

# 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:

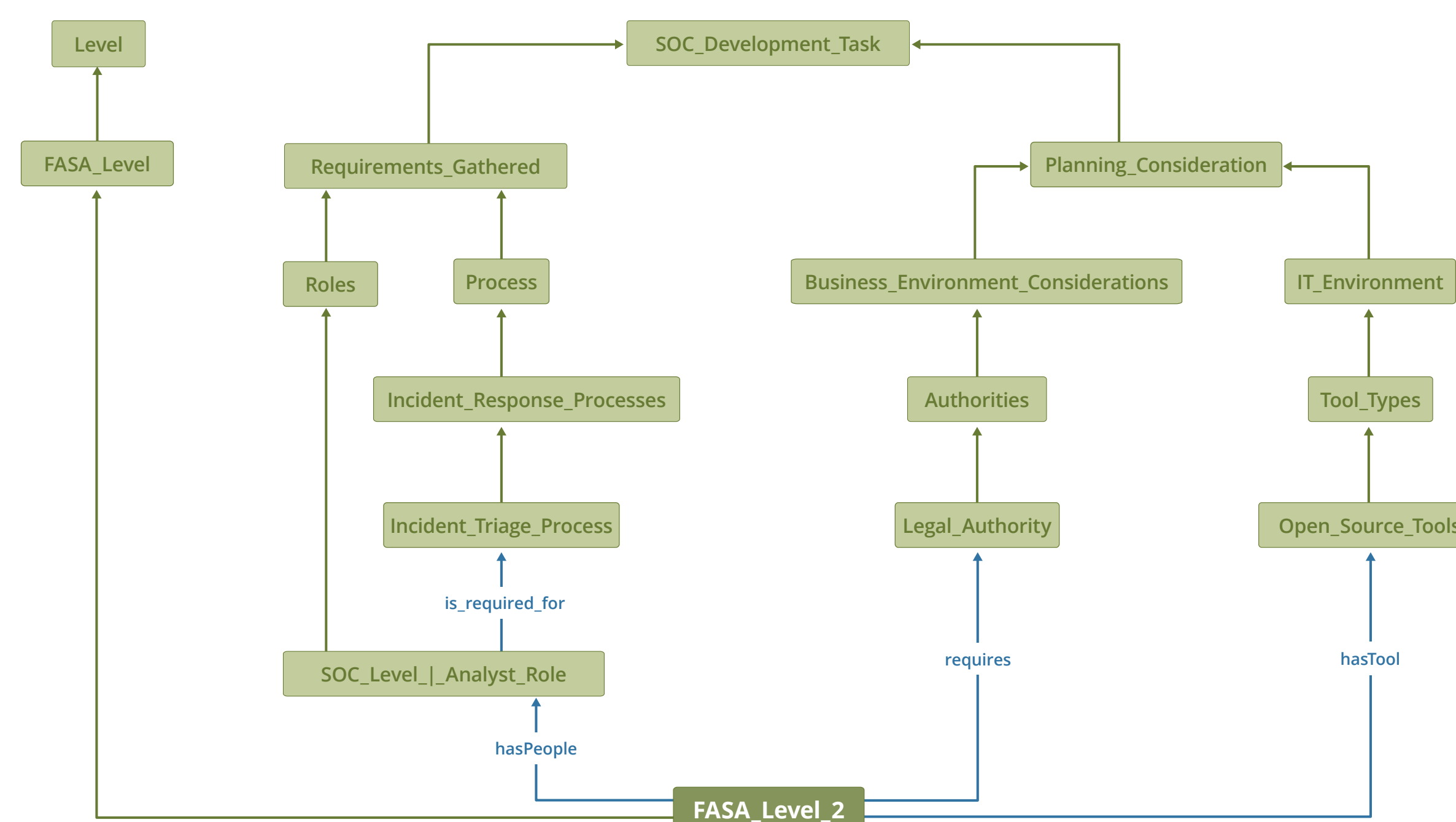
- limitations in the use of managed security service providers (MSSPs) and cyber security service providers (CSSPs)
- high cost of deployment
- specific knowledge requirements

## 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.

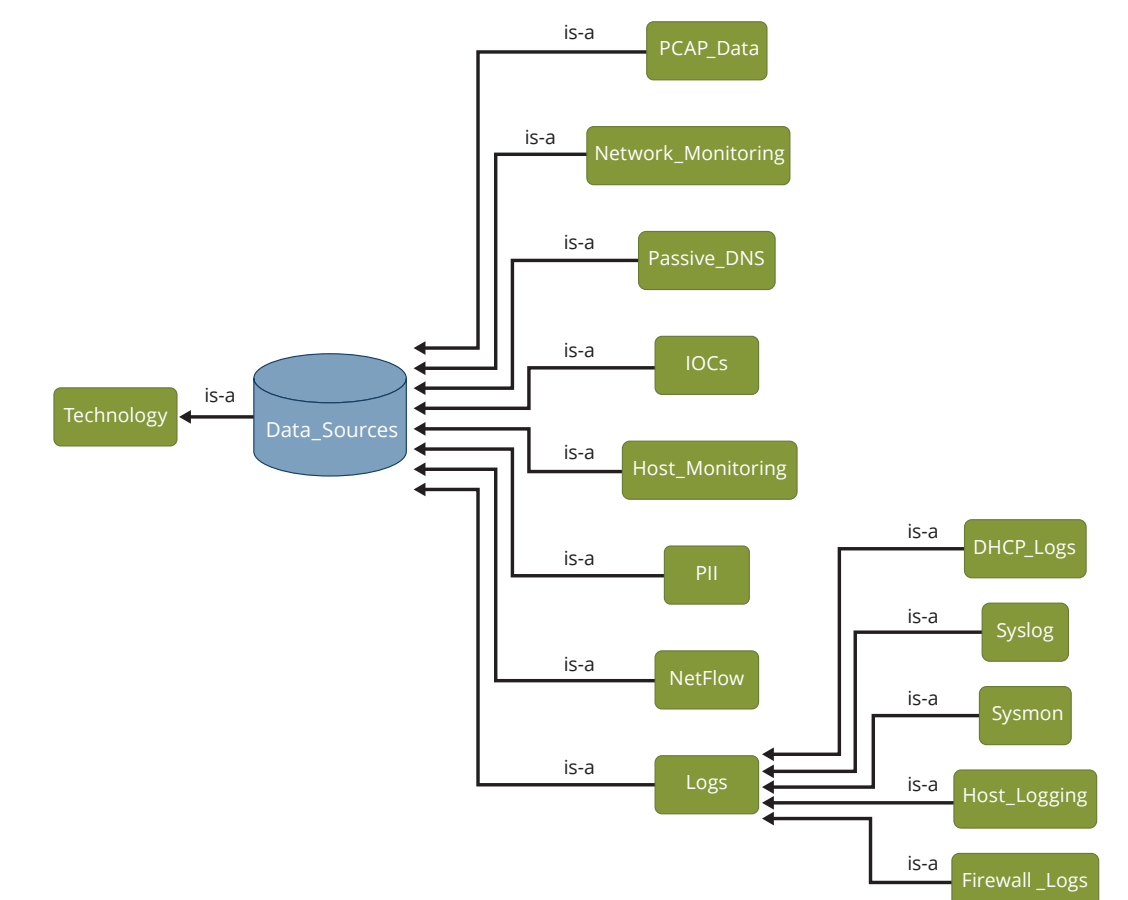
A formal knowledge domain and naming system enables organizations to **develop more effective SOCs in less time and at a lower cost.**



- 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
1 Class: ICSA_Level_5
2
3 Annotations: [in root-ontology]
4   rdfs: comment "IK Class"
5
6 SubClassOf: [in root-ontology]
7   ICSA_Level,
8   (hasPeople some
9     (Legal_Counsel__Role
10    and SOC_Level_I_Analyst_Role
11    and SOC_Manager_Role
12    and Staffing_Level_Needs))
13  and (hasPolicy some
14    (Acceptable_use_Policy
15    and Information_Classification_Policy
16    and Information_Sharing_Policy))
17  and (hasProcedure some POC_List)
18  and (hasProcess some Incident_Escalation_Process)
19  and (hasTechnology some Automation)
20  and (hasTool some
21    (Information_Sharing_Platform_Tool
22    and SIEM_Tool
23    and Vulnerability_Management_Tool)),
24  (hasPeople some (hasSkill some Incident_Response_Function))
25  and (hasTraining some Role_Based_Training)
26
  
```

Copyright 2024 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. Requests for permission for non-licensed uses should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

CERT® and Carnegie Mellon® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM24-1362