The TIP of the Stinger

EFFICIENTLY USING THREAT INTELLIGENCE WITH THEHIVE

Matthew Gracie
Senior Engineer
Security Onion Solutions

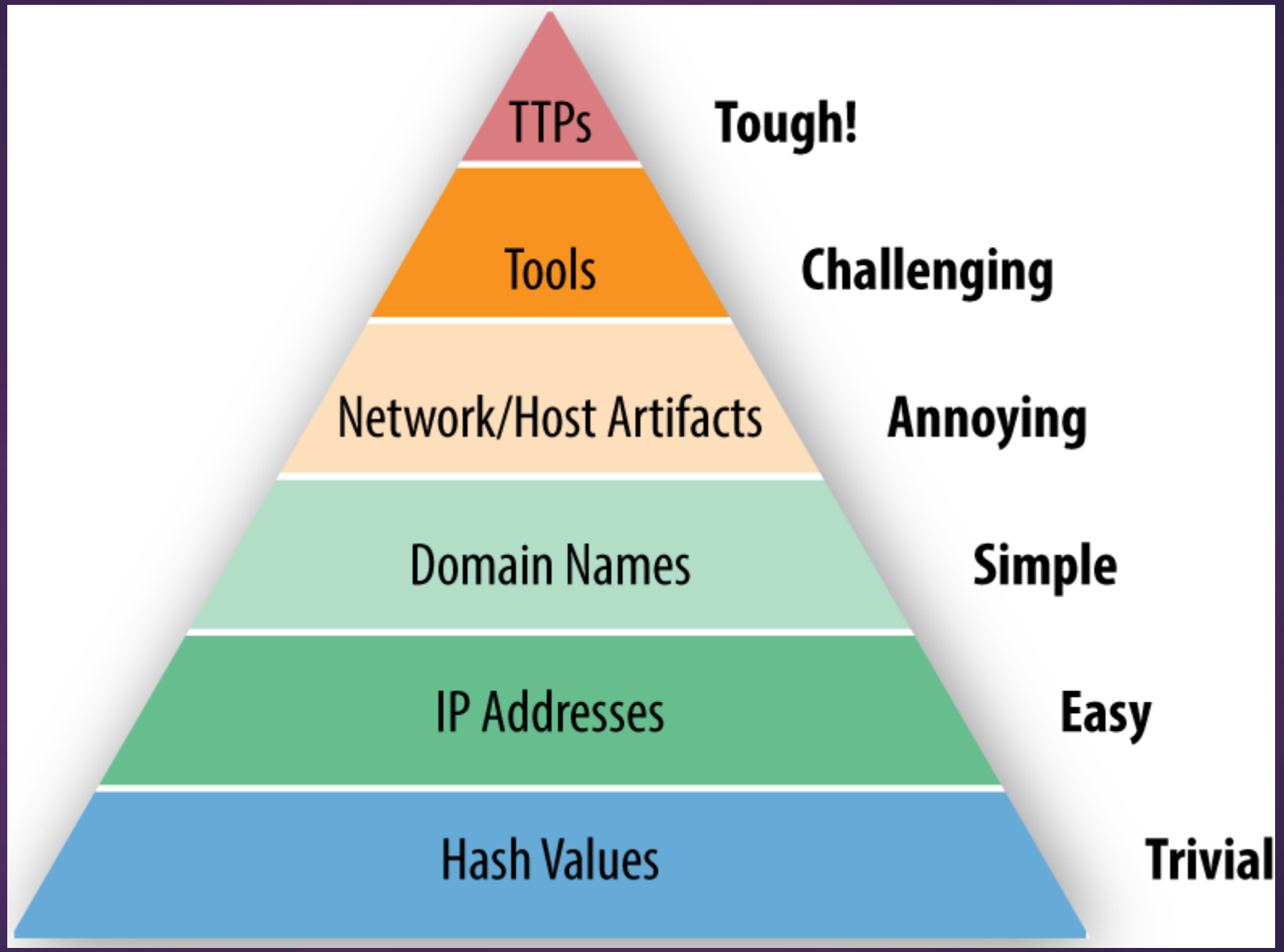
Who Am I And What Am I Talking About?


PEOPLE WHO
BUY THINGS
ARE SUCKERS
quickmeme.com

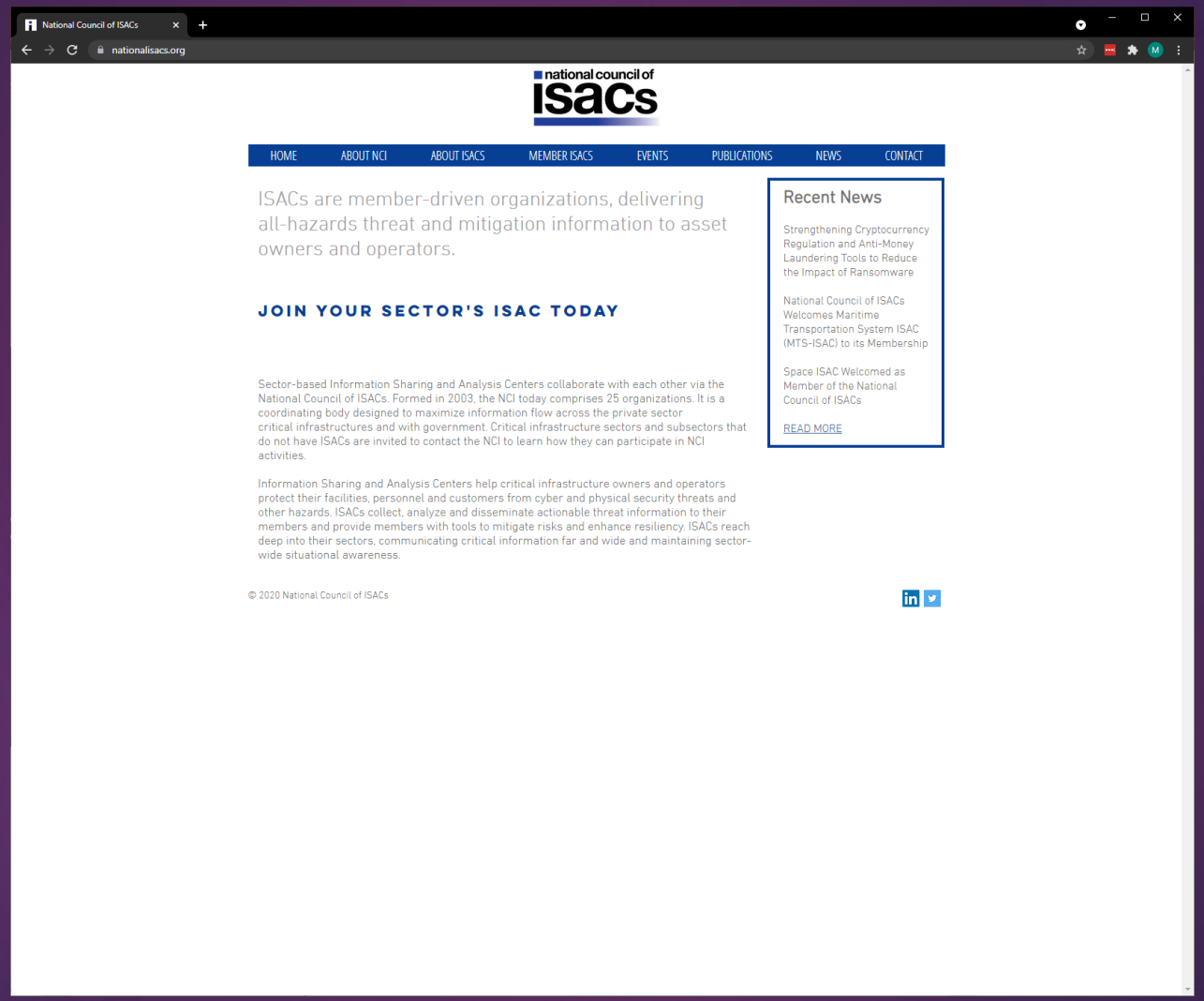
What is Threat Intelligence?

- “Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.” --Gartner *

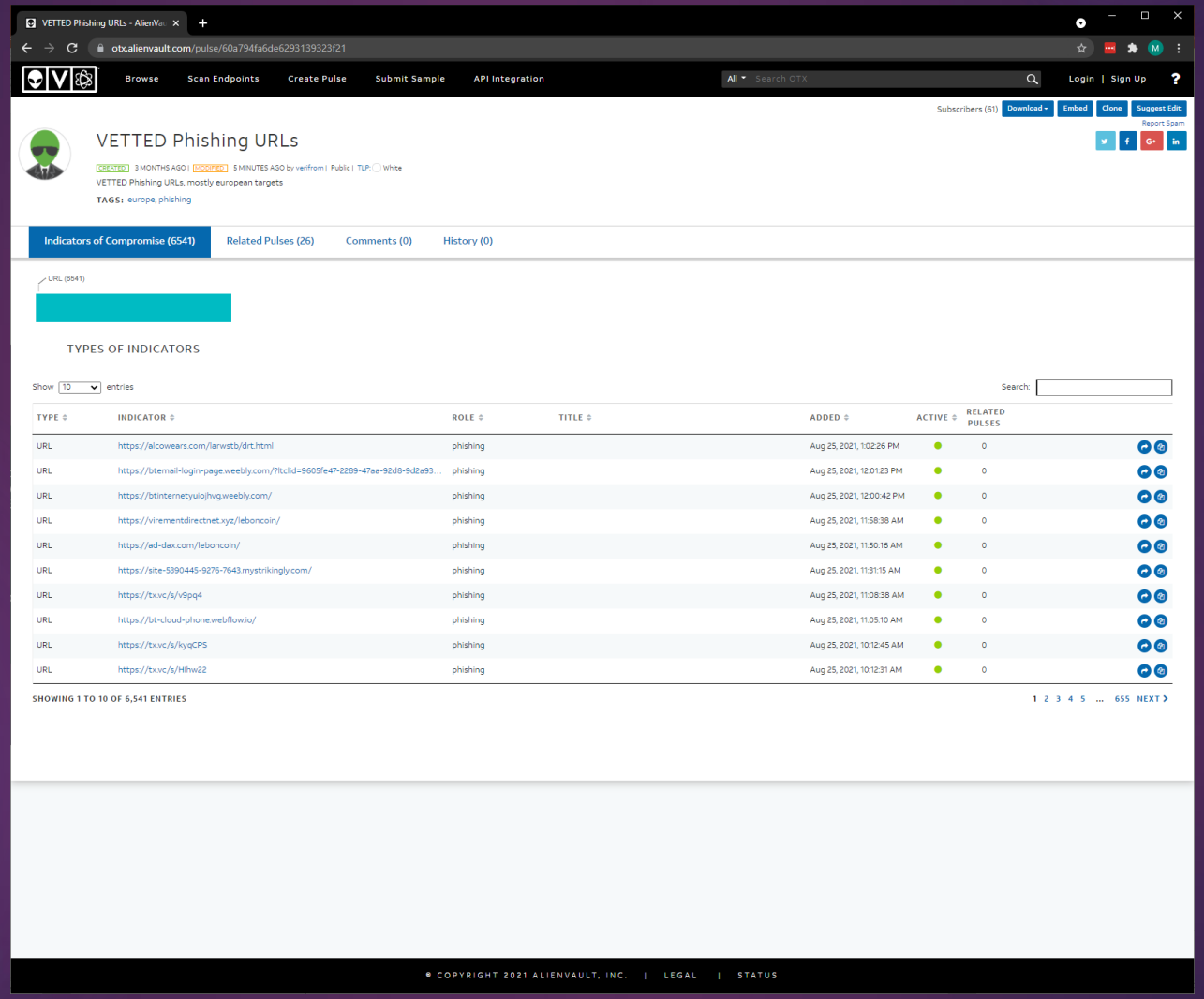
* https://www.gartner.com/doc/2487216/definition-threat-intelligence

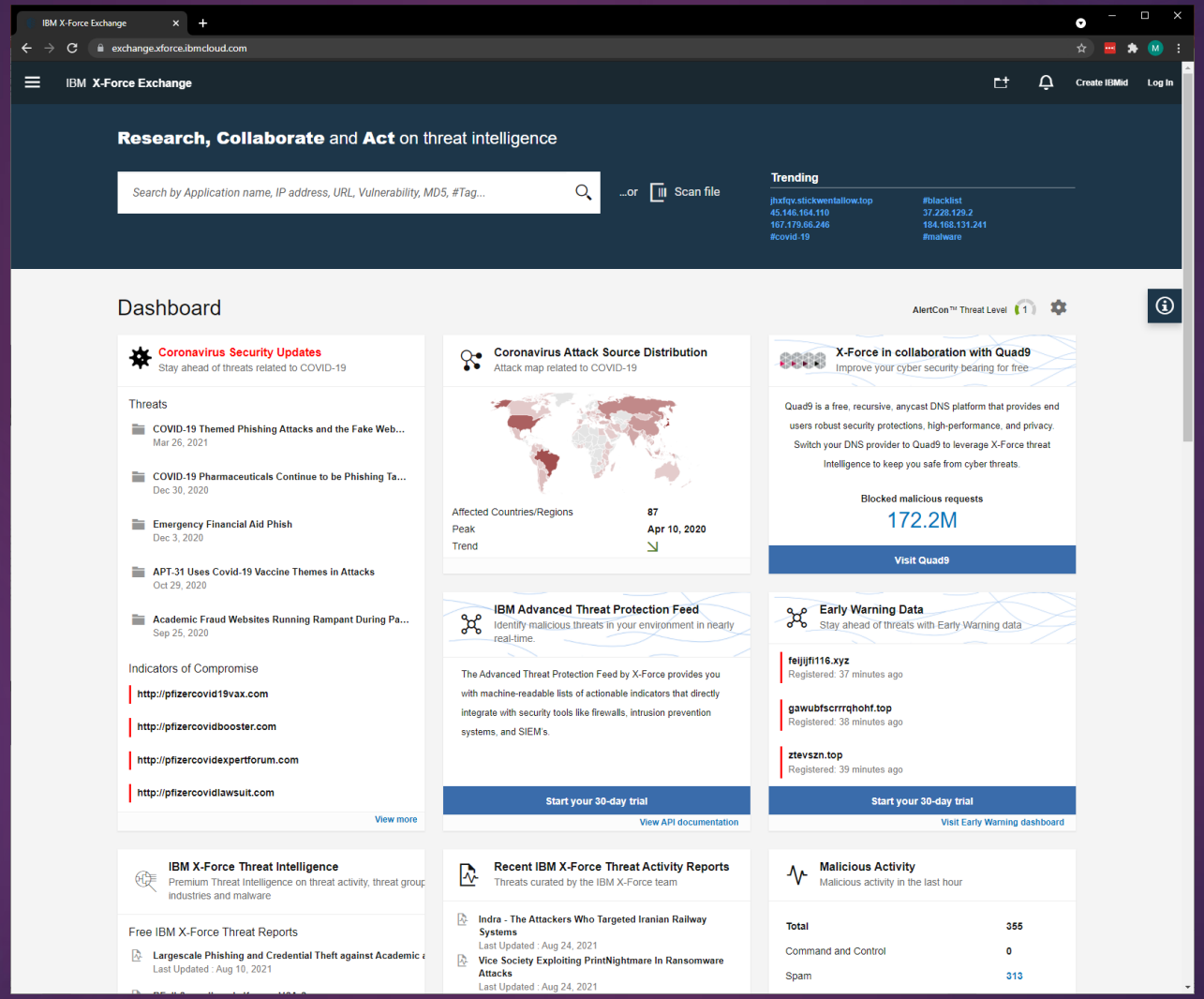

TTPs
Tough!
Tools
Challenging
Network/Host Artifacts
Annoying
Domain Names
Simple
IP Addresses
Easy
Hash Values
Trivial

Where Do I Get IOCs?


National Council of ISACs
nationalisacs.org
national council of ISACs
HOME
ABOUT NCI
ABOUT ISACS
MEMBER ISACS
EVENTS
PUBLICATIONS
NEWS
CONTACT
ISACs are member-driven organizations, delivering all-hazards threat and mitigation information to asset owners and operators.
JOIN YOUR SECTOR'S ISAC TODAY
Sector-based Information Sharing and Analysis Centers collaborate with each other via the National Council of ISACs. Formed in 2003, the NCI today comprises 25 organizations. It is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with government. Critical infrastructure sectors and subsectors that do not have ISACs are invited to contact the NCI to learn how they can participate in NCI activities.
Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.
Recent News
Strengthening Cryptocurrency Regulation and Anti-Money Laundering Tools to Reduce the Impact of Ransomware
National Council of ISACs Welcomes Maritime Transportation System ISAC (MTS-ISAC) to its Membership
Space ISAC Welcomed as Member of the National Council of ISACs
READ MORE
© 2020 National Council of ISACs


Bad Packets
@bad_packets
Mass scanning activity detected from the following hosts checking for Microsoft Exchange servers vulnerable to #ProxyShell (CVE-2021-34473).
172.93.194.119 (🇺🇸)
192.3.154.53 (🇺🇸)
37.44.253.125 (🇳🇱)
193.93.195.252 (🇷🇺/🇳🇱)*
#threatintel
*Geolocation vendors don't agree on location
4:46 PM · Aug 24, 2021 · Twitter Web App
16 Retweets 1 Quote Tweet 35 Likes


VETTED Phishing URLs - AlienVa
otx.alienvault.com/pulse/60a794fa6de629313923f21
Browse
Scan Endpoints
Create Pulse
Submit Sample
API Integration
All
Search OTX
Login | Sign Up
Subscribers (61)
Download
Embed
Clone
Suggest Edit
Report Spam
VETTED Phishing URLs
CREATED 3 MONTHS AGO | MODIFIED 5 MINUTES AGO by verifrom | Public | TLP: White
VETTED Phishing URLs, mostly european targets
TAGS: europe, phishing
Indicators of Compromise (6541)
Related Pulses (26)
Comments (0)
History (0)
URL (6541)
TYPES OF INDICATORS
Show 10 entries
Search:
TYPE
INDICATOR
ROLE
TITLE
ADDED
ACTIVE
RELATED PULSES
URL https://alcowears.com/larwstb/drt.html phishing Aug 25, 2021, 1:02:26 PM 0
URL https://btemail-login-page.weebly.com/?ltclid=9605fe47-2289-47aa-92d8-9d2a93... phishing Aug 25, 2021, 12:01:23 PM 0
URL https://btinternetyuiojhvg.weebly.com/ phishing Aug 25, 2021, 12:00:42 PM 0
URL https://virementdirectnet.xyz/leboncoin/ phishing Aug 25, 2021, 11:58:38 AM 0
URL https://ad-dax.com/leboncoin/ phishing Aug 25, 2021, 11:50:16 AM 0
URL https://site-5390445-9276-7643.mystrikingly.com/ phishing Aug 25, 2021, 11:31:15 AM 0
URL https://tx.vc/s/v9pq4 phishing Aug 25, 2021, 11:08:38 AM 0
URL https://bt-cloud-phone.webflow.io/ phishing Aug 25, 2021, 11:05:10 AM 0
URL https://tx.vc/s/kyqCP5 phishing Aug 25, 2021, 10:12:45 AM 0
URL https://tx.vc/s/Hlhw22 phishing Aug 25, 2021, 10:12:31 AM 0
SHOWING 1 TO 10 OF 6,541 ENTRIES
1 2 3 4 5 ... 655 NEXT
© COPYRIGHT 2021 ALIENVAULT, INC. | LEGAL | STATUS


IBM X-Force Exchange
exchange.xforce.ibmcloud.com
IBM X-Force Exchange
Create IBMid
Log In
Research, Collaborate and Act on threat intelligence
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
...or
Scan file
Trending
jhxfqv.stickwentallow.top
45.146.164.110
167.179.66.246
#covid-19
#blacklist
37.228.129.2
184.168.131.241
#malware
Dashboard
AlertCon™ Threat Level
1
Coronavirus Security Updates
Stay ahead of threats related to COVID-19
Threats
COVID-19 Themed Phishing Attacks and the Fake Web...
Mar 26, 2021
COVID-19 Pharmaceuticals Continue to be Phishing Ta...
Dec 30, 2020
Emergency Financial Aid Phish
Dec 3, 2020
APT-31 Uses Covid-19 Vaccine Themes in Attacks
Oct 29, 2020
Academic Fraud Websites Running Rampant During Pa...
Sep 25, 2020
Indicators of Compromise
http://pfizercovid19vax.com
http://pfizercovidbooster.com
http://pfizercovidexpertforum.com
http://pfizercovidlawsuit.com
View more
Coronavirus Attack Source Distribution
Attack map related to COVID-19
Affected Countries/Regions 87
Peak Apr 10, 2020
Trend
X-Force in collaboration with Quad9
Improve your cyber security bearing for free
Quad9 is a free, recursive, anycast DNS platform that provides end users robust security protections, high-performance, and privacy. Switch your DNS provider to Quad9 to leverage X-Force threat Intelligence to keep you safe from cyber threats.
Blocked malicious requests
172.2M
Visit Quad9
IBM Advanced Threat Protection Feed
Identify malicious threats in your environment in nearly real-time.
The Advanced Threat Protection Feed by X-Force provides you with machine-readable lists of actionable indicators that directly integrate with security tools like firewalls, intrusion prevention systems, and SIEM's.
Start your 30-day trial
View API documentation
Early Warning Data
Stay ahead of threats with Early Warning data
feijjfi116.xyz
Registered: 37 minutes ago
gawubfscrrrqhohf.top
Registered: 38 minutes ago
ztevszn.top
Registered: 39 minutes ago
Start your 30-day trial
Visit Early Warning dashboard
IBM X-Force Threat Intelligence
Premium Threat Intelligence on threat activity, threat group industries and malware
Free IBM X-Force Threat Reports
Largescale Phishing and Credential Theft against Academic
Last Updated : Aug 10, 2021
Recent IBM X-Force Threat Activity Reports
Threats curated by the IBM X-Force team
Indra - The Attackers Who Targeted Iranian Railway Systems
Last Updated : Aug 24, 2021
Vice Society Exploiting PrintNightmare In Ransomware Attacks
Last Updated : Aug 24, 2021
Malicious Activity
Malicious activity in the last hour
Total 355
Command and Control 0
Spam 313

Now That I Have The IOCs, What Do I Do With Them?

MISP

- MISP Threat Sharing is an open source Threat Intel Platform (TIP)
- Collects, sanitizes, normalizes, and distributes IOCs
- Comes with extensive catalog of preconfigured IOC feeds
- Supports tagging, TLP, galaxies, taxonomies, and much more
- Robust import and export capabilities
- This is an excellent “system of record”

Getting Data Into MISP

- Manual entry in web console
- Import local MISP JSON or CSV files
- Share data with other MISP instances
- Import .IOC files, Threatconnect, PDF, etc.
- Many third party extensions and add-ons

Security Onion

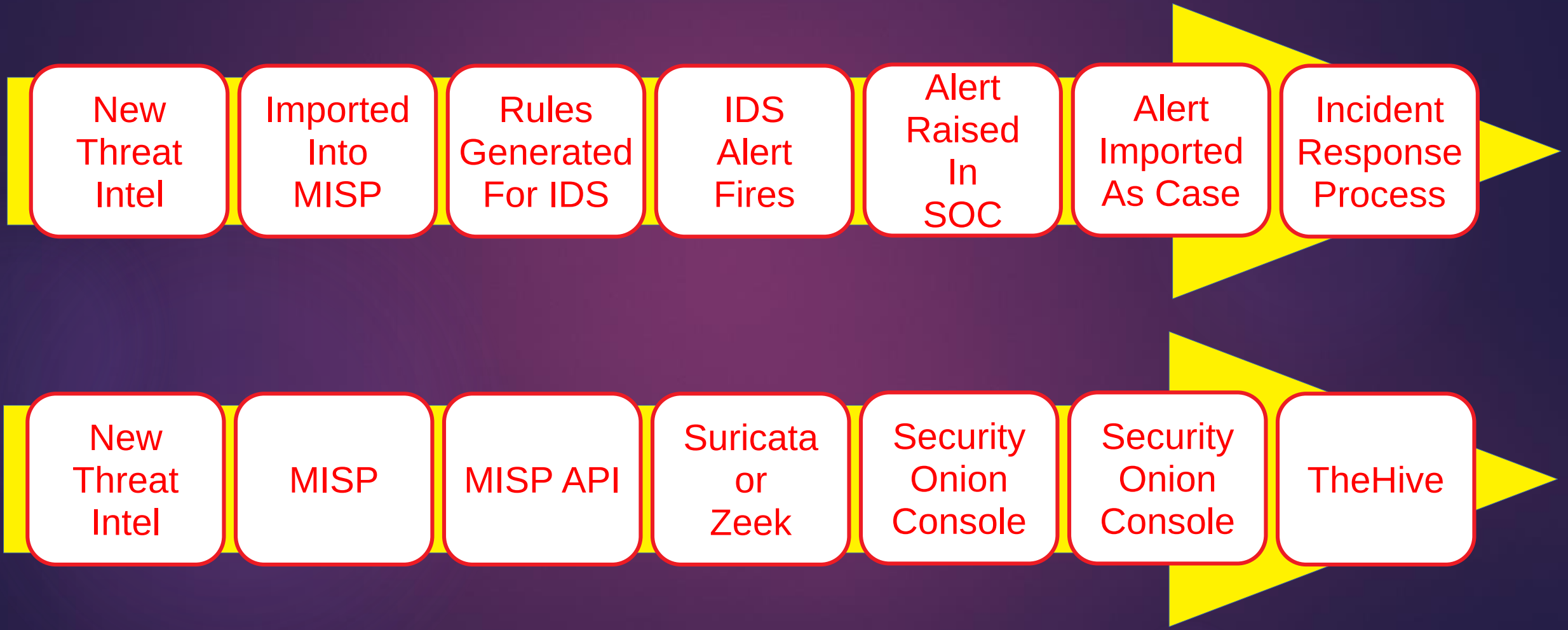
- Project started by Doug Burks (@dougburks) in 2008
- Prebuilt, Dockerized stack of Network Security Monitoring tools
- Available as an appliance ISO or can install on Ubuntu / CentOS
- Monitors traffic via a SPAN port or tap infrastructure

Security Onion

Five components in Security Onion are especially useful here:

- Suricata – Signature-based IDS
- Zeek – Network metadata generator
- Playbook – Custom alert generation via Sigma rules
- TheHive – Case management and record-keeping
- Security Onion Console (SOC) – Workflow and alerting

Hunting IOCs



Demonstration

Scenario

- An industry partner has shared some information about a web shell found in their environment
- This information includes the file hashes and name of the web shell itself, the IP address that it was downloaded from, and the IP address of the attacker that was accessing it in their environment
- What does it look like when these artifacts are put into MISP, used to populate our Security Onion rulesets, and then triggered?

How Can I Play With This?

- MISP:
  https://www.misp-project.org/
- Security Onion:
  https://www.securityonion.net/
- MISP / SO Integration Script:
  https://github.com/weslambert/securityonion-misp

Questions?

For More Information:

@InfosecGoon

infosecgoon@roadflares.org

https://github.com/InfosecGoon/