filename:comptia-secplussy0601-1-19-threat_actors_and_attack_vectors
Showname: Security+ \(SY0-601\)
Topic: Threats, Attacks and Vulnerabilities
Episode: Threat Actors and Attack Vectors
Learner Objectives:

Given a scenario, analyze potential indicators associated with wireless attacks.

Description:In this episode, the viewer will identify the types of threat actors within the cybersecurity landscape as well as the attributes or characteristics of these threat actors. The viewer will also be able to explain the attack vectors that threat actor's use in order to accomplish their goals.

---

* Threat Actor Types
    + Script Kiddies
    + Insider threats
        - [Tesla] Insider threat
        - [Google] insider threat
    + Hacktivist
    + Advanced persistent threat \(APT\)
        - Fireeye
        - Crowdstrike
        - https://apt.securelist.com/
    + State actors
    + Criminal syndicates
    + Shadow IT
        - The use of information technology systems, devices, software, applications, and services without explicit IT department approval.
        - Using Dropbox or Google drive instead of company authorized storage
    + Competitors
* Hackers vs. Attackers
* Hackers
    - White hat
    - Black hat
    - Gray hat
* Vectors
    + Direct access
        - Insider Threat
    + Wireless

        - Mobile, WiFi, RFID
    + Email
        - APTs
        - Hacktivists
        - Criminal Syndicate
    + Supply chain
        - [DarkReading]
    + Social media
        - Twitter and DDoDSecrets
    + Cloud
        - [Microsoft Security]

* Attributes of threat actors **No Slide**
    + Internal/external
        - Insider vs. all the others
    + Level of sophistication/capability
        - APTs vs Script Kiddies
    + Resources/funding
        - Hacktivists vs Nation States
    + Intent/motivation
        - Political

[Tesla]:https://www.cnbc.com/2018/06/18/elon-musk-email-employee-conducted-extensive-and-damaging-sabotage.html
[Google]:https://www.secureworldexpo.com/industry-news/google-insider-threat-pleads-guilty
[DarkReading]:https://www.darkreading.com/application-security/attackers-aim-at-software-supply-chain-with-package-typosquatting/d/d-id/1337611=
[Microsoft]: https://www.microsoft.com/security/blog/2020/09/24/gadolinium-detecting-empires-cloud/