Alert Automation and Response

Automation is a core tenet of the Detection & Response team. Our goal is to automate as many of the alert processing and response tasks as possible, and we have an 'API-first' mentality when considering new tools or services to support our operations.

That is why our Detection and Response team has embraced technologies to automate the response to security events. we desire to rely heavily on security automation to ensure we're not wasting valuable cycles performing repetitive, manual tasks.

Our Central tools of choice – SCOT + DISPATCH + SLACK + STATUS PAGE + Mobile App

The Sandia Cyber Omni Tracker, **SCOT**, is a cyber security incident response (IR) management system designed by cyber security incident responders to provide a new approach for managing security alerts, including coordinating team efforts, capturing team knowledge, and analysing data for deeper patterns. SCOT integrates with existing security applications to provide a consistent, easy to use interface that enhances analyst effectiveness.

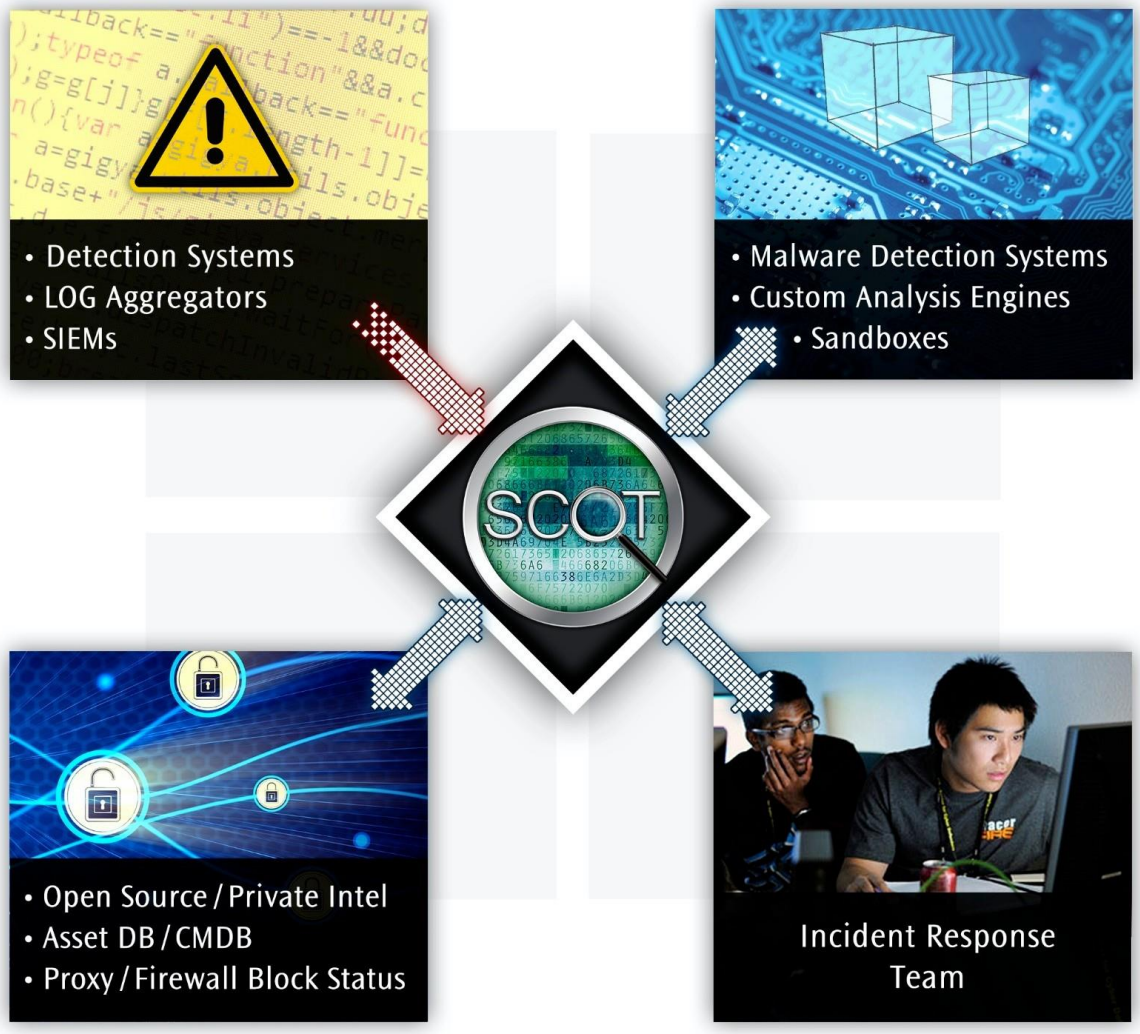
We currently have vendors that have open-sourced their bot on github and we will need to leverage and tune these for our internal automation.

The following BOT are available and accessible and we

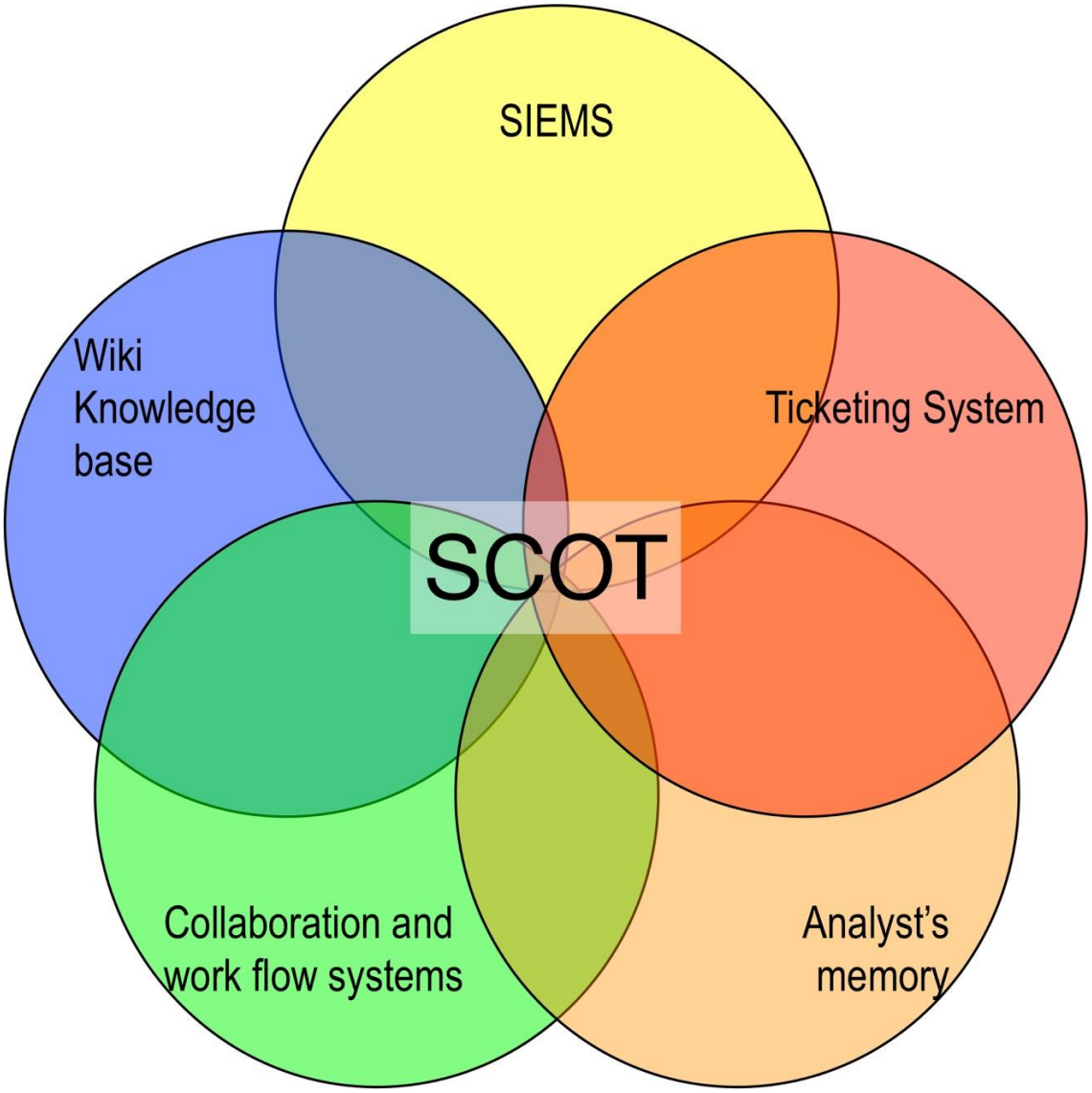
1. **Dispatch** – see link below
    a. https://hawkins.gitbook.io/dispatch/ ➔ official documentation
    b. https://netflixtechblog.com/introducing-dispatch-da4b8a2a8072
    c. https://www.youtube.com/watch?v=_HYShHaVUGg
    d. https://gigazine.net/gsc_news/en/20200308-netflix-dispatch/

2. SCOT – this is our incident response (IR) management system.
    a. https://github.com/sandialabs/scot
    b. https://scot.readthedocs.io/_/downloads/en/latest/pdf/
    c. https://scotdemo.com with the username: admin/ password: admin… Give SCOT a try online

High Level Functional Diagram of the SCOT Application



Diagrammatic overview of the SCOT Opensource Application



Requirement

1// Integrate at least 5 - 10 applications via api or smtp sources into SCOT. See list below*
2// Changes the front-end colour and logo of SCOT + any minor front-end tweak
3// Build an integration between SCOT and DISPATCH
4// Build a mobile app showing our clients a few graphical charts as seen on DISPATCH
5// Setup forwarding of only Events & Incidents to DISPATCH
6// Create a customer onboarding interface on the same client facing app. Details and layout will be provided
7// Enable SLACK integration from DISPATCH
8// Enable the PagerDuty (start with the free tier) or xMatters (start with the free tier – we might purchase the "starter" subscription) integration
9// Enable StatusPage (start with the free tier) integration for web customer updates
10// Enable/Integrate at least 5 automation on DISPATCH
11// Provide at least 3 months non billable warranty on the job, breakfix relating to coding issues
12// Provide detailed documentation of codes and a corresponding knowledge transfer.

Application to integrate (if and where possible) *

1. ArcSight ESM
2. LimaCharlie
3. ElasticSearch
4. Intel OWL
5. Darkweb Onion Scan
6. ForcePoint
7. Proxmox
8. SecurityOnion
9. Domotz
10. Dispatch
11. Velociraptor
12. ElastAlert
13. ArcSight investigate
14. TheHiveCortex (optional)

Architecture of our Requirement