- **CTI:** Cyber Threat Intelligence
- **DFIR:** Digital Forensics Incident Response
- **NSTR:** Nothing Significant to Report
- **BLUF:** Bottom Line Up Front - stating the basic thing at the start and then restating it at the end - don't bury the lead.
- **Threat Landscape** - all of the potential or identified threats affecting a sector or users or business
- **PIR:** Priority Intelligence Requirements, what should be prioritized https://sector.ca/sessions/priority-intelligence-requirements-pir-are-not-just-for-threat-intel-analysts/
- **GIR:** Generalized Intelligence Requirements - a framework for collecting baseline intel https://intel471.com/blog/introducing-intel-471s-cybercrime-underground-general-intelligence-requirements-cu-gir-a-common-framework-to-address-a-common-challenge/
- **Threat** - Any type of danger, such as malware, phishing attacks, network intrusion, etc.
- **Vulnerability** - A weakness in the system be it software, hardware, physical security, or with the team, which can be exploited by threat actors to achieve their goals. For example, unpatched VMWare software could lead to a vulnerability being exploited, which is a high level of threat due to its criticality.
- **Risk** - is the threat probability multiplied by the vulnerability impact and it can be accepted, mitigated, avoided, or transferred to a third-party (buying insurance).
- **Threat Actor or cybercriminal** (note hacking itself is not a crime - neither is using f12) - the individual or group perpetuating the security incident. Sometimes this can involve physical security.

- **Nation-State Actor** - threat actors funded by countries. For example, Lazarus Group funded by North Korea
- **APT:** Advanced Persistent Threat often used interchangeably with nation-state actors because of their funding and persistence
- **Attribution** - who is the root cause/group
- **Misattribution** - when a group attempts to misguide the
- **Kill Chain also called Cyber Kill Chain** is a model from Lockheed Martin for tracking what adversaries must do https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- **The Wild or In the wild** - are threats that are on real computers
- **POC:** Proof of Concept, this is important for believability for threats - is there an actual proof of concept?
- **DWUF:** Dark Web and Underground Forums
- **LOLbins/LOLBas:** Living off the land binaries, local to operating systems, and may be targeted by threat actors
- **Backdoor** is any method that allows another user to access your devices without your knowledge
- **OSINT:** Open-Source Intelligence is a type of way to gather the information that is not classified, but it is still a skill that can be honed through techniques like Google Dorking or the using tools like Maltego or items from the OSINT framework or tools for digital forensics like SIFT https://www.sans.org/webcasts/started-sift-workstation-106375/
- **IOCs:** Indicators of Compromise
- **TTPs:** Tactics, Techniques, and Procedures. A tactic is the behavior of an actor it is the and can be thought of as the high level how, the techniques are more

detailed and can be thoughts of as the why, and the procedures are the finest level of detail. All of this can be mapped with MITRE ATT&CK https://attack.mitre.org/#

- **Threat modeling** is a process used to organize threats, realize vulnerabilities, and assess risk.
- **MITRE ATT&CK** - a knowledge base from MITRE based on real-world situations and used to threat model https://attack.mitre.org/#
- **Diamond Model** - a framework for tracking adversaries, infrastructure, capabilities, and victims and the relationships between
- **Network Defense** is proactive threat blocking
- **Misinformation -** misleading or false information created or shared without malicious intent
- **Disinformation -** deliberate manipulation to distort the truth, which is often orchestrated and is malicious by its very nature.
- **SOC:** Secure Operations Center for monitoring the organization. If an organization is larger they might also have a NOC: Network Operations Center that is more specialized
- **IR:** Incident Response for analyzing targeted attacks and mitigating those attacks
- **RFI:** Request for Information - often what begins a threat report as a RFI
- **Malware** is any software designed to cause disruption or harm
- **Ransomware** is a type of malware that threatens to publish a victim's data and/or block access to data/end devices until a ransom is paid
- **Infostealer** is a trojan that is designed to gather information from a system
- **A Trojan** is a program that looks like one thing, but is another thing - it looks innocent, but is malicious

- **YARA:** used to hunt for malware with its binaries
- **STIX:** used to hunt for malware with its binaries
- **TAXII:** used to hunt for malware with its binaries
- **C2 Server or C&C Server:** command and control, which means malware will beacon back to it sending it a signal as if calling home
- **MISP:** A useful open-source threat intelligence sharing platform
- **BISO:** Business Information Security Officer
- **CISO:** Chief Information Security Officer
- **GRC:** Governance Regulation and Compliance - laws that are about cyber and privacy
- **M&A:** Mergers and Acquisitions - business term, but now some threat actors are targeting organizations based on M&A
- **Third-Party Risk** is supply chain risk due brought on by other organizations in one's ecosystem
- **ROI:** Return on Investment