**Advanced Cyber Threat Intelligence Report**

CYB-670

Student Name: Sam Perryman

Instructor Name: Babur Kohy

**Section 1: Incorporating Threat Intelligence into Incident Responses**

Threat intelligence plays a critical role in incident response by providing security data and information that helps organizations utilize the latest strategies and tactics to detect, respond to, and mitigate cyber threats and gain a more thorough sense of their threat landscape. “The goal of threat intelligence is to make threat intelligence an integral part of your cybersecurity strategy, enabling a proactive rather than reactive approach to threats” (Forbes 2024). Throughout each step of incident response, there are occasions to use threat intelligence to aid in the response process.

Threat intelligence is described by Kirvan, Cobb, and Wigmore as “information gathered from a range of sources about current or potential attacks against an organization…” (Kirvan et al., 2024). Threat intelligence is intended to give organizations an idea of the risk from external threats, including everything from zero-day vulnerabilities to advanced persistent threats though it also provides detailed information like context of the threats, attacker identities and motivations, and indicators of compromise.

**Threat Intelligence Types**

Computer Security Incident Response Teams (CSIRT), security analyst, and other IT professionals navigate the volumes of data resulting from threat intelligence by first understanding the four main types strategic, tactical, operational, and technical. Each focus on a different aspect of threat intelligence, combining to create comprehensive assessment environment. Strategic intelligence is focused on the collection and analysis of data that can be used to predict potential cyberattacks and its consequences. It is also considered to be a high-level view of an industry or organization’s threat landscape. Tactical intelligence is like a link between strategic and operational intelligence as it includes evidence-based knowledge about tactics, techniques, and procedures used by attackers, ground level details of threats, malware signatures, and indicators of compromise. Operational intelligence focuses on information collected from chat rooms, social media, antivirus logs, and past events to determine information for cyberattacks or campaigns. Technical intelligence concentrates on the signs that a cyberattack has begun and identifies the attack surface.

**Intelligence Lifecycle**

The lifecycle of intelligence is seen as a repeating circle of 5 steps: Goals and objectives, data collection, data processing, analysis of data, and reporting findings. The first step, goals and objectives, refers to the process of determining which threat intelligence sources and tools will be most effective and what hope to be achieved. Data is collected from logs and third-party data feeds such as hacker forums, social media, malicious IP addresses, and threat research reports. This data is then processed by automated systems and applications that correlate and aggregate data for dissemination. Once data is processed, it can be analyzed to answer questions like when, why, and how suspicious events occurred. Intelligence reports are then tailored to specific teams to identify how their area of responsibility is affected. The information in these reports is then used to set goals and objectives as the process begins anew.

An incident response is the result of an event triggering an alert, followed by a group of correlated alerts forming an incident that is deemed a genuine threat by human or automated tools. Incidents can occur in the form of phishing, ransomware, man in the middle, or unauthorized access to name a few. TTPs refers to the tactics, techniques, and procedures used in cyber attacks. “Tactics describe the technical objective an adversary is trying to achieve (“why”), techniques are different mechanisms they use to achieve it (“what”), and procedures are exactly how the adversary achieves a specific result (“how”).” (Cybersecurity and Infrastructure Security Agency 2024). The alternatives in types of incidents and the varying TTPs that can be used for each necessitates an incident response plan that “defines roles and responsibilities and includes the steps needed to properly resolve, document, and communicate about an incident” (Microsoft n.d.). Response plans not only provide detailed information on what should be done at each phase of an attack, but they also can be used in the aftermath to give customers and stakeholders peace of mind that all necessary steps were taken in response to the incident.

Incident response frameworks are provided by several organizations including NIST (National Institute of Standards and Technology, CISA (Cybersecurity and Infrastructure Security Agency), the SANS Institute, ISO (International Organization for Standardization), CrowdStrike and others. According to CISA’s “Cyber Incident Response” description, its playbook “Provides incident response, management and coordination activities for cyber incidents occurring in the critical infrastructure sectors as well as Government entities at the Federal, State, Local, Tribal, and Territorial levels” (Cybersecurity and Infrastructure Security Agency n.d.). This playbook also looks to track successful actions across the organization as well as assisting with cataloging incidents. Incidents that contain confirmed malicious activity and carry a major incident declaration or the reasonable possibility of one apply to this playbook.

CISA’s incident response process is triggered with the identification of and communication of an incident to CISA and agency network defenders’ constitution a declaration, though this does not require an official declaration of a major incident. CISA also breaks the incident response lifecycle into five phases Preparation, detection and analysis, containment, eradication and recovery, post-incident activity, and coordination. This differs from the NIST framework in the containment, eradication, and recovery and separated into two phases and the coordination phases is added.

**Preparation Phase**

The preparation phase has a goal of ensuring resilient architectures and systems so that even in a compromised state, critical operations are maintained by, preparing for major incidents to mitigate the impact on the organization as well as developing an understanding of “normal” activity through established system and network baselines. Strategic and operational threat intelligence can play a key role in the preparation phase for several ways by helping to identify threats, and updating plans, and in the training of personnel to name a few. When using threat intelligence an organization can develop an idea of the types and attacks it may face based on industry trends found in TI feeds. The ability to assess and update IR plans and training opportunities can be derived from adversary indicators, TTPs, and associated defensive measures shared through CISA’s Automated Indicator Sharing program.

**Detection and Analysis Phase**

The detection and analysis phase involves one of the more difficult aspects of incident response, accurately determining whether an incident occurred, and if so its type, extent, and severity. The purpose of this phase is “To detect and analyze events, implement defined processes, appropriate technology, and sufficient baseline information to monitor, detect, and alert on anomalous and suspicious activity. Ensure there are procedures to deconflict potential incidents with authorized activity” (Cybersecurity and Infrastructure Security Agency 2024). One example of the tactical intelligence used during this phase is to “Compare TTPs to adversary TTPs documented in ATT&CK and analyze how the TTPs fit into the attack lifecycle.” (Cybersecurity and Infrastructure Security Agency 2024).

**Containment Phase**

Containment, always a high priority for incident response, can include isolation of affected systems and networks, creating forensic images to preserve evidence, updating firewalls, blocking unauthorized access, changing administrative passwords, rotating private keys, and directing adversaries to a sandbox for observation. Based on operational and tactical intelligence the best containment strategy to use can depend on potential loss or damage to IT assets, forfeiture of critical services, time required to implement, and level of effectiveness. Real-time updates found on incident databases also allow IR teams to adjust containment strategies based on current best available threat reporting. Another way that threat intelligence plays a role in containment is “validating the IP addresses used to launch threats and cross-referencing them with IP addresses used in previous or similar incidents” (RSI Security, 2022) using tools such as MITRE ATT&CK framework, AbuseIPDB, or Auth0 Signals.

**Eradication and Recovery Phase**

The purpose of the eradication and recovery phase is to resume normal operations by removing all artifacts of the incident and performing remediation tasks on the vulnerabilities that allowed for the incident to occur. According to CISA, eradication activities include remediation of infected IT environments, reimaging affected systems, replacing compromised files, installing patches, and developing response scenarios for alternative attack vectors. Recovery includes connecting new and rebuilt systems to the network, tightening perimeter security, testing systems, and monitoring operations. (Cybersecurity and Infrastructure Security Agency 2024). Technical, operational, and strategic threat intelligence is incorporated into this phase guiding eradication efforts and when updating security measures. Detailed information on a threat’s behavior can drive eradication decisions based on known persistence mechanisms, while threat intelligence can also outline new updated configurations and patches to assist in recovery and prevention of future incidents.

**Post Incident Activity Phase**

The post-incident activity phase, which is the fourth and final phase of the NIST framework, is the time to perform a comprehensive examination of the incident to determine root cause, vulnerabilities, and steps taken in response. This is also an opportunity to meet with stakeholders and personnel to advise them on the details of the incident and the lesson that should be learned from it. NIST recommends questions like those below are asked and answered.

* Exactly what happened and at what time?
* How well did staff perform in dealing with the incident?
* Were documented procedures followed?
* What information was needed sooner?
* How could information sharing with other organizations have been improved?
* What corrective actions can prevent similar incidents in the future?
* What precursors or indicators should be watched for in the future to detect similar incidents?
* What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

(National Institute of Standards and Technology 2012)

Answering these questions can help one to achieve the objective of the post-incident analysis which is to “understand the intricacies of an incident to reveal invaluable insights that can inform future cybersecurity strategies, build organizational resilience, and pave the way for improved and optimized security operations” (Mukherjee 2023). Applying strategic and operational intelligence, this phase uses artifacts like the forensic images created during the Containment phase. Organizations should have established protocols and processes for efficiently preserving evidence including a chain of custody and adherence to any government and industry regulations. Threat intelligence plays a role in this phase by aiding in quick identification of threats to help minimize damage and learning from past incidents to refine defense and prepare for future attacks.

**Coordination Phase**

The coordination phase is for establishing channels for follow-up communications and identifying stakeholders to establish who will participate in incident response. For this final phase, threat intelligence can be used to compare alternative plans to find the best available options.

**Section 2: Alien Vault OTX Exercise Results**

Using the lab instructions for the Alien Vault OTX exercise, respond to each of the following questions:

1a. What is the name, category, count, and feature count of the malware with largest circle in the dashboard view?

***Name - Backdoor: Win32/Berbew***

***Category – Backdoor***

***Count – 26,626***

***Feature Count – 6***

1b. Pick one of the related pulses for the malware you selected and list the ID of the pulse, the total number of IOCS and type and count for each. Also, provide a screenshot of the results.

***Name - [GS 543] Miria Botnet IOCs 0 SEC-1275-1***

***ID – 66fe3c5883a62e0d171b78***

***Total IOCs – 517***

***FileHash-SHA256 – 157***

***FileHash-SHA1 – 157***

***FileHash-MD5 – 157***

***IPv4 – 38***

***URL – 4***

A blue and yellow color scheme

Description automatically generated with medium confidence

1c. For the same pulse you selected in part b, show the threat infrastructure screenshot along with the ID of pulse, and a table with the specific breakdown of counts for each country.

***Pulse ID – 66fe3c5883a62e0d171b78***

A screenshot of a computer

Description automatically generated

|  |  |  |
| --- | --- | --- |
|  | Country | Counts |
|  | Hong Kong | 10 |
|  | Other | 10 |
|  | United States | 9 |
|  | Czechia | 2 |
|  | France | 2 |
|  | Vietnam | 2 |

1d. Use the Browse->Indicators tab to provide a count for the IPv4 and IPv6 IOCs. In your response provide the exact count of IPv4 and IPv6 IOCs at the time of your query. Which count is larger between the IPv4 and IPv6? Explain why one has significantly more counts than the other.

***IPv4 – 14,000 | IPv6 – 215***

***IPv4 is has more indicators, due in part to it using a 32-bit address format with up to 4.3 billion addresses, while IPv6 uses a 128-bit address format allowing roughly 340 undecillion addresses. IPv4 also has been in use longer creating more extensive attack and vulnerability history.*** A screenshot of a computer

Description automatically generated

1e. Use the Browse->Indicators tab to search the role of Ransomware. What IOC type makes up most of the Ransomware IOCs for this query?

***The IOC type with the most occurrences for this query is FileHash-SHA256 with 121.***

f1. How many pulses has the user MetaDefender contributed? (Hint: /api/v1/pulses/user/{username}, You will need to use your OTX-API-KEY to retrieve this result.)

***MetaDefender has contributed 15,221 pulses. Syntax used - “curl https://otx.alienvault.com/api/v1/pulses/user/MetaDefender -H "X-OTX-API-KEY: e0f3f5da917e8d6939812a342f5e37e81f30dae157785f1c17a616d6a0d3b850”***

f2. What is the slug string for the Bitcoin Address indicator type. (Hint: the API will list the indicator, types, descriptions, slugs and other information)

***The slug string for the Bitcoin Address indicator type is “bitcoin\_address”.***

f3. Have there been any malware samples analyzed by AlienVault Labs which have been observed connecting to microsoft.com? If yes, then list one malware detected and the date of the detection. (Hint: /api/v1/indicators/domain/{domain}/{section}, Use malware for the section).

***Yes, 46,537***

***Win.Trojan.Tofsee-7102058-0***

***curl https://otx.alienvault.com/api/v1/indicators/domain/http://microsoft.com/malware***

f4. When does the SSL certificate for webapps.umgc.edu expire? (Hint: api/v1/indicators/domain/{domain}/http\_scans, Look for “443 Certificate Notafter”)

***Sep 4 23:59:59 2021 GMT***

***curl https://otx.alienvault.com/api/v1/indicators/domain/webapps.umgc.edu/http\_scans***

2. Summarize in 2-3 paragraphs, how you would use Alien Vault OTX as part of a cybersecurity program you managed or were part of. Discuss how it might integrate with other development tools and inform and be part of strategic, operational, and tactical threat intelligence.

AlienVault Open Threat Exchange (OTX) is a platform that allows you to access and share threat intelligence. Linke many cybersecurity tools, OTX has the ability to integrate with other tools that can be helpful and enhance its uses. This collaborative use of tools is aimed at enhancing an organization’s security posture with centralized threat data, real-time updates, and automation of manual processes. Additional objectives of tool integration are improving threat detection and community collaboration, which can bring together the global cybersecurity community to contribute. OTX plays a role in strategic, operational, and tactical intelligence in several ways.

Methods for integrating OTX with other tools includes

* DirectConnect API - Allows you to synchronize threat intelligence from OTX to existing security tools.
* Direct Connect Agents – These agents help integrate OTX into infrastructure to detect threats to your environment.
* SDKs – Software Development kits for Java, python, Node.js, and Go, assist with documentation, sample code, and debugging, and automation and ingestion of threat intelligence.
* STIX/TaxII Feeds – Indicators can be downloaded in STIX format, and OTX can be used as a TAXI server, to consume intelligence through the TAXII client.

OTX also plays a role in informing and contributing to all forms of intelligence. Strategic, operational, and tactical threat intelligence each make use of OTX. Strategic intelligence uses OTX to provide a comprehensive look at the global threat landscape with contributions from over 200,000 worldwide contributors. Planning and policies, another key portion of strategic threat intelligence can be enhanced with OTX. Operational threat intelligence benefits from the real-time threat detection and improved incident response. Tactical threat intelligence can be improve in terms of threat hunting and automation of workflows.

AlienVault OTX as threat intelligence sharing platform that brings a brings numerous capabilities to a cyber professional and when combined with additional tools through integration its uses and capabilities are that much more useful. OTX should also play a huge role in each type of threat intelligence.

**Section 3: Use Threat Intelligence Tools**

3.1 Cisco Talos

1. Which continent has the least amount of email reports? List the continent’s name and provide a screen capture of that continent.

**Africa A map of the world with a green point

Description automatically generated**

1. Use the zoom feature to zoom into the closest malware report to the area in which you live. Provide a screenshot showing the IP address, domain name, last day volume and email type.

A screenshot of a map

Description automatically generated

1. From the main talos page, search for mail.umgc.edu. Using the results answer these questions:
2. Who is the network owner for mail.umgc.edu? **microsoft corp**
3. What is the current web reputation for mail.umgc.edu? **Favorable**
4. When does the domain expire for umgc.edu (Hint: use the WhoIs tab) **31-Jul-2027**
5. Use the [email & spam filter](https://talosintelligence.com/reputation_center/email_rep) to determine which 3 countries send out the most spam. (Hint: select top 100 countries and the spam option.

**United States, Germany, and Russia**

1. Use the Vulnerability reports option to select recent (within the last 12 months) vulnerability that has a CVSS score of 10. Drill down into the data and provide the name of the vulnerability, the CVE-number, and the summary. Study the vulnerability and summarize how you would use this information to attack an organization if they hadn’t patched or updated their system.

Name- **Weston Embedded uC-HTTP HTTP Server heap-based buffer overflow vulnerability**

CVE- **CVE-2023-45318**

Summary - **A heap-based buffer overflow vulnerability exists in the HTTP Server functionality of Weston Embedded uC-HTTP git commit 80d4004. A specially crafted network packet can lead to arbitrary code execution. An attacker can send a malicious packet to trigger this vulnerability. (Cisco 2023)**

Possible Attack – **Based on the information provided, I think that be best method of attack would be to send a malicious network packet with a protocol version string within the request with “bytes whose value is less than 0x21 (exclamation point in ascii) or greater than 0x7e (tilde in ascii) [1], an integer underflow condition will occur within the internal variable used to store the remaining length of the receive buffer.” (Cisco 2023). Upon gaining access to the system, I would look to perform lateral movement searching for sensitive data and opportunities to create a persistent attack. Use of C2 for data exfiltration of any sensitive data that is located.**

3.2 Nmap exercise

1. What were the IP addresses for each of the sites you scanned?

* umgc-tomcat9.azurewebsites.net -**10.13.246.13**
* umgc-juiceshop.azurewebsites.net – **10.13.246.5**
* umgc-web-dvwa.azurewebsites.net – **10.13.246.8**
* Your UMGC VLE Windows Desktop – **10.11.48.133**
* Your UMGC VLE Kali Desktop – **10.11.48.132**

1. How many ports were scanned for each site?

* umgc-tomcat9.azurewebsites.net -**1000**
* umgc-juiceshop.azurewebsites.net - **1000**
* umgc-web-dvwa.azurewebsites.net - **1000**
* Your UMGC VLE Windows Desktop - **1000**
* Your UMGC VLE Kali Desktop - **1000**

1. Which ports were discovered as being open for each site?

* umgc-tomcat9.azurewebsites.net – **80, 443**
* umgc-juiceshop.azurewebsites.net – **80, 443**
* umgc-web-dvwa.azurewebsites.net – **80, 443**
* Your UMGC VLE Windows Desktop – **22, 135, 139, 445, 1947, 2179, 3389, 8000, 8089**
* Your UMGC VLE Kali Desktop – **22, 3389**

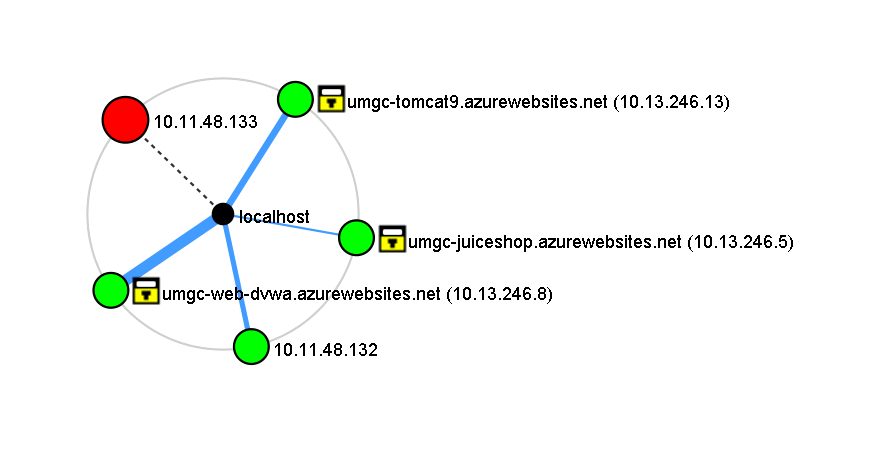
1. For the ports that were discovered to be open, what service runs on each port. Note, you only need to list each port once since the service will be same.

**22-ssh | 80-http | 135-msrpc | 139-netbios-ssn | 443-https | 445-microsoft-ds | 1947-http (Aladdin/Safenet) | 2179- vmrdp | 3389-ms-wbt-server | 8000-http (Splunkd) | 8089-http (Splunkd)**

1. What were the names of the operating system for each site scanned?

* umgc-tomcat9.azurewebsites.net – **No match found**
* umgc-juiceshop.azurewebsites.net – **No match found**
* umgc-web-dvwa.azurewebsites.net – **No match found**
* Your UMGC VLE Windows Desktop - **Microsoft Windows 10 1703**
* Your UMGC VLE Kali Desktop – **Linux 2.6.32**

1. Share a screenshot of the topology map resulting from the scans. Use the fishhook display.



1. What advantages do you see from a Cybersecurity defensive perspective for running an Nmap scan on your networked assets? Explain why scans should be run on a regular basis.

**There are several reasons that Nmap scan are important from a defensive perspective. First is that they can assist in the identification of vulnerabilities, threat detection, compliance, and incident response. Setting automated scans and running them often can provide continuous monitoring for your network. This will help to ensure that any new vulnerabilities and changes to the network are identified as quickly as possible.**

3.3 Maltego exercise **(Section completed in collaboration with Shayla Lee and James Korona)**

Note this a group project. Be sure to record which members completed each question. Also, be sure to discuss the results with your team before submitting so everyone is on board with the results.

1. Under the machines entity option, Perform a Level 1 (L1) Footprint for the umgc.edu. For the web.umgc.edu domain, what are the outgoing IP addresses? Look at one of the ending nodes listed as Microsoft-MSN-AS-Block. What do you think this does or represents? How could you use this information to help you better understand the domain you are analyzing?

**[Shayla Lee] The Outgoing IP addresses are 10.202.41.88 and 10.202.41.88. The Microsoft-MSN-AS-Block shows that the IP address is connected to Microsoft Azure which means there is a network block tied to Microsoft's cloud services. Knowing this can help us understand the domain better by identifying the hosting provider and network setup enabling an organization to look at security their security measures, traffic flow, and the cloud services that are being utilized.**

A screenshot of a computer

Description automatically generated

1. Run the “To DNS Name (interesting…)” transform under DNS from Domain group for umgc.edu and microsoft.com. How many DNS names are returned for umgc.edu? How many for Microsoft.com? Why do they return the same number of results?

**[Shayla Lee] Running the "To DNS Name (interesting...)" transform for umgc.edu and microsoft.com gives 12 DNS names each. This is because the transform finds only one main DNS record. It targets the most important DNS name instead of listing all subdomains.**

**UMGC.EDU**  A diagram of a network

Description automatically generated

**MICROSOFT.COM** A diagram of a network

Description automatically generated

1. Run the “To DNS Name - NS” transform under DNS from Domain group for umgc.edu and microsoft.com. What are the names servers listed for umgc.edu? What are the name servers listed for Microsoft.com? Explain what a name server does for an organization?

**[Shayla Lee] A name server monitors the Domain Name Server (DNS) records for a company. It converts easy-to-read domain names such as `umgc.edu into IP addresses that computers use to find and connect to services online.**

**UMGC.EDU A diagram of a company

Description automatically generated  
MICROSOFT.COM A diagram of a company

Description automatically generated**

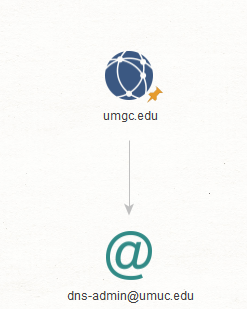
1. Run the “To DNS Name - MX” transform under DNS from Domain group for umgc.edu and microsoft.com. What are the MX servers for umgc.edu? What are the MX servers for Microsoft.com? Explain the purpose of an MX server.

**[James Korona] In the screenshot below you can see that Maltego locates the MX server for umgc.edu at umgc-edu.mail.protection.outlook.com and the MX server for microsoft.com at microsoft-com.mail.protection.outlook.com.  A MX server or “MX record” is a mail exchanger record for a domain.  It provides the mail server designated for e-mail messages for a particular domain.** A close-up of a logo

Description automatically generated

1. Run the “To Email address from whois” transform under Email address from Domain group for umgc.edu and microsoft.com. Are there any overlap in the results from umgc.edu and Microsoft. Describe the differences between the two results.

**[James Korona] The Maltego “To Email address from whois” returned** [**dns-admin@umuc.edu**](mailto:dns-admin@umuc.edu) **for umgc.edu and** [**msnhst@microsoft.com**](mailto:msnhst@microsoft.com)**,** [**admin@domains.microsoft**](mailto:admin@domains.microsoft)**,** [**abusecomplaints@markmonitor.com**](mailto:abusecomplaints@markmonitor.com)**, and** [**whoisrequest@markmonitor.com**](mailto:whoisrequest@markmonitor.com) **for microsoft.com.  These results are different because the e-mail addresses within WHOIS records are specific to the domain and are for purposes of administrative, technical, and general registrant contact.  The last two results are irrelevant for Microsoft.com as these are related to the registrar.  It looks like the Maltego transform retrieved all e-mail addresses from the record, however those two are not relevant.**

 A computer screen shot of a computer

Description automatically generated with medium confidence

1. Run the “To Phone numbers” transform under Domain Owner Detail group for umgc.edu and microsoft.com What is the 800 number listed for Microsoft? What number is listed for umgc.edu? What is the WhoIs registry and why is it important? Find the WhoIs and/or ICANN registry sites and compare the results obtained from Maltego.

**[James Korona] Maltego returned 5 numbers for Microsoft.  The 800 number is +1 800 745 9229.  Maltego returned 1 number umgc.edu which was +1 301 985 7447.  The WHOIS registry is composed of databases that contain information about registered users of internet resources.  This is important because it helps internet domains have identifiable information.  This helps to combat online abuse. According to domain.com “WHOIS is a free public directory of registered domain name owners. It contains their contact and technical info” (Suazo, 2024).  It uses a protocol for requests for the information and responses.  Some information in WHOIS records is registrant name, contact information, domain registration/expiration date, and DNS servers.  Methods exist to conceal WHOIS information for privacy reasons.  The actual regulations surrounding WHOIS data are complex and currently users can conceal this information if they choose to.  When comparing the results from the web-based WHOIS lookup to the results returned from Maltego, they are the same.  It is easier to discern the registrar information from the registrant information using the web-based interface.**

A computer screen shot of a company logo

Description automatically generated

1. What happens when you attempt to run the To DNS Name (attempt…) from the DNS from Domain group for umgc.edu and microsoft.com. What is an A record and why is it important?

**[Sam Perryman] When attempting to run the “To DNS Name” function the domains “umgc.edu and Microsoft.com” there are 0 entities returned for each. This process involves querying the DNS to find A records associated with the domain. An A(address) Record is “the most fundamental type of DNS record: it indicates the IP address of a given domain.” (Cloudflare n.d.)**

**A Records are important for several reasons.**

* **Directing internet traffic to the correct server.**
* **Ensuring that users can access websites using human-readable domain names.**
* **Multiple A records can be used for load balancing traffic across several servers.**
* **They also provide redundancy so that additional servers can take over if one fails.**

**A screenshot of a computer

Description automatically generated**

1. What happens is you attempt to conduct a Level 1 (L1) Footprint on umgc-tomcat9.azurewebsites.net or umgc-web-dvwa.azurewebsites.net? Explain the possible reason for the results.

**[Sam Perryman] There are no entities returned when running a Footprint L1 on “tomcat9.azurewebsites.net and umgc-web-dvwa.azurewebsites.net“. A Level 1 (L1) Footprint is a Maltego machine that is used in mapping an organization’s network infrastructure by identifying and documenting publicly accessible components of the network including DNS Names, Mail Exchange Servers, IP Addresses, Netblocks, Autonomous Systems Numbers, and Administrative Contacts.**

**The lack of data returned could be due to these domains to having more strict firewalls and intrusion detection systems. Access restrictions in which a server is configured to block responses to certain queries, privacy measures, and cloud infrastructures that hide or abstracts server techniques.**

A screenshot of a computer

Description automatically generated

3.4 VirusTotal exercise

1. Use the results from the Cisco Talos web site to cross check a URL and IP address that was shown as malware. List the URL and IP address. Describe your test case and show screen shots of the Talos and the VirusTotal website results. Do the two sources provide the same results? If not, what do you think might have caused the discrepancy?

**Watch.hxiso.com, 193.25.216.235**

**Both Talos and VirusTotal show the IP address (193.25.216.235) as being flagged as malicious by numerous vendors.**

**A screenshot of a computer program

Description automatically generatedA screenshot of a computer

Description automatically generated**

1. Pick a random file with no sensitive information in it on your Desktop and use a tool to generate its SHA-256 hash. Note, you can use powershell on Windows with the command Get-FileHash pathto/filename, or you can upload the file to <https://md5file.com/calculator> to generate the hash. Enter the resulting file hash into the Search window of the VirusTotal web site. Provide a screenshot of the results. Were the results as expected?

**data.safe.bin, (sha256)-34d745922a6a44898ee370bd0e5e2e0edff347d4a8e3061749c59642469c4f9d**

**As expected there were no vendor flags and the hash information matched. A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated**

1. Run domain checks for three (3) different vendors of your choice into the VirusTotal web site. Show screenshots of the results. Look carefully at the categories and popularity score in the details section of the report. Compare and contrast the 3 vendors you selected on this information. The report details may be useful to describe some of the data and information displayed in the output.

**Checkpoint, GreenSnow, CyberArk**

**The three vendors had some similar results, each had the Forcepoint ThreatSeeker designation of “Information Technology”. GS and CA had “business” as the bit defender while CP had “computersandsoftware”. Each had a (0/96) Community Score.**

**A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated**

1. Using the Relations tab on the output from the umgc.edu domain to compare the subdomains listed in VirusTotal to those listed in the community edition of Maltego. How many total domains does umgc.edu have listed in VirusTotal? Note, you can display additional subdomains in VirusTotal by clicking on the … option at the end of the subdomains section.

**UMGC has 253 subdomains listed in VitusTotal.**

3.5 Google Dorks exercise

1. Another useful Google Dork is the map: command. Use it to find maps Tangier Sound and Camp Arifjan? Show screenshots of the results of your Dorking for each map search. Where is Tangier Sound located? In what country is Camp Arifjan located? Is there a Food Court Zone in Camp Arifjan? If so, how did you determine this?

**Tangier sound is in the Chesapeake Bay.**

**Camp Arifjan is in Sabah Al Ahmad, Kuwait.**

**The food court is in Zone 6, the food court was located by zooming in on the camp using google maps**

**Tangier Sound Location** A map of the ocean

Description automatically generated

**Camp Arifjan** A screenshot of a map

Description automatically generated

**Camp Arifjan, Food Court** A map of a city

Description automatically generated

1. Set a timer on your desktop for 10 minutes using Google Dorks. Show the screenshot of your timer. What happens when the time expires?

**Timer turned red, with alarm sounding.**

A screenshot of a computer

Description automatically generated

1. The default web page for an initial web page for Apache2 running on Ubuntu has the following text in the title: "Apache2 Ubuntu Default Page: It works". How would you use this information to provide a list of sites that are using Ubuntu and have the default Web site for Apache2 still running. Show your Google Dork command and the results of running your command with a screenshot. How is this information useful in an ethical hacking or OS-INT gathering situation?

**9010 results found using the command [intitle:"Apache2 Ubuntu Default Page: It works"].**

**This information can be helpful for OSINT Gathering and Ethical hacking by identifying unsecured servers and assessing server configurations.**

A screenshot of a computer

Description automatically generated

1. Use the Google Dorking command “define:” to compare definitions of “Google Dorking” from 3 different sites. Based on the site results, provide a paraphrased definition for “Google Dorking” using the results from your query.

**Google Dorks are a set of methods and techniques used to find sensitive and hidden information about vulnerable sites.**

A screenshot of a computer

Description automatically generated

1. Use Google Dork commands to search the umgc.edu for xlsx extensions. Are xlsx documents present on the website? Show the command you used to search and the results in a screenshot for your report.

**There are no xlsx documents on the “umgc.edu” website.**

A screenshot of a computer

Description automatically generated

**Section 4: Final IOC Exercise**

1. A department in your organization has asked permission to have access to several web sites that currently appear to be blocked. The sites include: mars.umgc.edu, linuxhint.com, financereports.co, creativebookmark.com. Use Threat Intelligence tools to make a recommendation for each site. Be sure to justify using data and screenshots from the tools your decision.

**mars.umgc.edu – Allow Access, There are no known security threats associated with this domain.**

**linuxhint.com – Allow with Caution, this site is “whitelisted” by AlienVault OTX, however it does show 18 malicious files hosted and 1 malicious flag per Virustotal.**

**financereports.co – Block Access, This should be blocked for several reasons including, expiration date (2018-05-06) has passed, it is a DGA domain, legitimacy cannot be verified.**

**Creativebookmark.com – Block Access, This site should be blocked due to 11/94 Virustotal rating showing numerous phishing. Also appears to be a DGA domain, and has numerous related pulses per AlienVault OTX.**

1. An employee in your organization has had issues with their computer and is concerned if they may have a virus. Several files were uploaded to a safe sandbox for processing and analysis. The following SHA-256 hashes were submitted. Use appropriate tools to determine if any of the files should be quarantined.
2. b4bd56a2aebe3f5e020c5421e01c2d16804c25da673ecb125b074a94581cecfe

**Status – Malicious**

**Threat Name: Stealc Malware**

**Description: Used to gain unauthorized access to a system.**

**Most Recent Attack: July 2024**

1. d893a28a885344f46e74f3131d5ae3b3ecd2f5d29571afb124f556db86da40f3

**Status – Malicious**

**Threat Name: Red Line Stealer**

**Description: Hash corresponds to ransomware variant known to encrypt files.**

**Most Recent Attack: October 2024**

1. 5dc84570905973f2719578179596e36b4e29f2343ca360aeff730aacf7e37ed0

**Status – Malicious**

**Threat Name: Storm-0501**

**Description: This file attacks hybrid cloud environments for encryption and data exfiltration.**

**Most Recent Attack: September 2024**

1. D94BB76D6A8FBA54D6579A6265F6EAE66E905B8667D1B33080D28A2F7D068C0D

**Status – Malicious**

**Threat Name: FormBook**

**Description: Steals information such as keystrokes, passwords, and sensitive data.**

**Most Recent Attack: October 2024**

1. 456A194F501984067435393729294ECC02E75973C011F1E765EEB3FC6C23CBE4

**Status – Not Malicious**

For any hashes that are flagged as malware or malicious, provide more details to include a description of the specific threat, the virus or threat name, and the most recent attack date.

1. Your IT staff is short-staffed and need some assistance generating SHA-256 hashes for several files. This work is to verify the safety of the files in terms of malware but also for downloads processes so those using your organization’s data can confirm the hashes are identical. Use appropriate SHA-256 tools to generate the hashes for the following attached files:

* 2022-2023catalog.pdf

**D391a0bd202f075c9725bfa21422fa6ca378caa234bba743cf75012593b8ec93**

**Not Malicious**

**A screenshot of a computer

Description automatically generated**

* courseplanner.pdf

**9ed6d10aec6f0b9a3289f440003c4734ea931e2577cf05354a984437a092de3**

**Malicious**

**A screenshot of a computer

Description automatically generated**

* samplecoverletter.pdf

**b59633e1a54a06ff7c5cfa8dd7efa3217a1db9c6610fa8f9b857920a7e10c02f**

**Malicious**

**A screenshot of a computer

Description automatically generated**

After you generate the SHA-256 hashes, use a threat intelligence tool to verify there are no issues with malware.

For your report, list the SHA-256 results for each file along with a note stating if any issues were reported from the hash analysis. Provide screenshots verifying your malware analysis for each hash analysis.

1. Finally, in 4-6 paragraphs summarize your experience using threat intelligence tools. From your experience, discuss strengths and weaknesses for each tool used. Discuss your future envisioned use and tools that might be considered. For example, does it make sense to invest in commercial threat intelligence tool that uses multiple OS-INT and other sources, providing real-time alerts and visualization capabilities? If so, which tools might be good choices and why?

Threat intelligence play a crucial role in cybersecurity by helping organizations to identify and

prepare for potential threats. Awareness of the tactics, techniques, and procedures (TTPs) that are used

by bad actors is one key advantage that threat intelligence provides. The ability to anticipate potential

threats and understand the methods attackers may employ is a key to preventing attacks. Equally

important to preventing attacks, is responding to attacks quickly and effectively. Threat intelligence is

also an important part of risk management. In the following paragraphs I will discuss some of the tools

used in threat intelligence and the strengths and weaknesses that each provide.

AlienVault OTX is a useful tool that can provide real-time threat updates and extensive data

related to threats. As an open-source, community driven platform, AV OTX allows us to leverage the

shared knowledge and experiences for beyond one’s professional networks. It also possesses the

capability to integrate with numerous tools such as APIs, SDKs, and STIX/TAXII feeds to provide the most

comprehensive view of potential threats. A few of the negatives of AV OTX are that it requires additional

tools to fully unlock its potential and the volume of information can be overwhelming if proper filters

are not incorporated. Cisco Talos is known for providing detailed information on potential and existing

threats as well as vulnerabilities. Talos also provides strong incident response guidance and filtering

options for spam and email malware. Talos requires regular updates and maintenance in addition to

being complicated for inexperienced users. Nmap or Network Mapper is one of the most used tools for

network scanning and vulnerability detection. Nmap is an ideal tool for network monitoring and incident

response. Some major drawbacks to Nmap are its restriction to network level threats, lack of a fully

functional GUI, and extended scan times. Maltego is an exceptional information gathering tool that

provides users a visual depiction of connections and relationships between a range of entities.

Unfortunately, Maltego is subscription based, though there is a free community version that offers far

fewer features than the paid version. Our final tool, VirusTotal, is an internet-based application that

provides an aggregate of several antivirus engines. Its ease of use is offset by its limitation to known

threats and tendency to produce false positives.

I think that these tools can be best utilized when integrated into an organizations existing

security infrastructure. Integration of these tools can provide can improve automation and efficiency of

existing tools. The purchase and use of commercial threat intelligence tools can have many positives for

an organization. Establishing a proactive threat detection culture is possible through the real-time

insights provided. Also, the cost of responding to attacks and breaches can easily eclipse the cost of

these tools. The knowledge base contained within open-sourced tools can be an invaluable to

collaboration and decision making. I would recommend the use of Cisco Talos based on its in-depth

analysis of threats and the ease of integration with other applications and tools. Threat Connect is also

considered one of the top threat intelligence platforms, boasting a strong mix of features and

integrations. TC also has the capability to be deployed on-site, air-gapped, or on private cloud instances.

In conclusion the importance of threat intelligence tools cannot be overstated in today’s cyber

landscape. They provide advance threat detection, risk reduction, and help stakeholders make decisions

that can have profound impacts on overall security posture and organizational goals. Organizations

should amalgamate several threat intelligence tools to provide the most comprehensive security

strategy.

**References**

AT&T Cybersecurity. (n.d.). *Open Threat Exchange (OTX) Threat Intelligence*. [**https://cybersecurity.att.com/open-threat-exchange/otx-threat-intelligence**](https://cybersecurity.att.com/open-threat-exchange/otx-threat-intelligence)

Cisco Talos Intelligence Group. (2023, October 16). *TALOS-2023-1843*. [**https://talosintelligence.com/vulnerability\_reports/TALOS-2023-1843**](https://talosintelligence.com/vulnerability_reports/TALOS-2023-1843)

Cloudflare. (n.d.) What is a DNS record?. Cloudflare. Retrieved November 12, 2024, from <https://www.cloudflare.com/learning/dns/dns-records/dns-a-record/>

Cranford, J. (2023, July 7). *Incident Response Plan: Frameworks and Steps*. CrowdStrike. <https://www.crowdstrike.com/en-us/cybersecurity-101/incident-response/incident-response-steps/>

Cybersecurity and Infrastructure Security Agency. (n.d.). Cyber incident response. U.S. Department of Homeland Security. Retrieved October 13, 2024, from <https://www.cisa.gov/resources-tools/services/cyber-incident-response>

Cybersecurity and Infrastructure Security Agency. (2024). *Federal government cybersecurity incident and vulnerability response playbooks*. <https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf>

Forbes Advisor. (2024, June 5). What is threat intelligence? Definitions, types & process. Forbes. <https://www.forbes.com/advisor/business/what-is-threat-intelligence/>

Goldman, J. (2018, April 3). *AlienVault vs Splunk: Top SIEM Solutions Compared*. eSecurity Planet.  [**https://www.esecurityplanet.com/products/alienvault-vs-splunk/**](https://www.esecurityplanet.com/products/alienvault-vs-splunk/)

Kirvan, P., Cobb, M., & Wigmore, I. (2024, October 1). *What is threat intelligence?* TechTarget.com. <https://www.techtarget.com/whatis/definition/threat-intelligence-cyber-threat-intelligence>

Microsoft. (n.d.). *What is incident response?* Microsoft. Retrieved October 13, 2024, from <https://www.microsoft.com/en-us/security/business/security-101/what-is-incident-response?msockid=0e127cf549826a0226f5683248456b79>

Mukherjee, A. (2023, June 13). *Post-incident analysis: Lessons for a Cybersecurity Excellence*. Threat Intelligence. <https://www/threatintelligence.com/blog/post-incident-analysis>

National Institute of Standards and Technology. (2012). *Computer Security Handling Guide (NIST Special Publication 800-61 Revision 2)*. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/61/r2/final>

RSI Security (2022, June 15). *How to Execute the Containment Phase of Incident Response*. RSI. <https://blog.rsisecurity.com/how-to-execute-the-containment-phase-of-incident-response/>

Suazo, G. (2024, September 23). *What is WHOIS and How to Look Up a Domain?*. Domain.com Blog. <https://www.domain.com/blog/what-is-whois-and-how-is-it-used/>