SOC BASICS:
THREAT INTELLIGENCE

@Mu_Abdel_Aal

https://github.com/MuhammadEissa

THE HISTORY OF THREAT INTELLIGENCE

- Threat Intelligence : -
  - The threats concepts long as the humans begging and there was always evolutions of using the information and utilizing it to give the best and fastest results, such as predicting attacks of thefts, terrorism and many more, we can't understand the concept of nowadays CTI (Cyber Threat Intelligence) without trying to understand the actual concept of threats.
  - Examples of threats: -
    - terrorism.
    - National Threats from enemy countries.
    - Planning for Theft that could harm the economy
    - Murderers tracking.
  - The main tools were used in Threat Intelligence are databases which mostly where paper and later they start to use computer systems to store and search this data, CCTV which used mainly to detect using criminal data bases based on the computerized data bases.

THE HISTORY OF THREAT INTELLIGENCE

- Cyber Threat Intelligence : -
  - With the begging of the .com revolution and internet become available for everyone to use, and a lot of services start to use the internet to expand, the concept of cyber attacks start to take a place in this words in many forms such as Virus attacks, malware attacks, phishing, ransomware and many more we know and will know.
  - There was no concept like this one we have nowadays for Cyber threat intelligence but there was list of blacklisted IP`s mainly, were used to block this list from your side to be proactive from its attacks.
  - Then start the concept of file hashes and virus signature, but attackers where always ready with new technics to avoid detection and keep them attacks stronger than before.

THE HISTORY OF THREAT INTELLIGENCE

- Cyber Threat Intelligence : -
  - In the last few years, the technology providers start to use the benefits of the internet connectivity and started to generate data which detected to be malicious such as IP`s, hashes, file names, process names and now we have service such as Viruses total which provide dynamic analyses and integration with other vendors that may have data related to your submitted files in order to help you identify whither their file malicious or not.
  - The revolution of hackers and the used technics forced the tech vendors to develop new tools with new abilities such as EDR,NDR,SIEM,SOAR,FIM any many more and expected to see more new techs like NGFW,NG-SIEM ☺
  - Now we can see pure security vendors only not just tech vendors and Threat Intelligence are paort of them services.
  - And with this wide range of security controls, we can't manage threat intelligence separately, so we can find now CTI platforms which hosted on the cloud or on prim with API integration with your other security controls, so you centralize your threat intelligence configuration.
  - Detected Vendors for CTI now also can be found in the last few years.

The History of Threat Intelligence

- Cyber Threat Intelligence : -
  - STIX/TAXII: -
  - STIX, short for Structured Threat Information eXpression.
  - TAXII, short for Trusted Automated eXchange of Intelligence Information.
    - Developed From a Need for a Threat Intelligence Sharing Standard, STIX and TAXII are standards developed to improve the prevention and mitigation of cyber-attacks. STIX states the "what" of threat intelligence, while TAXII defines "how" that information is relayed. Unlike previous methods of sharing, STIX and TAXII are machine-readable and therefore easily automated.

The History of Threat Intelligence

- Cyber Threat Intelligence : -
  - Intelligence TLP
    - RED
      - For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
    - AMBER
      - Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP:AMBER+STRICT restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.
    - GREEN
      - Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.
    - CLEAR
      - Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

THE HISTORY OF THREAT INTELLIGENCE

- CTI & SOC: -
  - SIEM AND CTI INTEGRATION NOW IS ONE OF THE MOST CRITICAL SETUPS TO HAVE IN YOUR ENVIRONMENT AND CONSIDERED THE MOST PROACTIVE ACHIEVEMENT OF CTIA.
  - SOC SHOULD OPERATE 24/7 AND WITH CTI YOU WILL HAVE DETECTION OF CTI THROUGH YOU SIEM AND FOR SURE IN ORDER TO DO SO YOU WILL NEED TUNED SIEM AND ALL CRITICAL SYSTEM TO FEED THE SIEM WITH THE LOGS/FLOW.
  - IP`S,HASHES,FILE NAMES, EVEN THE TECHNIQUES.

THE HISTORY OF THREAT INTELLIGENCE

- CTI & SOC: -
  - Dashboards, Alerts and the other methods available in your SIEM should be configured to detect the IOC`s.
  - Use Cases bases on the Threat Actros data, and for threat actors' data we can now use service such as MITRE ATT&CK® which provide a great matrix for attacks & APTS tactics and technics.
  - And integration with tools such as SOAR in order to centralize your action across the network.

THE HISTORY OF THREAT INTELLIGENCE

- CTI & SOC: -
  - Dashboards, Alerts and the other methods available in your SIEM should be configured to detect the IOC`s.
  - Use Cases bases on the Threat Actros data, and for threat actors' data we can now use service such as MITRE ATT&CK® which provide a great matrix for attacks & APTS tactics and technics.
  - And integration with tools such as SOAR in order to centralize your action across the network.

Caution: -
The document and data within only represent myself and don't represent to my employer.

List of references: -

- https://attack.mitre.org/matrices/enterprise/
- https://github.com/hslatman/awesome-threat-intelligence
- https://oasis-open.github.io/cti-documentation/
- https://www.misp-project.org/
- https://github.com/OpenCTI-Platform/opencti
- https://urlscan.io/
- https://www.abuseipdb.com/
- https://www.first.org/tlp/


THANK
YOU