NETSCOUT | Arbor

Threat Intelligence 101

Because nobody teaches this stuff in school

Andrew Beard, ASERT Software Architect

COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION

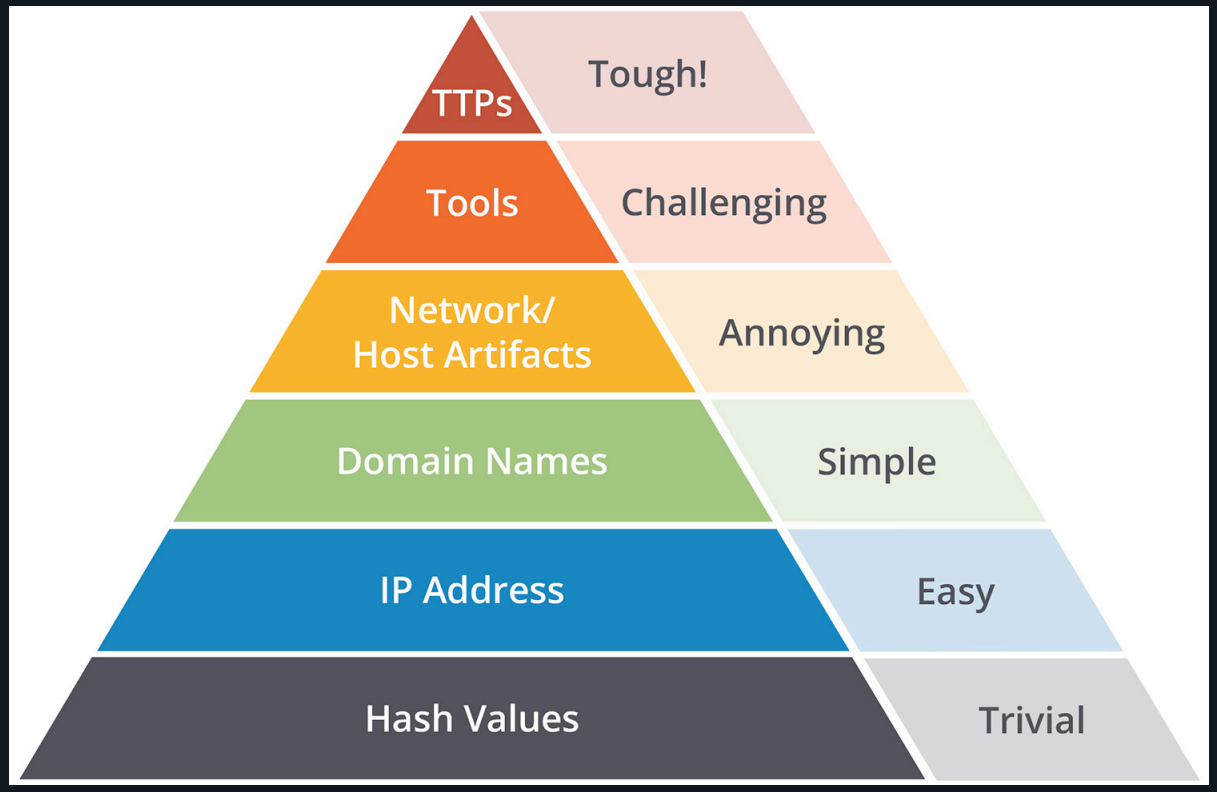
Indicators of Compromise

IOCs

- Bad Stuff™
- Usually ingested by security controls
- Not always conclusive by themselves
- Lots of different types, and of differing values

COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION

The Pyramid of Pain



Source: David Bianco

COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION

COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION

Your Environment

Threat Intel begins at 127.0.0.1

- What controls do you have?
- What can they leverage?
- Who are your adversaries?
- What kind of intel can YOU generate?
- Cost/benefit analysis

COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION

OSINT

- Bambenek Consulting - https://osint.bambenekconsulting.com/feeds/
- abuse.ch - https://abuse.ch/
- Alienvault OTX - https://otx.alienvault.com/
- CleanMX - https://support.clean-mx.com/clean-mx/viruse
- Malware Domain List - http://www.malwaredomainlist.com/forums/index.php?topic=3270.0

COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION

Ask Yourself Some Questions

- What – Can I actually observe this?
- Where – Can this be narrowed down to a subset of my environment?
- Why – Do I know why it's bad? Is there a motive?
- When – How old is it? Is it still relevant?
- Who – Targeting. Are the attacks likely to affect you?

COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION

Commercial Providers

- Ask questions
- Compare to OSINT and make sure there's original content
- Understand how the provider expects it to be used

COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION

Threat Intelligence Platforms

TIP

- Take in multiple feeds and data sources
- Aggregate and normalize indicators
- Filter content that is not relevant
- Deliver content to your controls
- Some also enrich threat data and resulting alerts

COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION

STIX and TAXII

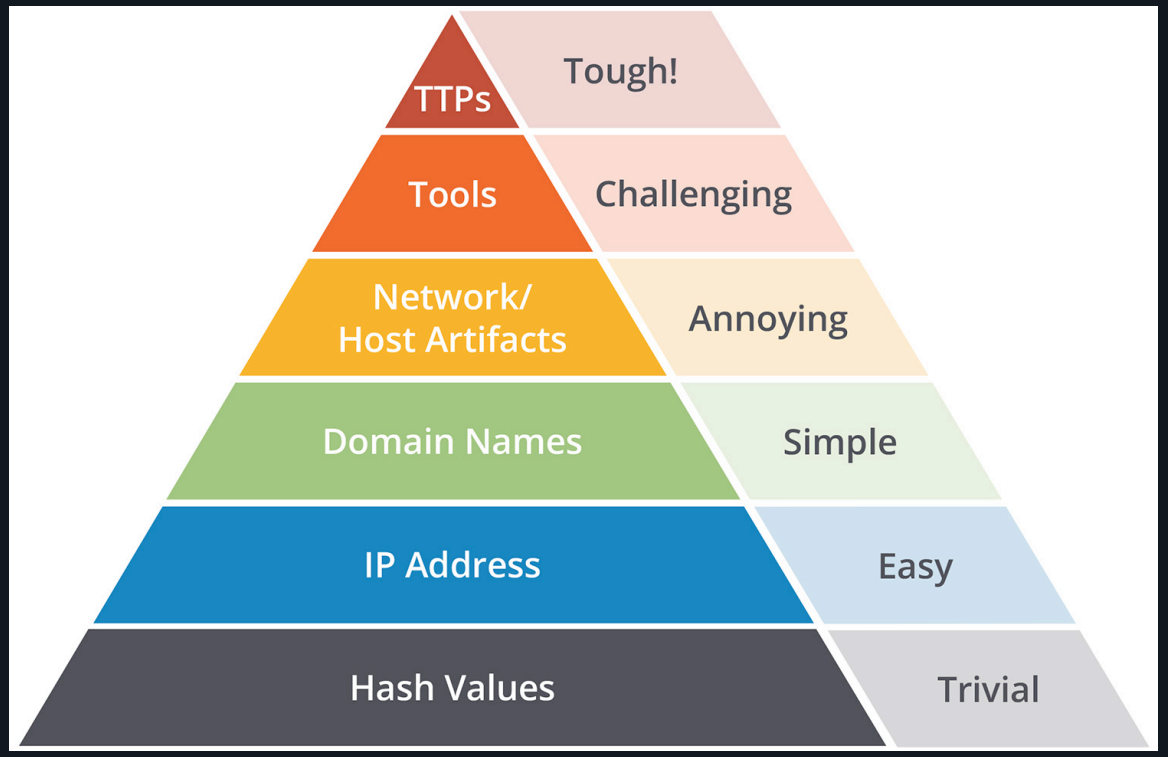
A format so awesome and flexible that it's a pain to actually use

- Structured format for threat intel
- Either XML (1.x) or Json (2.x)
- Able to express complex relationships beyond just IOCs
- Good examples here

COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION

A Quick Case Study

- Malware hashes
- IP Addresses
- Domain Names
- DGA
- Certificate Attributes



COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION

The road to hell is paved with good intentions

DFIU

- Monitor before you act
- Make sure your data is trustworthy
- Verify before you overreact

COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION

Thank You.

Andrew Beard
andrew.beard@netscout.com
@bearda24

www.netscout.com

COPYRIGHT © 2019 NETSCOUT SYSTEMS, INC. | PUBLIC DISTRIBUTION