OSCAR: The Ontology for SOC Creation Assistance and Replication

A SOC-Development Knowledge Base and Ontology

Introduction

Security operations centers (SOCs) are necessary and critical organizations for ensuring Department of Defense (DoD) enterprise-wide cybersecurity and incident response capabilities. Many DoD military departments, combatant commands, and other agencies require these capabilities.

At the same time, the DoD faces challenges in deploying SOC capabilities:

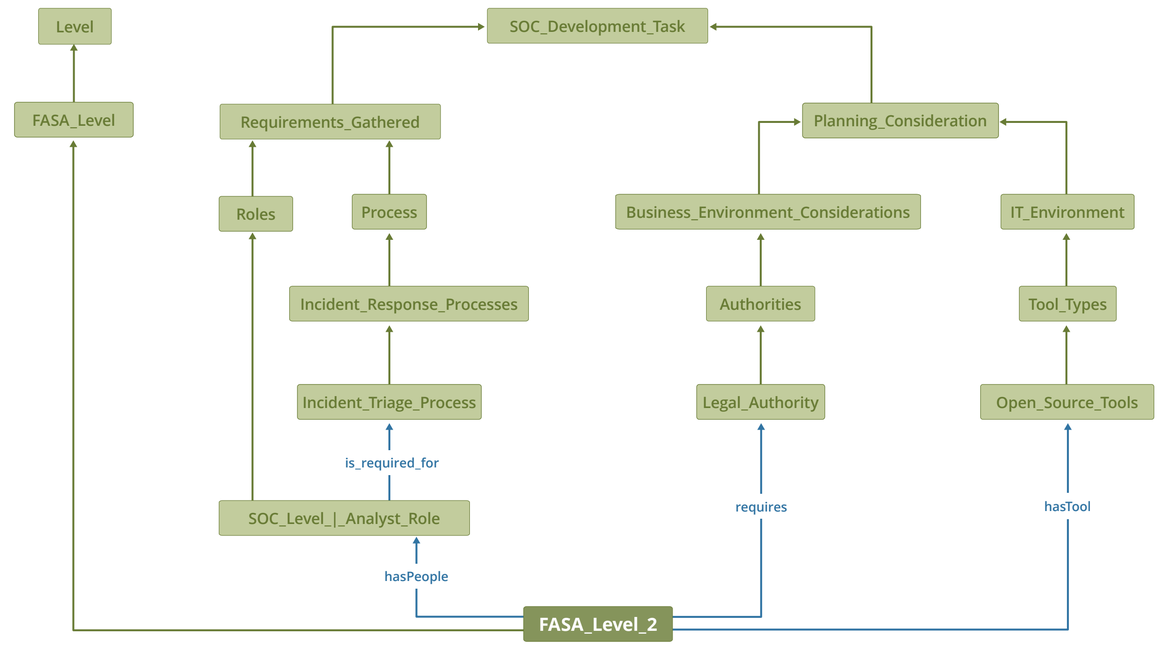
- limitations in the use of managed security service providers (MSSPs) and cyber security service providers (CSSPs)
- high cost of deployment
- specific knowledge requirements

Our Approach

We significantly reduce the time and cost of deploying SOC capabilities by capturing expert knowledge in the Ontology for SOC Creation Assistance and Replication (OSCAR), which formalizes domain knowledge and can be deployed to support SOC development. In our work developing OSCAR, we did the following:

1. We identified knowledge domains (i.e., people, process, technology).
2. We gathered more than 60,000 potential data points.
3. We coded data into an ontology and augmented it using industry best practices.

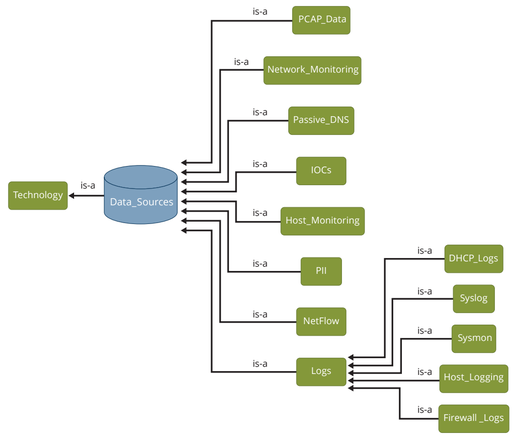
A formal knowledge domain and naming system enables organizations to **develop more effective SOCs** in **less time** and at a **lower cost**.



- Our base OSCAR ontology describes SOCs according to service areas and functional levels.
- An assessment tool is used to determine the current level of capability within each service area.
- A *reasoner* determines which knowledge classes are required to increase the capability to a higher functional level.

Our Solution

We developed OSCAR using a purpose-built dataset that we created by extracting the knowledge of SOC expert practitioners. It contains robust, real-world insights into the SOC knowledge domain. Here is an example of such a dataset:



Beyond capturing and formalizing existing knowledge, OSCAR enables DoD organizations to infer new relationships. It does that by defining properties and relationships between knowledge classes and using a reasoner to show them.

OWL Entity Description Editor: ICSA_Level_5

```
Class: ICSA_Level_5

    Annotations: [in root-ontology]
        rafs: comment "IK Class"

SubClassOf: [in root-ontology]
    ICSA_Level,
    (hasPeople some
        (Legal_Counsel__Role
        and SOC_Level_I_Analyst_Role
        and SOC_Manager_Role
        and Staffing_Level_Needs))
    and (hasPolicy some
        (Acceptable_use_Policy
        and Information_Classification_Policy
        and Information_Sharing_Policy))
    and (hasProcedure some POC_List)
    and (hasProcess some Incident_Escalation_Process)
    and (hasTechnology some Automation)
    and (hasTool some
        (Information_Sharing_Platform_Tool
    and SIEM_Tool
    and Vulnerability_Management_Tool)),
(hasPeople some (hasSkill some Incident_Response_Function))
    and (hasTraining some Role_Based_Training)
```

Carnegie Mellon University
Software Engineering Institute

Dr. Justin Novak | jnovak@cert.org