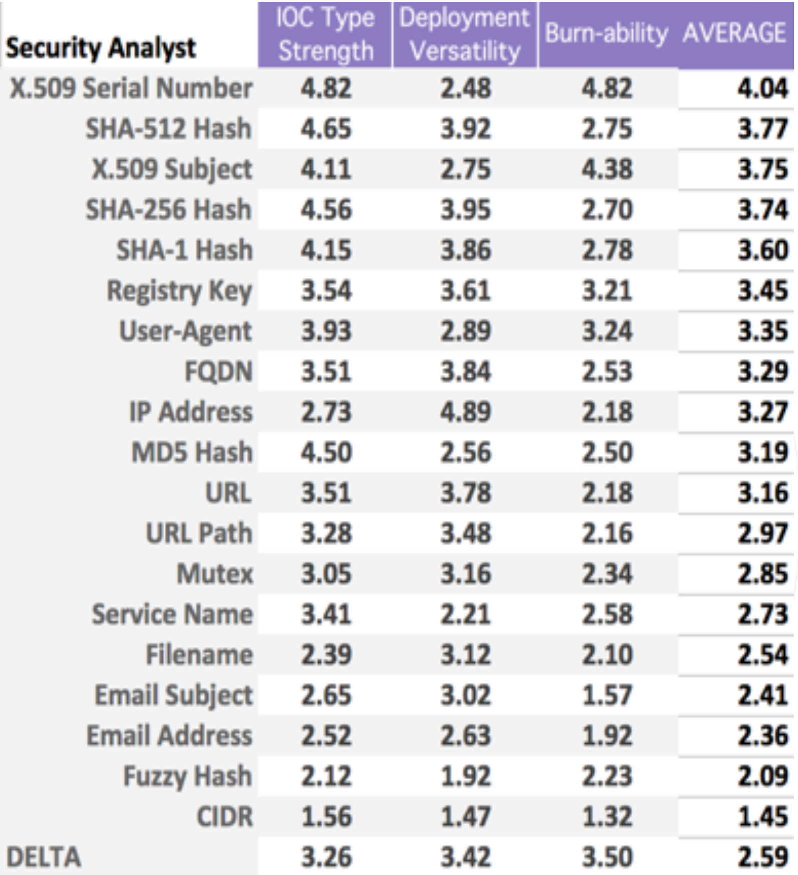
| Adversary Attributes | NO VALUE | POOR VALUE | GOOD VALUE | GREAT VALUE |
|---|---|---|---|---|
| Motivation | 27 | 72 | 109 | 50 |
| Intent | 27 | 85 | 114 | 32 |
| Langauge | 19 | 64 | 134 | 41 |
| Adversary Group | 23 | 14 | 172 | 49 |

| Attack Attributes | NO VALUE | POOR VALUE | GOOD VALUE | GREAT VALUE |
|---|---|---|---|---|
| CVE | 26 | 69 | 118 | 45 |
| Impact | 16 | 53 | 149 | 40 |
| Targeted Industry | 12 | 28 | 95 | 123 |
| Targeted Geography | 94 | 77 | 45 | 42 |
| Malware Family | 17 | 12 | 152 | 77 |
| Vector | 2 | 12 | 221 | 23 |
| Attack Category | 0 | 13 | 143 | 102 |
| BotName | 8 | 15 | 137 | 98 |
| CNC Name | 4 | 21 | 129 | 104 |
| Malware Name | 15 | 9 | 158 | 76 |
| Malware Category | 0 | 8 | 149 | 101 |
| Geolocation | 48 | 152 | 37 | 21 |
| CVSS | 119 | 68 | 51 | 20 |

# SecAnalyst – Results & Observations

Observations:

- Interesting several host-based hash IOCs ranked so high
  - Maybe de-sensitized by number of false positives from IP/FQDN/URL/etc.?
- Delta score [2.59] between the highest and lowest average amongst the various IOC types is the highest spread across the various roles
- A .27 difference between #1 [4.04] and #2 [3.77] is a huge gap comparatively
- Interesting X.509 Subject was so high (#3); the highest position another role had it was #10
- Deployment – IP Address yielded the highest score in the survey w/ 4.89



| Security Analyst | IOC Type Strength | Deployment Versatility | Burn-ability | AVERAGE |
|---|---|---|---|---|
| X.509 Serial Number | 4.82 | 2.48 | 4.82 | 4.04 |
| SHA-512 Hash | 4.65 | 3.92 | 2.75 | 3.77 |
| X.509 Subject | 4.11 | 2.75 | 4.38 | 3.75 |
| SHA-256 Hash | 4.56 | 3.95 | 2.70 | 3.74 |
| SHA-1 Hash | 4.15 | 3.86 | 2.78 | 3.60 |
| Registry Key | 3.54 | 3.61 | 3.21 | 3.45 |
| User-Agent | 3.93 | 2.89 | 3.24 | 3.35 |
| FQDN | 3.51 | 3.84 | 2.53 | 3.29 |
| IP Address | 2.73 | 4.89 | 2.18 | 3.27 |
| MD5 Hash | 4.50 | 2.56 | 2.50 | 3.19 |
| URL | 3.51 | 3.78 | 2.18 | 3.16 |
| URL Path | 3.28 | 3.48 | 2.16 | 2.97 |
| Mutex | 3.05 | 3.16 | 2.34 | 2.85 |
| Service Name | 3.41 | 2.21 | 2.58 | 2.73 |
| Filename | 2.39 | 3.12 | 2.10 | 2.54 |
| Email Subject | 2.65 | 3.02 | 1.57 | 2.41 |
| Email Address | 2.52 | 2.63 | 1.92 | 2.36 |
| Fuzzy Hash | 2.12 | 1.92 | 2.23 | 2.09 |
| CIDR | 1.56 | 1.47 | 1.32 | 1.45 |
| DELTA | 3.26 | 3.42 | 3.50 | 2.59 |

# SecAnalyst – IOC Type Breakdown

| | IOC Type Strength |
|---|---|
| X.509 Serial Number | 4.82 |
| SHA-512 Hash | 4.65 |
| SHA-256 Hash | 4.56 |
| MD5 Hash | 4.50 |
| SHA-1 Hash | 4.15 |
| X.509 Subject | 4.11 |
| User-Agent | 3.93 |
| Registry Key | 3.54 |
| FQDN | 3.51 |
| URL | 3.51 |
| Service Name | 3.41 |
| URL Path | 3.28 |
| Mutex | 3.05 |
| IP Address | 2.73 |
| Email Subject | 2.65 |
| Email Address | 2.52 |
| Filename | 2.39 |
| Fuzzy Hash | 2.12 |
| CIDR | 1.56 |

Notable amount of host-based

| | Deployment Versatility |
|---|---|
| IP Address | 4.89 |
| SHA-256 Hash | 3.95 |
| SHA-512 Hash | 3.92 |
| SHA-1 Hash | 3.86 |
| FQDN | 3.84 |
| URL | 3.78 |
| Registry Key | 3.61 |
| URL Path | 3.48 |
| Mutex | 3.16 |
| Filename | 3.12 |
| Email Subject | 3.02 |
| User-Agent | 2.89 |
| X.509 Subject | 2.75 |
| Email Address | 2.63 |
| MD5 Hash | 2.56 |
| X.509 Serial Number | 2.48 |
| Service Name | 2.21 |
| Fuzzy Hash | 1.92 |
| CIDR | 1.47 |

| | Burn-ability |
|---|---|
| X.509 Serial Number | 4.82 |
| X.509 Subject | 4.38 |
| User-Agent | 3.24 |
| Registry Key | 3.21 |
| SHA-1 Hash | 2.78 |
| SHA-512 Hash | 2.75 |
| SHA-256 Hash | 2.70 |
| Service Name | 2.58 |
| FQDN | 2.53 |
| MD5 Hash | 2.50 |
| Mutex | 2.34 |
| Fuzzy Hash | 2.23 |
| IP Address | 2.18 |
| URL | 2.18 |
| URL Path | 2.16 |
| Filename | 2.10 |
| Email Address | 1.92 |
| Email Subject | 1.57 |
| CIDR | 1.32 |

# SecAnalyst – IOC-centric Breakdown

Observations within this attribute category:

- *Role* was superior (65%) for Great Value

- *Source of Information* (79%) for Good Value

- *Domain/Email Address/IP Type* also demonstrated consistent consensus amongst SecAnalysts

- *Compile Time* received the most pushback (50%) for No Value

| Security Analyst | No Value | Poor Value | Good Value | Great Value |
|---|---|---|---|---|
| ASN | 38% | 39% | 21% | 2% |
| File Size | 17% | 31% | 48% | 4% |
| Packer | 9% | 36% | 52% | 3% |
| Port | 14% | 33% | 50% | 3% |
| Protocol | 25% | 47% | 22% | 7% |
| Attack Country Origin | 28% | 10% | 55% | 7% |
| Role | 0% | 5% | 30% | 65% |
| First Seen | 6% | 8% | 55% | 31% |
| Last Seen | 5% | 6% | 58% | 31% |
| Source of Information | 5% | 3% | 79% | 14% |
| Confidence | 12% | 36% | 28% | 24% |
| Threat/Risk Score | 10% | 34% | 34% | 22% |
| Compile Time | 50% | 27% | 18% | 5% |
| Domain Type | 0% | 5% | 65% | 30% |
| Email Address Type | 5% | 9% | 67% | 20% |
| IP Address Type | 0% | 4% | 67% | 29% |
| Status | 9% | 3% | 59% | 28% |
| Severity | 9% | 29% | 47% | 15% |

# SecAnalyst – Adversary-centric Breakdown

Observations within this attribute category:

- Overall a pretty boring split across Adversary-centric attributes

| Security Analyst | No Value | Poor Value | Good Value | Great Value |
|---|---|---|---|---|
| Motivation | 10% | 28% | 42% | 19% |
| Intent | 10% | 33% | 44% | 12% |
| Langauge | 7% | 25% | 52% | 16% |
| Adversary Group | 9% | 5% | 67% | 19% |

# SecAnalyst – Attack-centric Breakdown

Observations within this attribute category:

- *Vector* (86%) dominated the results with a Good Value

- *Targeted Geography and CVSS* received the most pushback (36%) and (46%) respectively for No Value

| Security Analyst | No Value | Poor Value | Good Value | Great Value |
|---|---|---|---|---|
| CVE | 10% | 27% | 46% | 17% |
| Impact | 6% | 21% | 58% | 16% |
| Targeted Industry | 5% | 11% | 37% | 48% |
| Targeted Geography | 36% | 30% | 17% | 16% |
| Malware Family | 7% | 5% | 59% | 30% |
| Vector | 1% | 5% | 86% | 9% |
| Attack Category | 0% | 5% | 55% | 40% |
| BotName | 3% | 6% | 53% | 38% |
| CNC Name | 2% | 8% | 50% | 40% |
| Malware Name | 6% | 3% | 61% | 29% |
| Malware Category | 0% | 3% | 58% | 39% |
| Geolocation | 19% | 59% | 14% | 8% |
| CVSS | 46% | 26% | 20% | 8% |

# SecAnalyst – Attribute Analysis

| Security Analyst | No Value | Poor Value | Good Value | Great Value |
|---|---|---|---|---|
| Total Average | 12% | 19% | 48% | 21% |
| | | | | |
| IOC-Centric Average | 13% | 21% | 47% | 19% |
| Adversary-Centric Average | 9% | 23% | 51% | 17% |
| Attack-Centric Average | 11% | 16% | 47% | 26% |

…compare categories

…compare assessments within a category

Total Average Observation – Security Analyst predominantly lean towards “Good Value”

Attribute Breakdown Observation:

- re: Great Value scores SecAnalysts lean towards Attack-centric TTPs vs. IOC- or Adversary-centric
- re: All other categories are pretty evenly split across the survey participants

# Lessons Learned

# Lessons Learned

Participate breakdown by Role resulted in interesting data; however, should have asked

- **# of years of experience!**
- Average size of team across work experience
- Previous career path (i.e., 10 years as a security analyst and now spearhead incident response, etc.)

*Get more friends who aren't Security Analysts!*

# Questions?
# ryan . trost @ threatq . com