K7 SECURITY

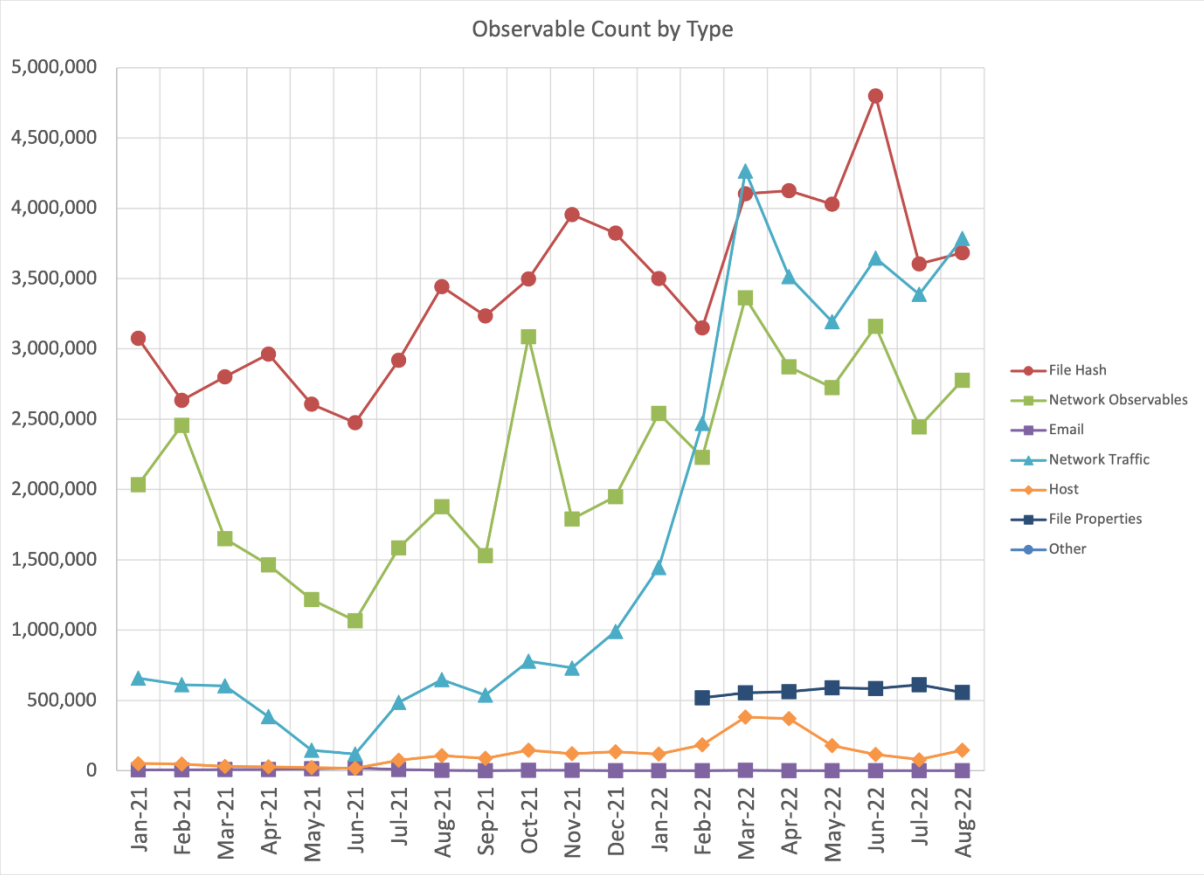
CYBER THREAT ALLIANCE

THREAT INTELLIGENCE PRACTITIONERS' SUMMIT

Tips for Vetting and Generating Value in Automated TI

Samir Mody
VP – Threat Research
K7 Labs

The Glut

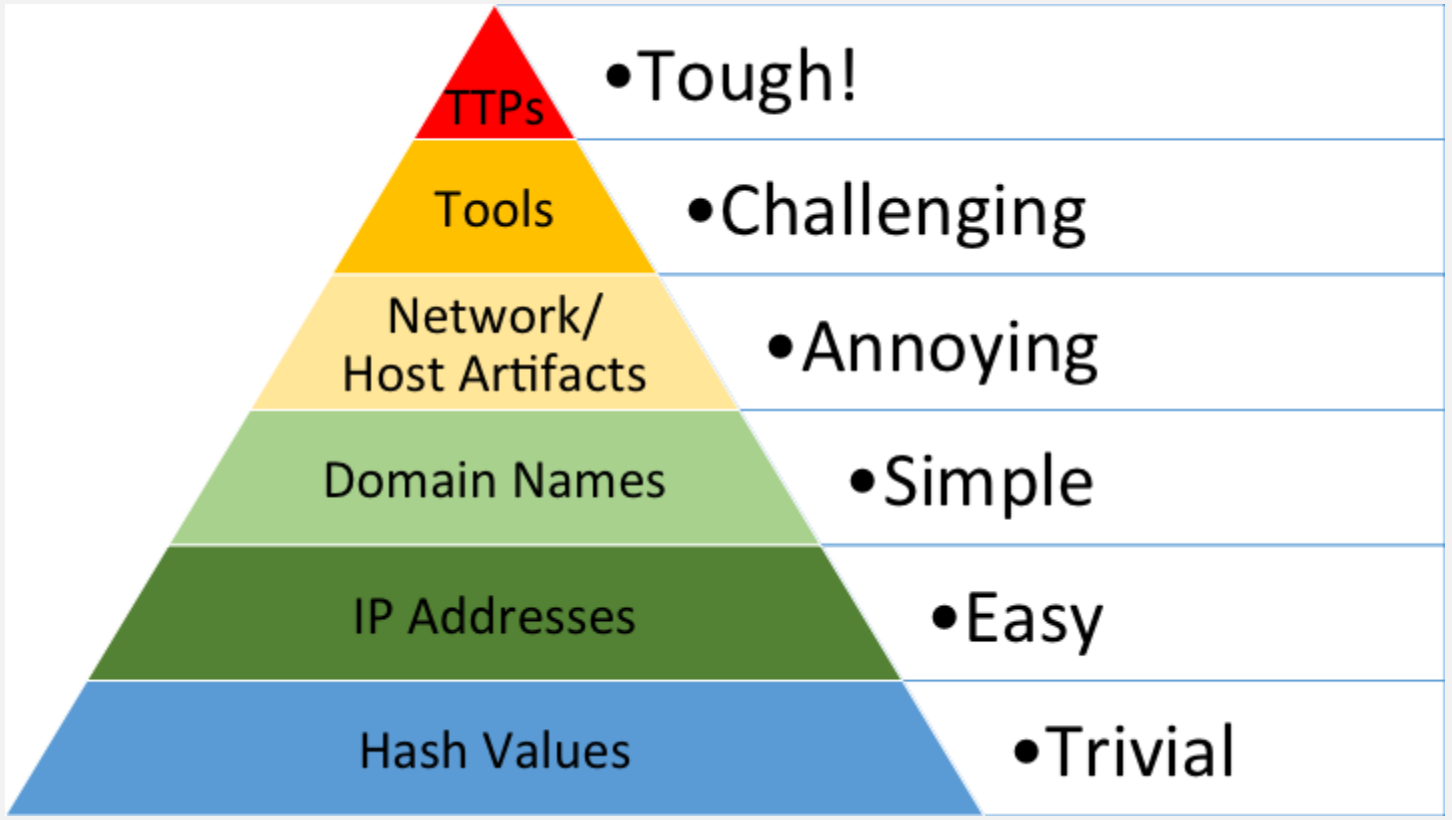


Courtesy: Cyber Threat Alliance

Fundamental Principles of TI Efficacy

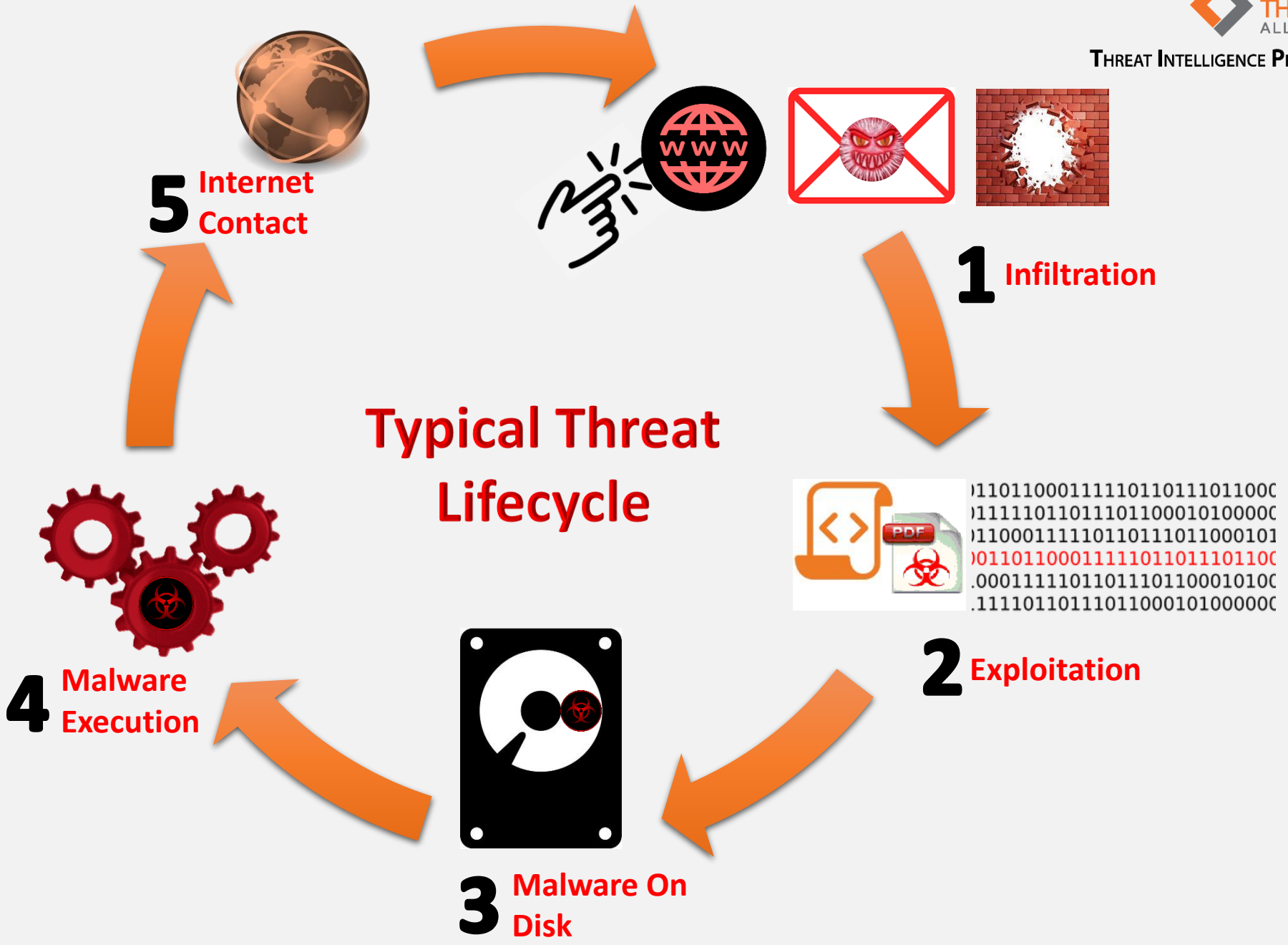
1. **Relevant**: Give the recipient only useful data
2. **Actionable:** Give the recipient only data which can be acted upon
3. **Timely**: Give the recipient the relevant and actionable data ASAP

Pyramid of Pain

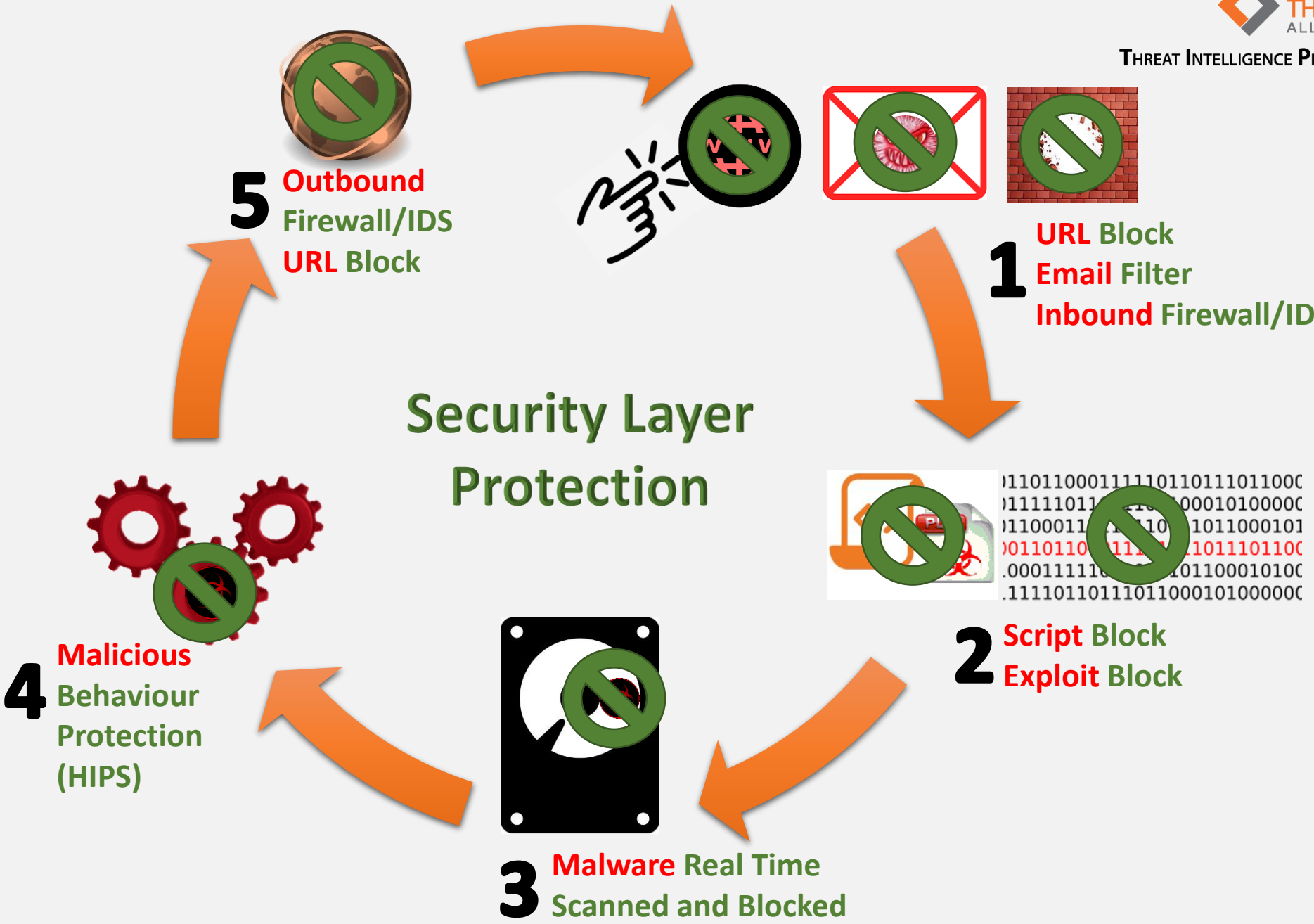


Courtesy: David J Bianco

Typical Threat Lifecycle



Security Layer Protection



Valuable Threat Intel

1 **URL Block**
Email Filter
Inbound Firewall/IDS

URLs
Domains
Sender@Email
IPs & Ports
Snort Rules?

2 **Script Block**
Exploit Block

Artefacts
CVEs (know-how /mitigations)

3 **Malware Real Time Scanned and Blocked**

Artefacts
Hashes
Yara Rules?

4 **Malicious Behaviour Protection (HIPS)**

Artefact Filepaths
Registry Entries
Mutexes
ATT&CK IDs

5 **Outbound Firewall/IDS**
URL Block

C2s/Payloads
- URLs
- Domains
- IPs & Ports

Vetting External TI Feeds

Fundamental Principles	Criterion
Actionability Relevance	What types of objects?
Relevance	Do we already have the same samples?
Timeliness	When did we first know about them?
Relevance	Do we have any of the samples in our whitelists?
Relevance	Are they already detected?
Relevance	How many detections created post evaluation?
Relevance Actionability	How many samples submitted in total?

Purified Telemetry

Generating Valuable Automated TI

Telemetry

- Real-world
- Threat events (malware context)
- Unique (geo, timestamp)

Real-time (almost)

We know the use cases. We want to be able to provide TI to match those contexts.

Validation of Telemetry Data (Obvious)

URL HASH IP

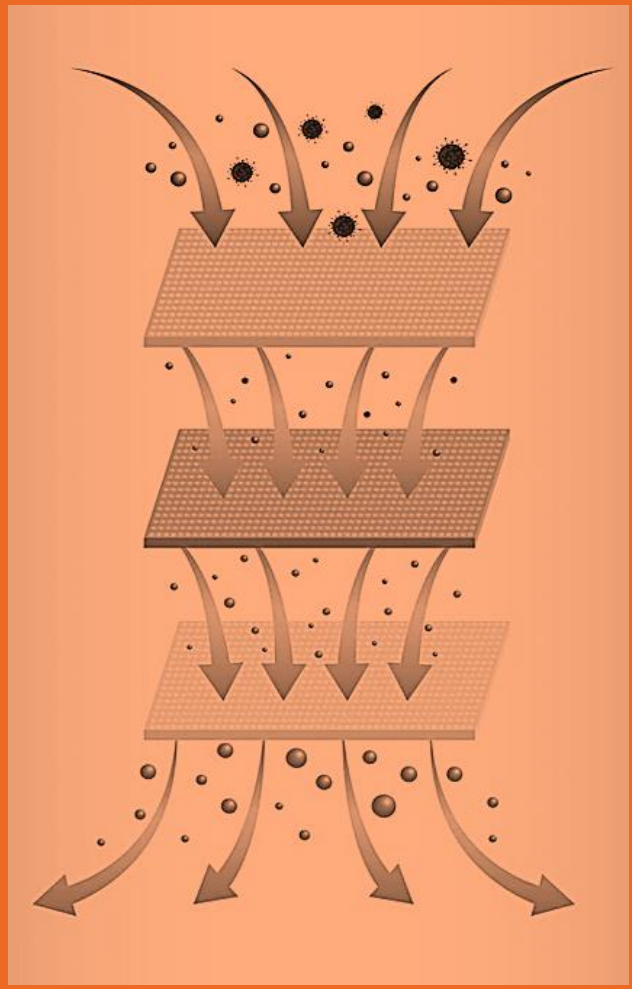
Known Good
- Whitelist
- Reputed Good (H)

Paranoid Good
- Top List
- Reputed Good (M)

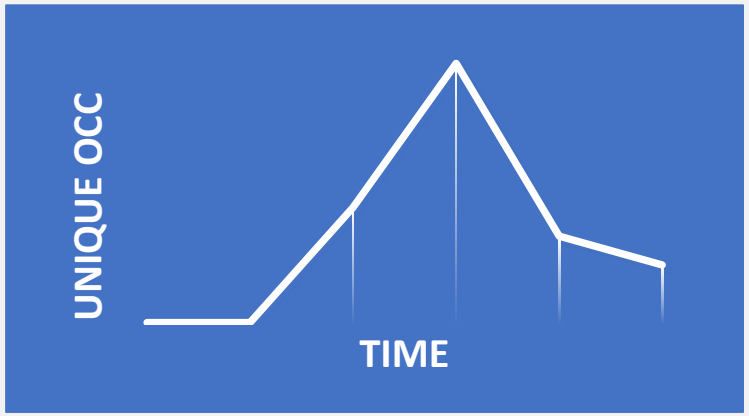
Usability
- File Infector
- Externally Routable

Preferences
- PUA
- Geolocation
- Vertical

URL HASH IP



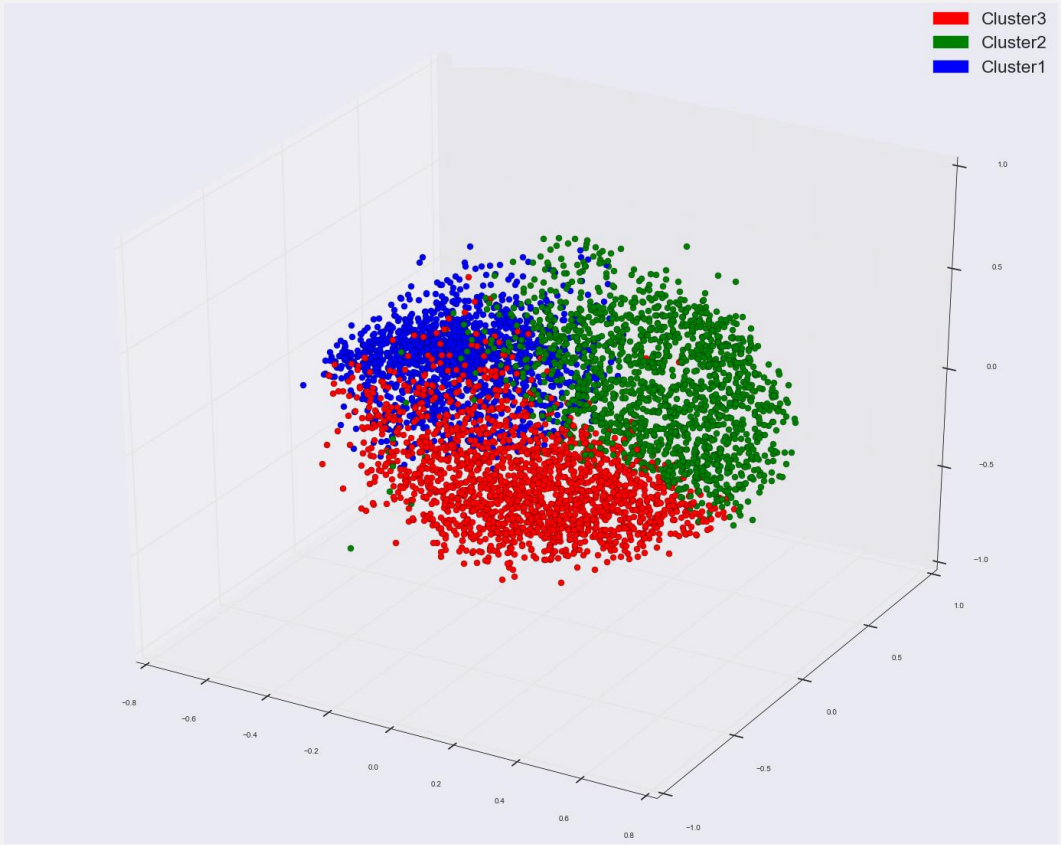
Correlation of Telemetry Data (Subtle)



Upstream

Downstream

URL — HASH — BEHAVIOUR



CYBER THREAT ALLIANCE

THREAT INTELLIGENCE PRACTITIONERS' SUMMIT

Questions ?

K7 SECURITY

www.k7computing.com