# Onion Server: Playbook & ATT&CK Navigator

Within Security Onion, the Playbook tool integrates with Zeek, Suricata, Navigator and Elastic Search to create premade workflows to tackle cybersecurity investigations. It acts as a way of organizing knowledge and procedures on handling specific threats, including ways to automate the process to minimize response time to incidents.

Playbook is used mostly for incident response and alert management but can be useful as a database as well for training, compliance and standardization. The premade “plays” are a way of dealing with known threats, but also an excellent tool in teaching others on how to respond to those same threats.

Navigator, on the other hand, is a way of organizing the ATT&CK knowledge base in a way that visualizes the database based on different attack vectors. When Navigator is paired with Playbook, it allows the premade plan from Playbook to be imported into Navigator, where the detection rules are cross-referenced with the ATT&CK KB to see if common methods are found and used.

Playbook uses Sigma, a programming language like .yaml files to build its plays. This allows others to share and create their own plays by simply importing the raw text of the Sigma code into Playbook. Once the Sigma imported code is run on Playbook, it creates an ElastAlert rule file using some included templates.

Once the play is enabled, depending on the Sigma code imported, an alert will be generated in Security Onion where then a case can be created

# Bibliography

[Security Onion Essentials 2.3 – Detection Engineering](https://www.youtube.com/watch?v=IS2SOlDedPc)

[Official Navigator Documentation](https://github.com/mitre-attack/attack-navigator)

<https://www.infosecinstitute.com/resources/mitre-attck/how-to-use-mitre-attck-navigator-a-step-by-step-guide/>

[Security Onion Conference 2019: Constructing Your Playbook within Security Onion by Josh Brower](https://www.youtube.com/watch?v=qBXg3IUJPjY)