Chapter 4:
- Incident management, ticketing system
- Alerts, events, incidents
- Events Detection&prevention mechanisms: Yara Rules & Regex
- Using Open-source Intelligence (OSINT)

Presented by **Alexandru Balanica** and

Radu Cirstea

- 12th of November 2021

Agenda

- ✓ **Incident management**
- ✓ **Ticketing system**
- ✓ **Alerts, events, incidents**
- ✓ **Events Detection & prevention mechanisms: Yara Rules & Regex**
- ✓ **Using Open-source Intelligence (OSINT)**

Incident Management

- Incident management (IcM) is a term describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence.
- An incident is an event that could lead to loss of, or disruption to, an organization's operations, services or functions.
- The first goal of the incident management process is to restore a normal service operation as quickly as possible and to minimize the impact on business operations

Incident Handling – Roles

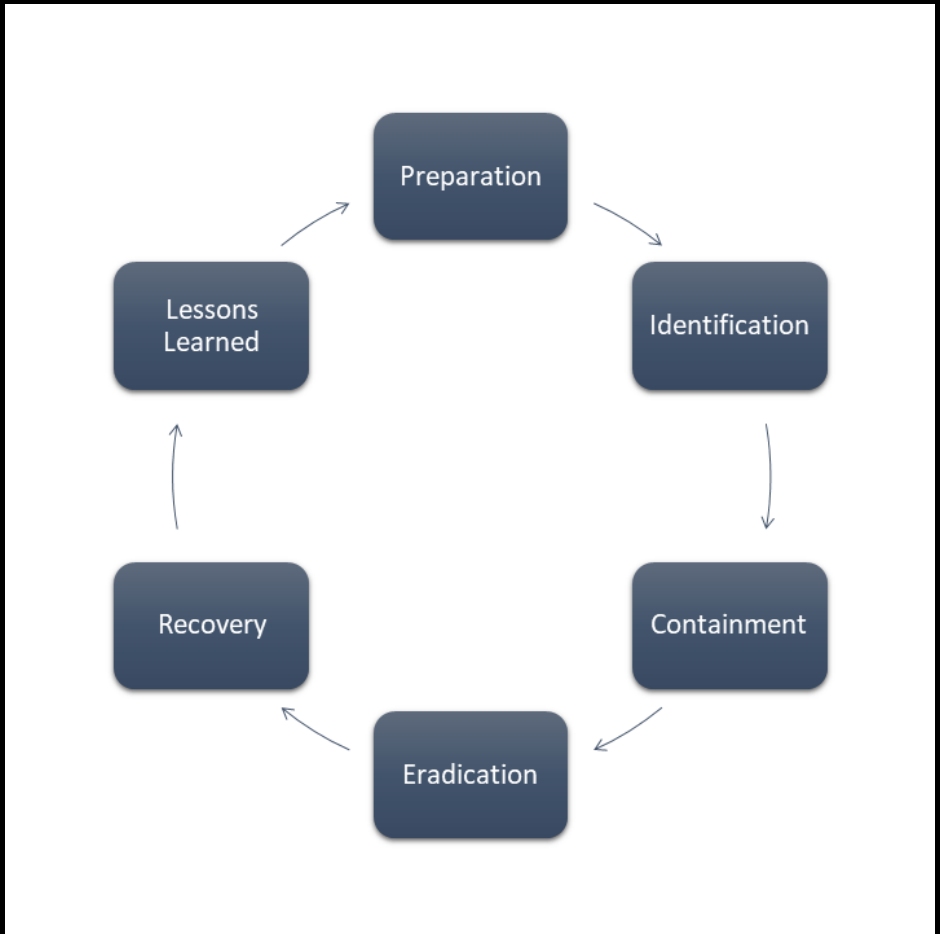
Tier 1 –Triage: deals with the reported security events, decides whether there is an incident that needs to be handled and by whom

Tier 2 Incident handler - works on the incident: analyze data, create solutions, resolve the technical details and communicates about the progress to the manager and the constituents.

Tier 3 Subject Matter Expert – experienced analyst that deals with complex cases that involve a cross-filed investigation.

Incident Handling

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned



Incident management ticketing system

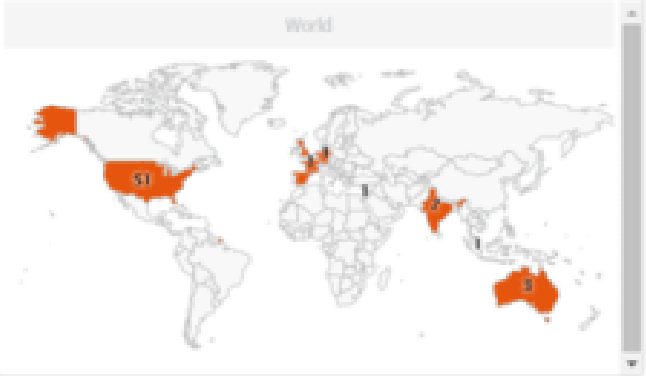
- Incident management software allows you set up parent-child relationship between incident and their associated problem tickets.
- Furthermore, incident management software delivers flexible automation rules to allow IT technicians to simplify service request progression and management. Reducing considerably the time and effort support agents spend to manage incidents
- Alert and report on SLA timelines and ticket status
- Intuitive reporting dashboards to monitor technician performance & track ticket status
- Centralized Web-based interface provides single pane of glass for managing incident tickets.

Examples

- SNOW – Service Now
- Jira
- Spiceworks (Open Source)
- SolarWinds

IT Incident Overview

Open Incidents Map



Open Incidents

72

Open P1 - Incident

0

Open Unassigned

5

Open Overdue Incidents

14

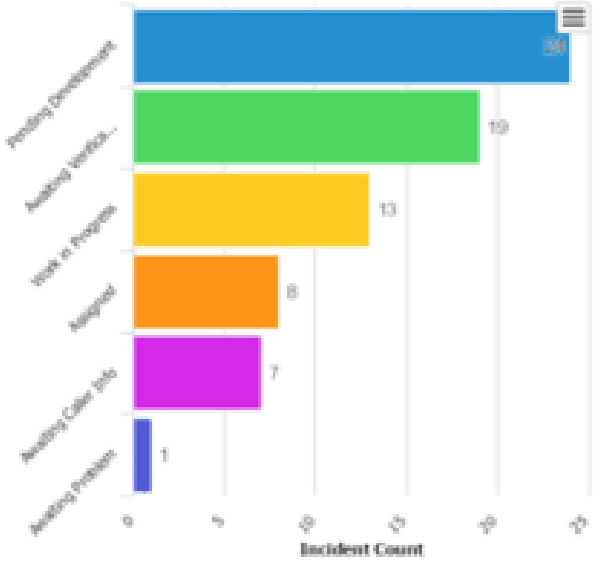
Open P2 - Incident

3

Open Incidents - Storied

18

Open Incidents - By State



Open P3 - Incident

34

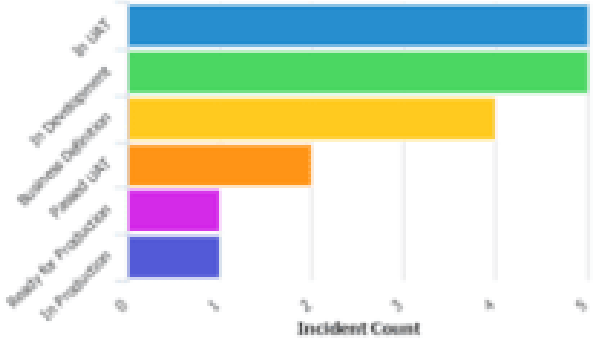
Open P4 - Incident

35

INC not Updated (7 Days

19

Incident Stories By State



Incident Service Levels

Priority - 1

Type	SLA
Acknowledged	30 min
Assigned	15 min
Resolution	4 hrs

Priority - 2

Type	SLA
Acknowledged	2 Days
Assigned	1 day
Resolution	1 week

Priority - 3

Type	SLA
Acknowledged	2 Days
Assigned	1 day
Resolution	1 week

Priority - 4

Type	SLA
Acknowledged	2 days
Assigned	1 day
Resolution	2 weeks

Security Information and Event Management Systems SIEM

- A subsection within the field of computer security, where software products and services combine Security Information Management (SIM) and Security Event Management (SEM).

Capabilities	Examples
• Data Aggregation • Correlation • Alerting • Dashboards • Compliance • Retention • Forensics Analysis	• Splunk • Qradar • CTP

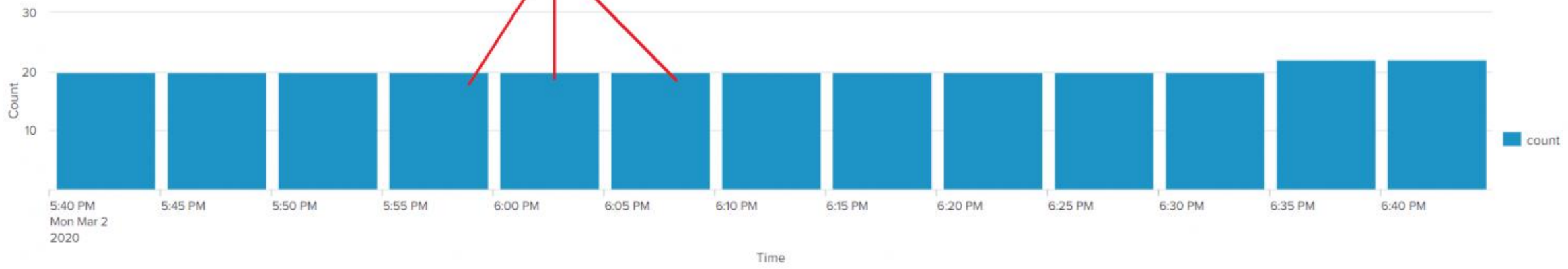
Home Metrics Hosts Alerts Search Settings *nix Splunk App for Unix

Help

Alert Time Range

Alert counts

Time range picker Last 60 minutes



Host / Name / Severity filters

Statistics

Reset

Hosts

Netapp-DCN VMware-DCN

Click to get details on a specific alert

Summary

Click to see individual events for the alert

264 Alerts From 03/02/2020 5:40:00 PM to 03/02/2020 6:40:00 PM

Prev 1 2 3 4 5 ... 27 Next

Time	Name	Severity	Hosts	Action	Description
March 2nd, 2020 6:40:00 PM	Memory_Exceeds_MB_by_Process	High	VMware-DCN	Open in Search	
March 2nd, 2020 6:40:00 PM	Memory_Exceeds_MB_by_Process	High	Netapp-DCN	Open in Search	


Events
Alerts
Incidents

Events

- An event is any observable occurrence in IT infrastructure. An event can be something benign and unremarkable and it is not necessarily something malicious.
- According to ITIL (Information Technology Infrastructure Library - a framework of best practices for delivering IT services) there are 3 categories of events:
- informational (INFO)
- warning (WARN / ALERT):
- exception (ERROR):

Informational event

- An event that does not require any immediate action and does not represent an exception. They are recorded in the log files and maintained for a predetermined period.
- Below is an example from a live environment of an information event: nothing outstanding happened, just a host who made a query (connection) to google.com:

```
Nov  3 09:56:35 [redacted]dns.[redacted].com named[30250]: 03-Nov-2020 09:56:35.629 client 10.180.100.27#6478: UDP: query: google.com IN AAAA response: NOERROR + google.com. 142 IN AAAA 2404:6800:4008:c07::8b; google.com.
host = [redacted]dns.[redacted].com | source = /logs/infoblox/dns/[redacted]dns.[redacted].com/2020-11-03-09-dns.log | sourcetype = infoblox:dns
```

Warning event

- Event is generated when a device or service, (application / utility), is approaching an agreed threshold or when an unusual activity is recorded.
- Below is a type of warning event: unusual, but not exceptional (a host made multiple queries to the same domain in a short period of time)

Nov 3 10:25:17 [redacted]dns.[redacted].com named[28512]: 03-Nov-2020 10:25:17.558 client 10.168.26.42#45878: UDP: query: gc-device-api.apps.playnetwork.com IN A response: NOERROR + gc-device-api.apps.playnetwork.com. 2 IN A 52.24.180.217;

host = [redacted]dns.[redacted].com | source = /logs/infoblox/dns/[redacted]dns.[redacted]om/2020-11-03-10-dns.log | sourcetype = infoblox:dns

Nov 3 10:24:17 [redacted]dns.[redacted].com named[28512]: 03-Nov-2020 10:24:17.569 client 10.168.26.42#27209: UDP: query: gc-device-api.apps.playnetwork.com IN A response: NOERROR + gc-device-api.apps.playnetwork.com. 10 IN A 52.88.255.146;

host = [redacted]dns.[redacted].com | source = /logs/infoblox/dns/[redacted]dns.[redacted]com/2020-11-03-10-dns.log | sourcetype = infoblox:dns

Exception event

- Means that a service or device is currently operating below the normal parameters/indicators (predefined). This mean that the business service is impacted, and the device or service presents a failure, performance degradations or loss of functionality.
- Below is an example of exception event: one host stopped sending security events logs:

Our event flow monitoring has detected a disruption in the flow of events from TEST.dcamucp.local located at Company. This system generated ticket indicates that SECURITY events have not been received from this device within defined limits. Status is DOWN; last SECURITY event received on Tue Nov 03 12:25:48 UTC 2020.

Alerts

- An alert is a notification that a notable event has happened. The alert goes to those responsible for taking actions (if needed). Not every event demands an alert – just those that will require action.

- Not every event demands an alert – just those that will require action. If the threshold is too low, multiple alerts will be raised and you might not see real issues through the noise. Set the threshold too high and you will not have enough warning to take preventative action.

Alert example

5:29:18 am Nov 3, 2020	A suspected virus was detected running. A Deny Policy Action was applied.

ALERT DETAILS

Alert ID: 19E4JKKQ

Reason	A suspected virus was detected running. A Deny Policy Action was applied.

Hide

Threat category	Non-Malware
Last seen	5:29:18 am Nov 3, 2020
Location at time of threat	Off-premises

PROCESS

epevenue_sh.exe

Deleted	Not deleted
Signed	税友软件集团股份有限公司
Techniques	policy_deny, run_suspect_app

Hide

SHA-256	83351fa3d85b6c69efa75d24c0e4715a68b6d544a0e16f86522c0fe863707e03
First seen	5:29:18 am Nov 3, 2020

Incidents

- An incident is an event that negatively affects the confidentiality, integrity, and/or availability (CIA) at an organization in a way that impacts the business. Not all events are incidents, but all incidents are events. It is an unplanned interruption or reduction in quality of an IT service. For example, a DDoS attack, or flooding of a server room are both incidents. Events do not have to be negative – incidents always are.
- A *Security Incident* has a similar relationship to a Security Event. It specifically affects a business' information security – normally by damaging or breaching it. Again, while the majority of Security Events do not need dealing with, a Security Incident requires action.

OSINT: Open-Source Intelligence

OSINT – Open-source intelligence

Information or data that is accessed and gathered from public and free sources for any specific purpose.

- Common OSINT sources: the Internet (i.e. blogs, social media, websites, government portals, deep web, dark web), traditional channels (i.e. Newspaper, Television, Radio, Magazines; Books, Academic Publications such as journals & research papers etc.)
- In infosec analysis OSINT is used in researching active threats, contextualizing attacks, identifying security gaps, strengthening security posture

Threat Intelligence

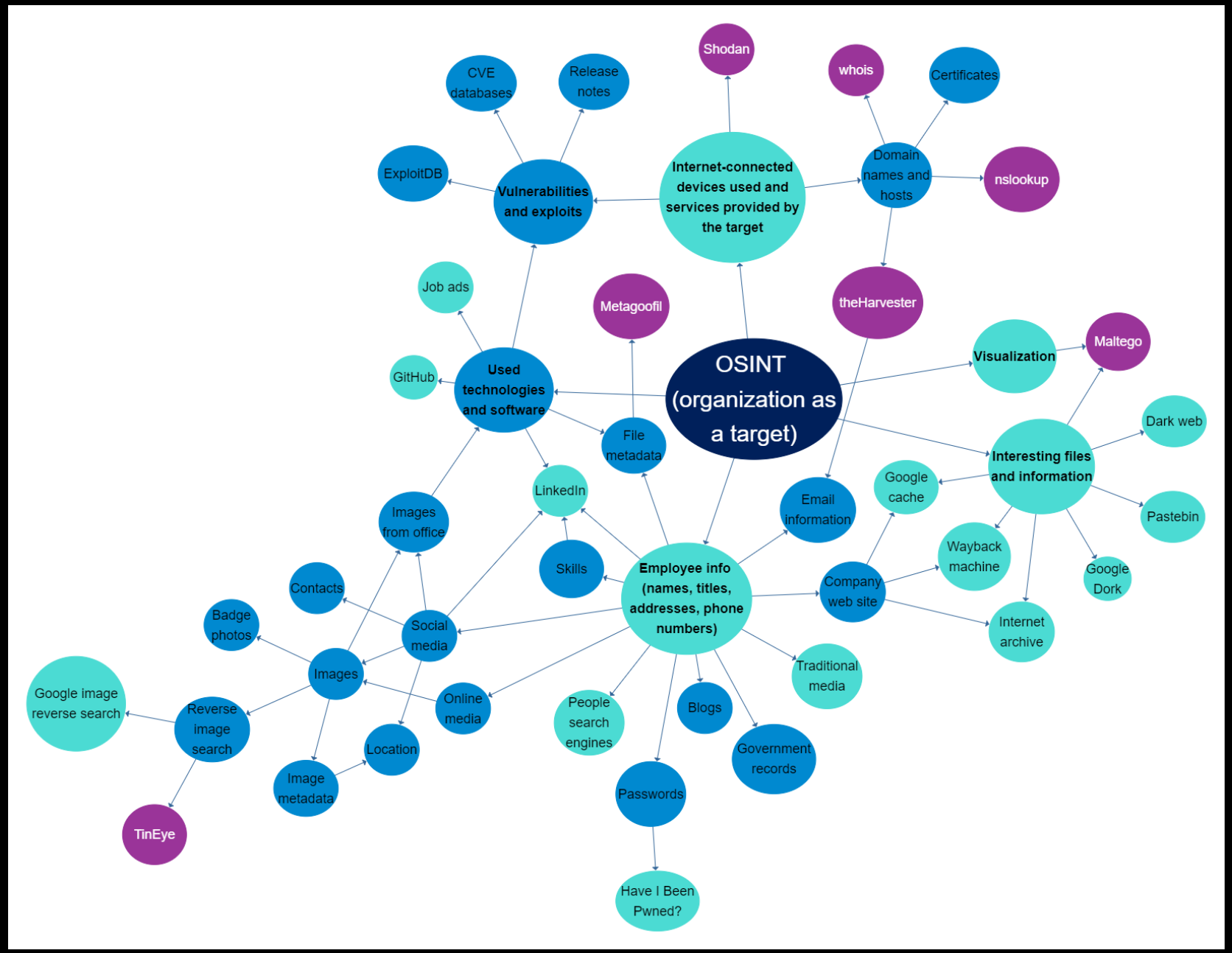
Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or threat, that can be used in prevention and/or mitigation of security incidents.

- help organizations understand the risks of the most common and severe external threats
- provides context on threat actors and associated indicators of compromise (IoC)
- Information on exploits and exploit kits - mitigation techniques

IoC – Indicator of Compromise

Forensic metadata or artifacts that identify potentially malicious activity

- metadata elements ranging from file hashes, file names to IP addresses, Ports, Domain Names, URLs, email addresses to Anomalies in Privileged User Account Activity, Geographical irregularities, Log-In red flags , HTML response sizes
- OpenIOC – standard XML schema that enables you to describe the technical characteristics that identify a known threat


OSINT (organization as a target)
Internet-connected devices used and services provided by the target
Shodan
whois
Certificates
Domain names and hosts
nslookup
theHarvester
Vulnerabilities and exploits
CVE databases
Release notes
ExploitDB
Used technologies and software
Job ads
GitHub
Metagoofil
File metadata
Visualization
Maltego
Interesting files and information
Dark web
Pastebin
Google Dork
Internet archive
Wayback machine
Google cache
Company web site
Email information
Employee info (names, titles, addresses, phone numbers)
LinkedIn
Skills
Traditional media
Social media
Contacts
Images from office
Online media
Images
Badge photos
Reverse image search
Google image reverse search
TinEye
Image metadata
Location
People search engines
Blogs
Government records
Passwords
Have I Been Pwned?

What is OSINT used for?

OSINT can be beneficial for different actors

- Government
- International Organizations
- Law Enforcement Agencies
- Business Corporations
- Businesses Corporation – Security
- Penetration Testers and Black Hat Hackers/Criminal Organizations
- Terrorist Organizations

Vulnerability Databases

Vulnerability – exploitable security weakness

- Common Vulnerabilities and Exposures (CVE) - provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures.
- U.S. National Vulnerability Database (NVD) - U.S. government repository
- Open Sourced Vulnerability Database (OSVDB) – currently VulnDB, overshadowed by NVD
- Secunia database - The Secunia database is updated continuously (daily) with CVE information.
- Symantec's Threat Database / Broadcom (SYM) - detailed information about vulnerabilities and mitigation recommendations – not what it use to be
- Microsoft Security bulletin – released on a monthly basis addressing security vulnerabilities in Microsoft software and their remediation
- MFSA: Mozilla Foundation Security Advisories - database for vulnerablities in Mozilla products
- National Computer Network Intrusion Prevention Center (NIPC) – Chinese vulnerability database
- Exploit Database @exploitdb.com – archive of public exploits and corresponding vulnerable software
- Rapid7 Vulnerability & Exploit Database - vulnerabilities and exploits database, framework in the Metasploit framework

People Search Engines:

- Spokeo
- PeekYou
- That'sThem
- Usersearch
- Qwant
- Webmii
- ZabaSearch
- Intelius
- Yasni
- iTools

Privacy centric search engines:

- DuckDuckGo
- searx.me
- Qwant
- Startpage
- Cyberd
- Infinity Search
- NotEvil
- Runnaroo
- Tineye

Threat Intelligence feeds:

- AbuseHelper
- AlienVault Open Threat Exchange
- Combine
- MalPipe
- MISP
- Pulsedive
- threataggregator
- ThreatCrowd
- Maltego

Malware samples:

- Clean MX
- Contagio
- Exploit Database
- Infosec - CERT-PA
- Javascript Mallware Collection
- Malpedia
- Malshare
- theZoo
- VX Underground

Online multi-AV analyzer

- AVCaesar
- Cryptam
- DeepViz
- DRAKVUF
- Hybrid Analysis
- IRMA
- Joe Sandbox
- malice.io
- Malwr
- VirusTotal

Online Sandbox

- anlyz.io
- any.run
- Cuckoo Sandbox
- detux
- Limon
-

Domain and IP:

- AbuseIPDB
- Desenmascara.me
- IPinfo
- Machinae
- MaltegoVT
- Multi rbl
- MXToolBox
- Spyse
- SpamHaus
- Talos Intelligence
- URLhaus
- URLQuery
- urlscan.io
- Whois – DomainTools
- ZScalar Zulu
- Malware Domain List

Phishing Threat intelligence:

- dnstwist
- mailchecker
- NormShield Services
- PhishStats
- haveibeenpwned

Cross-browser testing:

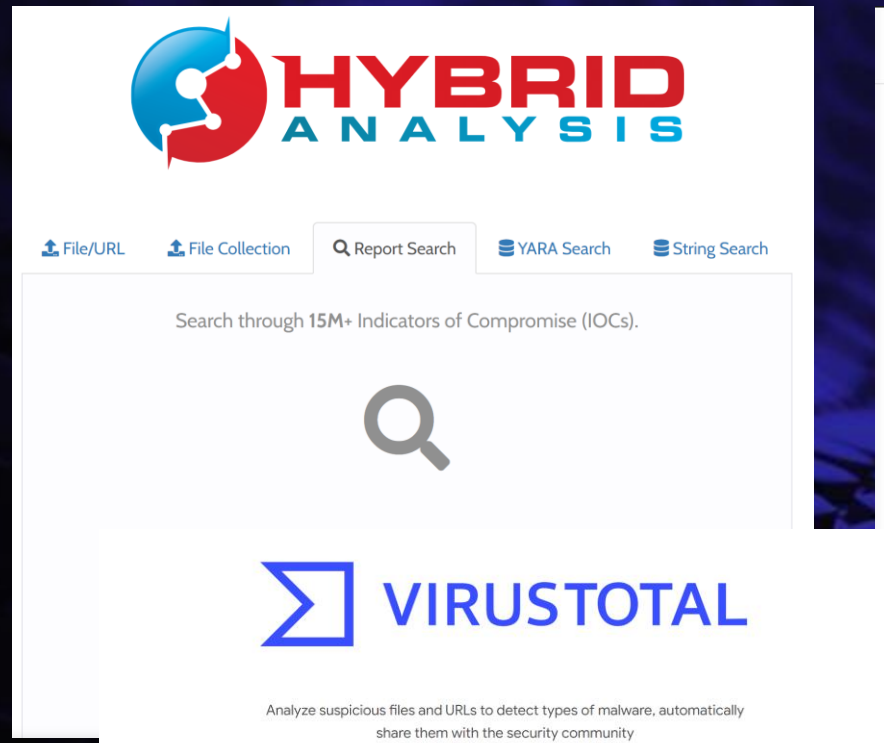
- browserling.com
- BrowserStack
- Selenium
- Karma
- LambdaTest
- Sauce Labs
- WebdriverIO

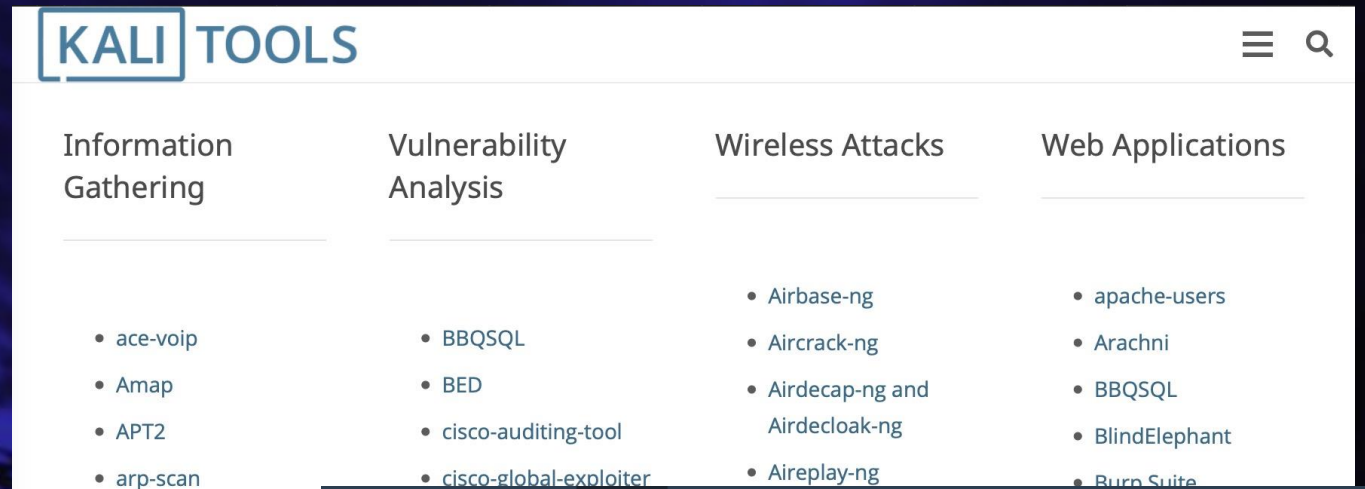
IoC resources:

- FireEye IOCs
- HoneyDB
- InQuest REPdb
- Proofpoint Threat Intelligence
- Yara rules
- YETI

Tools:

- Kali Linux
- REMnux
- TOR Browser
- CyberChef
- Wireshark
- NOTEPAD++


HYBRID ANALYSIS
File/URL
File Collection
Report Search
YARA Search
String Search
Search through 15M+ Indicators of Compromise (IOCs).


KALI TOOLS
Information Gathering
Vulnerability Analysis
Wireless Attacks
Web Applications
ace-voip
Amap
APT2
arp-scan
Automater
bing-ip2hosts
braa
CaseFile
CDPSnarf
BBQSQL
BED
cisco-auditing-tool
cisco-global-exploiter
Airbase-ng
Aircrack-ng
Airdecap-ng and Airdecloak-ng
Aireplay-ng
apache-users
Arachni
BBQSQL
BlindElephant
Burp Suite


VIRUSTOTAL
Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community
FILE
URL
SEARCH
URL, IP address, domain, or file hash
By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.
Want to automate submissions? Check our API, free quota grants available for new file uploads


urlscan.io
Home
Search
Live
API
News
About
Products New!
Login
Sponsored by SecurityTrails
urlscan.io
A sandbox for the web
URL to scan
Public Scan
Options
Recent scans
Updates every 10s - Last update: 13:32:17
URL
Age
Size
IPs
intelimasters.com/ 22 seconds 4 MB 69 10 2
www.centrumkrakowska.com.pl/ 25 seconds 716 KB 52 1 1
www.epattison.com/c4y7nk/en_index.cfm?aa=TAGS25CRYE25R3CI15HO2DH6&bba=YB4E35CA8... 25 seconds 77 KB 6 1 1
www.claudiahagedorn.de/ 27 seconds 1 MB 68 2 2
www.surveymonkey.com/r/?sm=RTUMAjuCju18kAb4aDjzCg_3D_3D 28 seconds 374 KB 20 4 2
www.latelierciuorbaleno.it/ 30 seconds 780 KB 71 3 2
support.shipshave.no/ 31 seconds 482 KB 10 1 1
www.ebiternapoli.it/ 35 seconds 621 KB 27 1 1
www.youaremythical.com/ 37 seconds 1 MB 40 1 1
ww25.capitaonefacts.com/?subid1=20201104-2231-3848-9e76-88c0945edd4d 39 seconds 193 KB 14 5 3

YARA

Tool developed to identify and classify malware samples via the use of textual or binary based rules

- often used in malware research and threat detection
- static in nature

YARA Rule: set of strings and a Boolean expression which determines a specific pattern match

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true
    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition:
        $a or $b or $c
}
```

Strings

Defines raw sequence of bytes or standard text used in pattern matching

- can be omitted
- each string is defined as a variable using the “$” identifier

Hexadecimal strings

- define a raw sequence of bytes in hexadecimal format
- allow for a more flexible special construction using wild-cards (“?”), jumps, and alternatives
- enclosed in curly brackets {}

Text strings

- ASCII-encoded, case-sensitive string
- enclosed in double quotes
- used in conjunction with **modifiers** which alter the way the string is interpreted

Regular expressions

- enclosed in forward slashes
- powerfull syntax used in defining complex patterns

Conditions

Boolean expressions that define the logic under which the rule is satisfied

- Boolean operators: and, or, not
- relational operators: >=, <=, <, >, ==, !=
- arithmetic operators: +, -, *, \, %
- bitwise operators: &, |, <<, >>, ~, ^

Special variables:

- counting strings – number of occurrences in a file, variable used is "#"
- string offsets or virtual addresses – string search in specific offset of file or specific virtual address within process address space, "at" operator is used
- file size – expressed in bytes, variable used is "filesize"
- Executable entry point – variable used is "entrypoint", can be used while scanning a running process of a PE or ELF file, will hold the virtual address of the main executable's entry point, can be used to check for packers

Metadata

Contains additional information about the rule

- defined with keyword meta
- contains identifier/value pairs

Keyword	String Types	Summary
`nocase`	Text, Regex	Ignore case
`wide`	Text, Regex	Emulate UTF16 by interleaving null (0x00) characters
`ascii`	Text, Regex	Also match ASCII characters, only required if `wide` is used
`xor`	Text	XOR text string with single byte keys
`base64`	Text	Convert to 3 base64 encoded strings
`base64wide`	Text	Convert to 3 base64 encoded strings, then interleaving null characters
`fullword`	Text, Regex	Match is not preceded or followed by an alphanumeric character
`private`	Hex, Text, Regex	Match never included in output

```
rule Base64Example1
{
    strings:
        $a = "This program cannot" base64

    condition:
        $a
}
```

```
rule CaseInsensitiveTextExample
{
    strings:
        $text_string = "foobar" nocase

    condition:
        $text_string
}
```

```
rule EntryPointExample1
{
    strings:
        $a = { E8 00 00 00 00 }

    condition:
        $a at entrypoint
}

rule EntryPointExample2
{
    strings:
        $a = { 9C 50 66 A1 ?? ?? ?? 00 66 A9 ?? ?? 58 0F 85 }

    condition:
        $a in (entrypoint..entrypoint + 10)
}
```

```
rule AtExample
{
    strings:
        $a = "dummy1"
        $b = "dummy2"

    condition:
        $a at 100 and $b at 200
}
```

Limitations

Signature-based protection is not enough. Packing, encryption, polymorphism can easily bypass any YARA centric detection.

- YARA only does pattern/string/signature matching in a static manner
- cannot be applied to live network traffic

Although YARA rules can be found online, they require heavy customization and complex configuration to be applied to a dynamic environment. Enter SNORT.

"YARA is to files what Snort is to network traffic."
-- Victor Manuel Alvarez, Yara Developer

Who uses YARA:

- AlienVault
- Avast
- CrowdStrike FMS
- Cuckoo Sandbox
- ESET
- FireEye, Inc.
- inQuest
- Joe Security
- Avast
- Kaspersky Lab
- Lastline, Inc.
- McAfee Advanced Threat Defense
- PhishMe
- RSA ECAT
- Symantec
- Tenable Network Security
- ThreatConnect
- Trend Micro
- VirusTotal Intelligence

```
Stephans-MacBook-Pro:FuxSocy stephansimon$ cat fuxsocy.yar
rule FuxSocy : ransomware
{
    meta:
        author = "Stephan Simon <stephan.simon@binarydefense.com>"
        date = "2019-10-24"
        description = "A ransomware tweeted about by @malwrhunterteam"
        modified = "2019-10-24"
        reference = "https://twitter.com/malwrhunterteam/status/1187360440734625798"
        tlp = "WHITE"
    strings:
        $n1 = "FuxSocy_Evaluated" wide
        $n2 = "FuxSocy_InstallPlace" wide
        $n3 = "FuxSocy_Instance" wide

        $s1 = "{RAND}" wide
        $s2 = "\\x*x.exe" wide
        $s3 = "%.4d-%.2d-%.2dT%.2d:%.2d:%.2d" wide
        $s4 = "PT1M" wide
        $s5 = "PT0S" wide
        $s6 = "/d /c taskkill /f /pid %d > NUL & ping -n 1 127.0.0.1 > NUL & del \"%s\" > NUL & exit" wide
        $s7 = "/d /c start \"\" \"%s\"" wide
        $s8 = "Win32_ShadowCopy.ID='%s'" wide
        $s9 = "SuperHidden" wide
        $s10 = "ShowSuperHidden" wide
        $s11 = "Shell.IPC.%s" wide
        $s12 = "\\StringFileInfo\\%04x%04x\\%s" wide
    condition:
        uint16(0) == 0x5a4d and
        filesize <= 100KB and
        (1 of ($n*) or 4 of ($s*))
}
Stephans-MacBook-Pro:FuxSocy stephansimon$ du -h -d 0 ~/Documents/Malware
5.6G    /Users/stephansimon/Documents/Malware
Stephans-MacBook-Pro:FuxSocy stephansimon$ yara -r fuxsocy.yar ~/Documents/Malware
FuxSocy /Users/stephansimon/Documents/Malware/FuxSocy/c6866a33a75b9c6c1d90e76729d6879206c7786f323fbbf9d0552c7b037fa87c.bin
Stephans-MacBook-Pro:FuxSocy stephansimon$
```

YARA rule for FuxSocy randsomeware

RegEx

Powerful search mechanism for patterns in files and databases, functionality which is incorporated into many modern programming languages

- used in conjunction with tools like Perl, grep, sed or awk for parsing large amounts of data

Commonly, security tools or devices deployed on a network are using some form of Regex to parse the data it inspects. These could be NGFirewalls, Snort rules, logs collected by SIEM (Splunk, Kibana).

Retrieve IP address from subnet 192.168.25.0/24 from a logfile

```
grep "192\.168\.25\.[[:digit:]]\{1,3\}" query.log
grep -e "192\.168\.25\.\{1,3\}" query.log
```

Remove ‘http’ from file using regex and sed

```
sed 's/http://g' file.txt > newfile.txt
```

Remove empty lines and count

```
file.txt wc –l
sed '/^$/d' file.txt | wc -l
```

Short RegEx Refercence

. matches any single character except for \n (newline.)
* Modifier. Zero or or more of the preceding character. ".*" to match a bunch of characters. "*" by itself probably won't do what you want, because "*" is a modifier.
+ Modifier. One or more of the preceding character. Same idea as "*", except that it requires at least one character to be present.
? Modifier. Zero or one of the preceding character.
\d Single digit. [0-9]. Use \d+ to match one ore more digits.
\w Word character. [A-Za-z0-9_] Upper and lower case letters, digits and underscore. No punctuation.
\s White space [\r\t\n\f] Space, carriage return, tab, new line, or form feed.
\b Word boundry anchor. Anything that can come before or after a word. White space, punctuation and/or the beginning or end of a line.
^ Anchor. Requires that the pattern be at the beginning of the line. The "^" in the /^([A-Z][a-z]{2}) (match month) example means that this pattern must be at the beginning of the line to match.
^ Negation. "^\d" would match any single character except for a digit. Um, context counts.
$ Anchor. Same thing, only for the end of the line.

References:

- https://medium.com/factory-mind/regex-tutorial-a-simple-cheatsheet-by-examples-649dc1c3f285
- https://www.regexlib.com/CheatSheet.aspx?AspxAutoDetectCookieSupport=1
- https://regexr.com/

www.menti.com

Code: 40201561

Thank you!