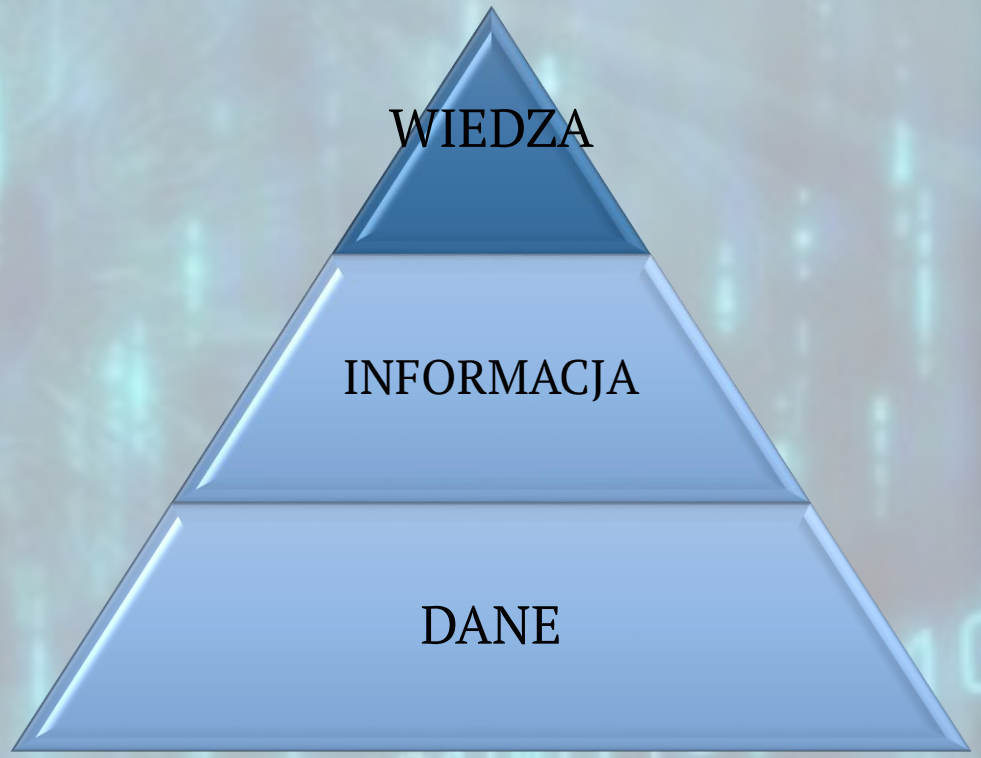
Cyber threat intelligence (CTI) – narzędzia do analizy potencjalnych wycieków informacji

kpt. Grzegorz Data
OISW w Rzeszowie

Popowo, wrzesień 2018

Cyber Threat Intelligence

- Można je tłumaczyć jako rozpoznanie, wywiad, czy nawet analizę zagrożeń cybernetycznych (informatycznych).
- Jedna z najkrótszych definicji (przez analogię do *business intelligence*) to proces przekształcania **danych** o zagrożeniach cybernetycznych w **informację** (dane w określonym kontekście) a informacji w **wiedzę**.



Źródła CTI

- Wewnętrze –wszystkie informacje zbierane wewnątrz organizacji. firewalle, systemy zapobiegania włamaniom (IPS), systemy zabezpieczeń, antywirusy,.
- Społecznościowe – każdą społeczność, relacje zaufania i wspólne interesy, nieformalna grupa np. przedsiębiorców reprezentujących tę sama gałąź przemysłu lub zrzeszenie wyższych uczelni.
- Zewnętrzne –wszystkie informacje zdobywane spoza własnej organizacji lub zaufanych partnerów.
  - źródła publiczne.-dostępne dla każdego i zwykle są bezpłatne. (CVE,CPE,CVSS,NVD,CVSS, OTX, ET, malshare, abuse…)
  - Źródłą zamknięte udostępniających adresy IP, domeny skróty niebezpiecznych plików, w różnych formatach, często po uprzedniej rejestracji (*SANS Institute , 2013, pp. 9-10), (Liska, 2015)*.

Wymiana Wiedzy

- Z modelu „Need to Know” do „Need to Share”, „Sharing is Caring”
- Wszystkie formy rozpoznania zagrożeń, jeśli są dzielone, pomogą innym organizacjom w obronie przed atakami
- Organizacja lub firma może ponieść straty, gdy ktoś włamie się do komputera z konkurencji, ponieważ informacje skradzione mogą być często używane przeciwko innym organizacjom z tego samego sektora (MWR Infosecurity, 2015).

Serwisy wspomagające wykrywanie incydentóe

virustotal.com (file, url, haash)
community.riskiq.com (pasivetotal) (url IP)
reverse.it – sandbox (hash, file, URL)
hybrid-analysis.com (hash, file, URL)
censys.io (IP, url)
exchange.xforce.ibmcloud.com - framework
community.riskiq.com (IP, url
www.shodan.io
totalhash.cymru.com
www.malwares.com

CRITS
Collaborative Research Into Threats

platforma do zespołowych badan nad zagrożeniami

- MITRE 2010 Mike Goffin, zarządzanie złośliwym oprogramowaniem. Kod uwolniono 18 czerwca 2014 r.
- Ułatwia agregację, analizę i dzielenie się technicznymi informacjami o zagrożeniach cybernetycznych.
- Zarządza olbrzymią ilością danych zgromadzonych przy analizie pojedynczych, często odmiennych ataków cybernetycznych i przeprowadza analizy w celu odkrycia wzorców w celach, narzędziach i technikach przeciwnika.
- CRITS składa te pozornie rozłączone kawałki układanki w spójny obraz zagrożenia cybernetycznego. Używając wspólnego słownictwa, CRITS natychmiast rozpowszechnia to "zdjęcie" do innych użytkowników, aby zapobiec przyszłym naruszeniom.

CRITS struktura

- Obiekty (Top-Level Objects - TLOs):

  Actors Campaigns Certificates Domains Emails Events Indicators IPs PCAPs Raw Data Samples Targets

- Pojęcia:

  Bucket Lists, Campaign Attribution, Comments Downloading, Email Targets, Favorites, Notifications, Objects, Relationships, Releasability Screenshots, Sectors, Sources, Subscriptions

- Serwisy:

  Chopshop, clamd, Cuckoo, entropycalc, exiftool, macroextract, malshare, metachecker, office_meta, passivetotal, pyew, pdfinfo, pdf2txt, relationships, shodan, taxi,stix, threatexchange, virustotal, whois, yara – 56 rozszerzeń.

CRITS struktura

PREZENTACJA

MISP
Malware Information Sharing Platform

- Zbieranie, przechowywanie, dystrybucja i udostępnianie wskaźników zagrożenia bezpieczeństwa cybernetycznego.
- Analiza na temat incydentów związanych z bezpieczeństwem cybernetycznym i analiza złośliwego oprogramowania.
- Wsparcie dla misji NCIRC TC – *NATO Computer Incident Response Capability Technical Centre*.
- Posiada łatwo przeszukiwane repozytorium z wielokierunkowym mechanizmem dzielenia się informacjami.
- Posiada zaawansowaną automatyzacje przy eksporcie i imporcie danych i łączeniu się z innymi systemami.
- Głównym cel to przyśpieszenie wykrywania incydentów bezpieczeństwa, które nie mają jeszcze zdefiniowanych sygnatur lub wyrafinowanych ataków APT (NATO Communications and Information Agency, 2015)

MISP główne cechy

- Wydajna baza wskaźników kompromitacji oraz wskaźniki pozwalające na przechowywanie informacji technicznych i nietechnicznych o złośliwych próbkach, incydentach, atakujących i rozpoznaniu.
- Automatyczna korelacja odnalezionych powiązań między atrybutami i wskaźnikami.
- Wbudowana funkcjonalność współdzielenia, ułatwiająca wymianę danych za pomocą różnych formatów. MISP automatycznie synchronizuje zdarzenia i atrybuty od innych serwerów
- Intuicyjny interfejs użytkownika dla użytkowników końcowych do tworzenia, współdziałania i aktualizacji informacji o wydarzeniach i wskaźnikach kompromitacji.

MISP główne cechy

- Przechowywanie danych w formie strukturalnej (umożliwiające zautomatyzowane korzystanie z bazy danych dla różnych celów, np. jako źródło danych dla systemów bezpieczeństwa) ze wsparciem wskaźników cyberbezpieczeństwa a także wskaźników oszustwa, (fraud) do współpracy z sektorem finansowym.
- Eksport: generowanie sygnatur dla IDS (Suricata, Snort i Bro), OpenIOC, tekst, CSV, MISP XML lub JSON do integracji z innymi systemami (NIDS HIDS) STIX (XML i JSON), NIDS oraz wiele innych formatów
- import: import całych zestawów, , import z OpenIOC, sandoboksa, ThreatConnect CSV. wiele innych formatów
- udostępnianie danych: automatycznej wymiana i synchronizacja z innymi organizacjami i społecznościami korzystającymi z MISP.

MISP główne cechy

PREZENTACJA

CUCKOO

- Sandbox, środowisko fizyczne i wirtualne (kvm, esx, virtualbox, qemu, vsphere, xenserver– Windows, Linux, OS X, Android (agent napisany w pythonie).
- Sieć – Net, VPN, InetSIM, TOR, Suricata Snort, MITM,
- Formaty - exe,dll, pdf, office, url, html, php, cpl, VB, zip, yar, py, apk,…
- Zrzuty pamięci, PCAP, procesy, wywołania API, screenshot.
- Tworzy pliki, symulowane jest poruszanie kursorem, maszyna przywracana ze snapshota.
- Współpraca – CRITS, MISP, VirusTotal, Moloch, IRMA, elasticsearch, mattermost.

CUCKOO

PREZENTACJA

AIL

Framework doanalizy wycieków informacji

- AIL to modułowa platforma do analizy potencjalnych wycieków informacji z niestrukturalnych źródeł danych, takich jak posty z pastebin lub podobnych usług lub innych strumieni danych. Struktura AIL jest elastyczna i można ją rozszerzyć, aby obsługiwać inne funkcje do wydobywania lub przetwarzania poufnych informacji (np. Zapobieganie wyciekom danych).

AIL

- Modułowa architektura do obsługi strumieni niestrukturalnych lub strukturalnych informacji
- Obsługa wielu kanałów
- Wyodrębnianie i weryfikowanie potencjalnych wycieków numerów kart kredytowych, danych uwierzytelniających, ...
- Wykrywanie i wyodrębnianie adresów URL, w tym ich położenie geograficzne (np. Lokalizacja adresu IP)
- Wyodrębnianie i sprawdzanie poprawności adresów e-mail wyciekło, w tym sprawdzanie poprawności DNS MX
- Moduł do wyodrębniania adresów Tor.onion (do dalszego przetwarzania w celu analizy)
- Wysyłanie alertów do MISP w celu udostępnienia znalezionych wycieków w ramach platformy wywiadowczej zagrożeń przy użyciu standardu MISP
- Systemu znakowania z MISP Galaxy i MISP taksonomii tagów
- Twórz wydarzenia i alerty w MISP i sprawy w The Hive

AIL

PREZENTACJA

TheHIVE

- Skalowalna, otwarta i bezpłatna platforma reagowania na incydenty bezpieczeństwa, ściśle zintegrowana z MISP (platformą wymiany informacji o złośliwym oprogramowaniu), zaprojektowana w celu ułatwienia życia organizacjom społecznym, zespołom CSIRT, CERT i wszelkim praktykom zajmującym się bezpieczeństwem informacji w zakresie incydentów bezpieczeństwa, które należy zbadać i podjąć działania szybko.

CORTEX

- Wielu analityków SOC i CERT może współpracować przy badaniach jednocześnie. Dzięki wbudowanemu strumieniowi na żywo, informacje w czasie rzeczywistym dotyczące nowych lub istniejących spraw, zadań, obserwowalnych i IOC są dostępne dla wszystkich członków zespołu. Specjalne powiadomienia umożliwiają im obsługę lub przypisywanie nowych zadań, przeglądanie nowych zdarzeń MISP, alarmy SIEM, raporty e-mail, importowanie i zbadanie ich od razu.
- Można dodawać kilka(naście, set) obserwabli do każdego przypadku, który tworzymy lub importujemy bezpośrednio ze zdarzenia MISP lub dowolnego alertu wysłanego na platformę(np. AIL). Można je segregować i filtrować. Automatycznie można badać za pomocą analizatorów, istnieje możliwość tagowania, oznaczania IOC, porównywać z już przeanalizowanymi przypadkami , po analizie można wyeksportować do MISP.

CORTEX

Dzięki Cortex obserwowalne obiekty, takie jak adresy IP i adresy e-mail, adresy URL, nazwy domen, pliki lub skróty można analizować za pomocą interfejsu WWW. Analitycy mogą również zautomatyzować te operacje i przesłać duże zestawy obserwowalnych z TheHive lub interfejsu API REST z Cortex z alternatywnych platform SIRP, niestandardowych skryptów lub MISP.

HIPPOCAMPE

- Hippocampe regularnie pobiera i analizuje źródła informacji o zagrożeniach, publiczne lub prywatne, z Internetu i przechowuje je w Elasticsearch.

THE HIVE, CORTEX, HIPPOCAMPE

PREZENTACJA

SCUMBLR

Scumblr to aplikacja internetowa Ruby on Rails, która umożliwia wyszukiwanie w Internecie witryn i treści. Scumblr zawiera zestaw wbudowanych bibliotek, które umożliwiają tworzenie wyszukiwań popularnych witryn, takich jak Google, Facebook i Twitter, 4chan, 8chan, Pastebin, iTunes Store, Certificate Transparency, Ebay, Google Play, Reddit, RSS Feeds and YouTube W przypadku innych witryn tworzenie wtyczek jest łatwe, dzięki czemu można przeprowadzać ukierunkowane wyszukiwania i zwracać wyniki. Po skonfigurowaniu Scumblr możesz uruchomić wyszukiwania ręcznie lub automatycznie cyklicznie..

Scumblr integruje się również z Sketchy, co pozwala na automatyczne generowanie zrzutu zidentyfiko- wanych wyników, aby zapewnić migawkę w czasie na temat tego, jak dana strona i wynik wyglądały, gdy zostały zidentyfikowane.

SCUMBLR

- Skanuje sieć, szukając wycieku danych lub poufnych informacji
- Powiadomienie o naruszeniach danych i publicznie dostępnych zrzutach danych do MISP
- Monitoruje witryny mediów społecznościowych pod kątem świadomości marki lub potencjalnych zagrożeń

SCUMBLR

PREZENTACJA

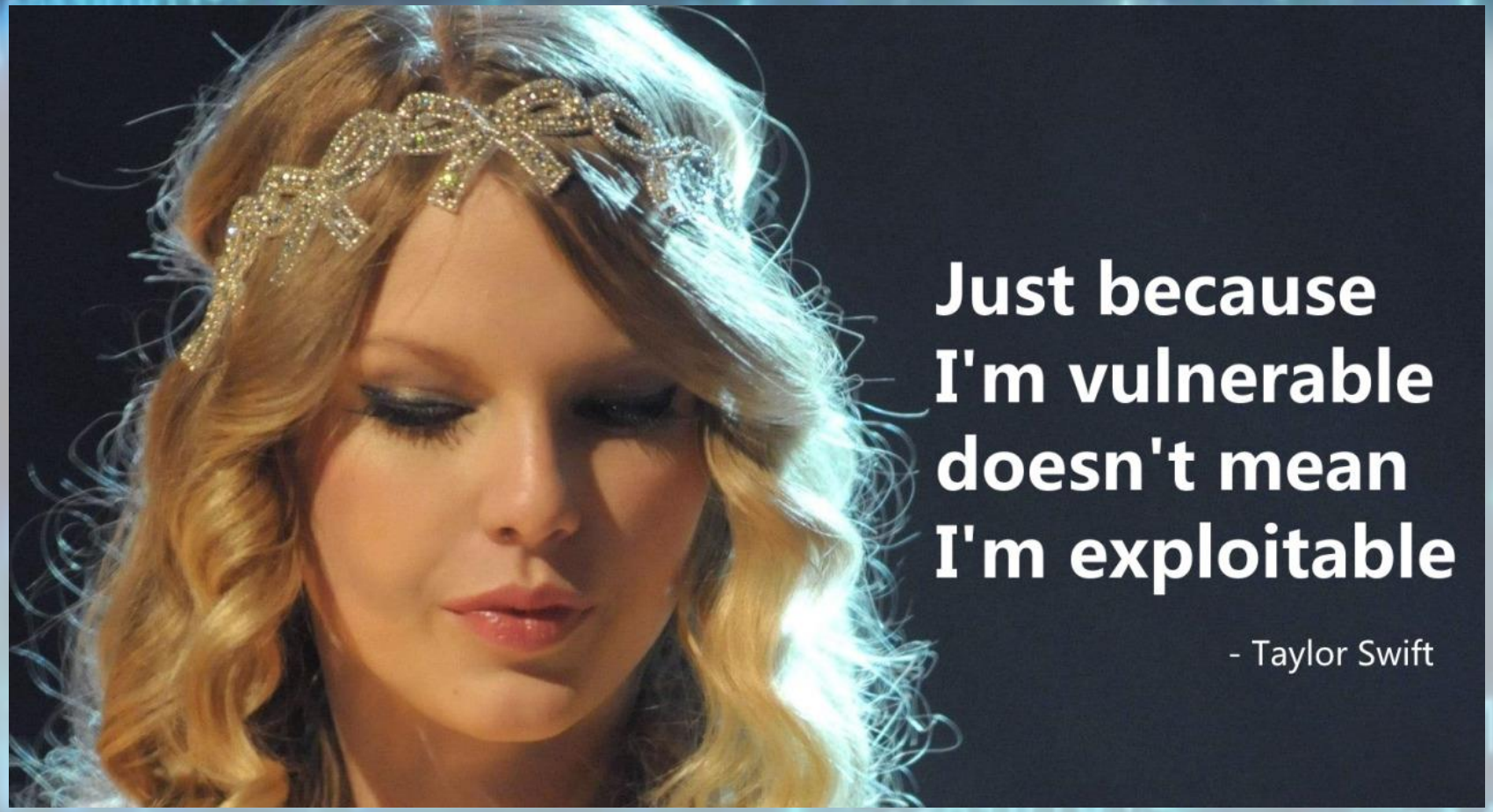
SPIDERFOOT

- SpiderFoot to narzędzie rozpoznawcze, które automatycznie przesyła zapytania do ponad 100 publicznych źródeł danych (OSINT) w celu zebrania informacji wywiadowczych na temat adresów IP, nazw domen, adresów e-mail, nazw i innych. Wystarczy określić cel, wybrać moduły do włączenia, a następnie SpiderFoot zbierze dane, aby uzyskać zrozumienie wszystkich elementów i ich wzajemne relacje.
- Dane zwrócone ze skanowania SpiderFoot ujawnią wiele informacji o twoim celu, zapewniając wgląd w możliwe wycieki danych, luki lub inne wrażliwe informacje, które można wykorzystać podczas testu penetracji, ćwiczenia w zespole czerwonym lub w celu wykrycia zagrożenia. Warto wypróbować go go w swojej własnej sieci, aby zobaczyć, mogło wyciec!

SKANERY PODATNOŚCI

- OpenVAS to w pełni darmowy oraz łatwo dostępny framework pełniący rolę skanera podatności. Służy do badania urządzeń sieciowych, szerokiej gamy systemów operacyjnych oraz wielu usług sieciowych pod kątem podatności na różnego typu ataki. OpenVAS potrafi przeskanować obrany cel, sporządzić listę wykrytych podatności oraz zaproponować sposób na zwiększenie poziomu bezpieczeństwa.Jest to fork Nessusa (obecnie płatny), inny skaner to Nexpose firmy RAPID7. do szybkiego i prostego skanu wystarczy nmap.
- Sn1per – prosty framework obsługujący różne skrypty.

SKANERY PODATNOŚCI



Malware do analizy

- MALTRIEVE - Narzędzie do pobierania złośliwego oprogramowania bezpośrednio ze źródła można bezpośrednio wysłać do VIPER, CUCKOO, CRITS
- ph0neutria - Malc0de, Malshare, VX Vault. System tagów
- The ZOO – „ Repozytorium złośliwych programów LIVE dla twojej własnej radości i przyjemności”
- VIPER - Viper to binarna platforma do analizy i zarządzania. Jego podstawowym celem jest dostarczenie rozwiązania umożliwiającego łatwe organizowanie kolekcji złośliwego oprogramowania i wykorzystywanie próbek, a także zbiór skryptów utworzonych lub znalezionych w danym czasie w celu ułatwienia codziennych badań.

Reguły Wymiany
Traffic Light Protocol (US-CERT)

Kolor	Znaczenie dla odbiorcy
TLP: RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.
TLP: AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań.
TLP: GREEN	Odbiorcy mogą dzielić się informacji ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.
TLP: WHITE	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).
CHR:	zasada zezwalająca na upublicznianie uzyskanych informacji, pod warunkiem nieujawniania tożsamości.

Dziękuję za uwagę

kpt. Grzegorz Data
OISW w Rzeszowie

tel: 17 8580775
voip: 6021060
email: grzegorz.data@sw.gov.pl
JID: 021036gdat@swnet.sw.gov.pl