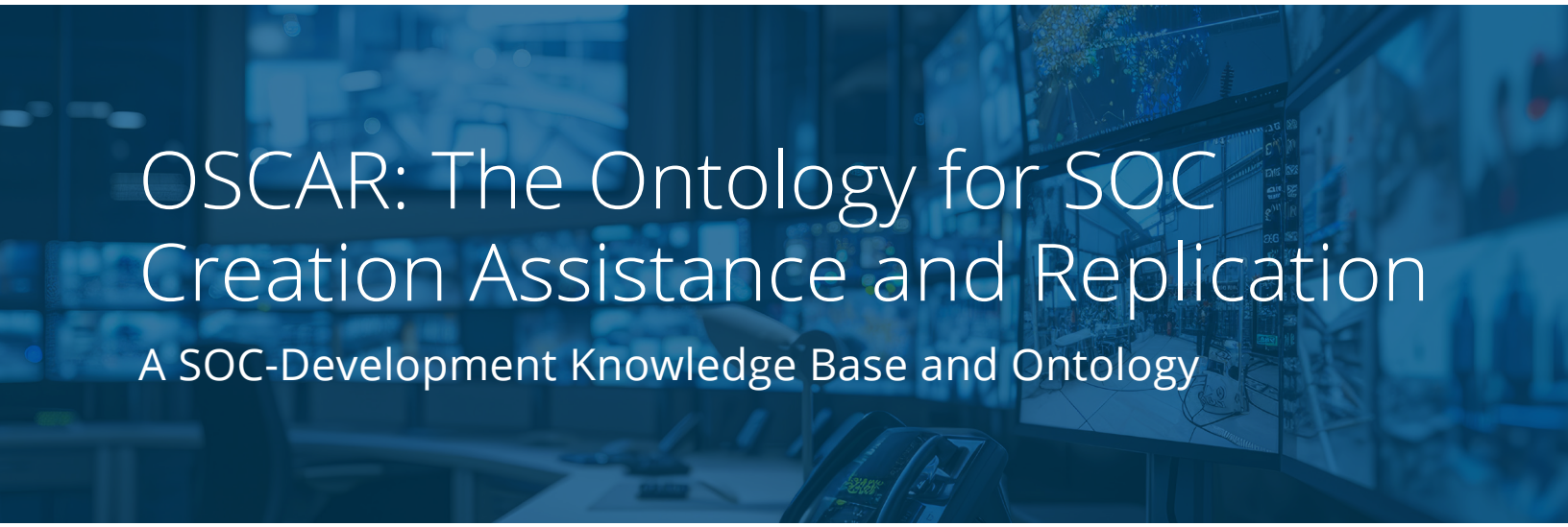
Carnegie Mellon University
Software Engineering Institute



OSCAR: The Ontology for SOC Creation Assistance and Replication

A SOC-Development Knowledge Base and Ontology

DEPARTMENT OF DEFENSE (DoD) ORGANIZATIONS RELY ON THEIR SECURITY OPERATIONS CENTERS (SOCs) TO PROVIDE THEM WITH PRINCIPAL CYBERSECURITY AND INFORMATION DEFENSE EXPERTISE. THEREFORE, IT IS IMPORTANT THAT THESE ORGANIZATIONS DEVELOP STRONG SOC CAPABILITIES.

However, DoD organizations face challenges when developing effective SOC capabilities. Doing so is costly and time consuming. Perhaps the most significant challenge is that each SOC's resources and service offerings must be unique to reflect the needs of the organization it serves.

To overcome these challenges when developing a SOC capability, a DoD organization requires robust and extensive domain-specific expert knowledge in the complex realm of cybersecurity operations and development. Moreover, that domain-specific knowledge must be informed by a deep understanding of the organization's mission and requirements.

Carnegie Mellon University's Software Engineering Institute (SEI) is conducting research into a SOC-development knowledge base and ontology that helps DoD organizations strengthen their domain-specific expert knowledge. The Ontology for SOC Creation Assistance and Replication (OSCAR) helps organize and codify SOC-development knowledge into a formal body of knowledge.

The SEI will design OSCAR to do the following:

- map SOC-development knowledge to more than 300 knowledge classes to identify more than 50 distinct relationships between them
- employ a *reasoner* to identify inferred relationships that are otherwise unknown or easy for humans to miss
- enable effective SOC operations by allowing the visualization of a function-by-function set of requirements in the people, processes, and technology knowledge domains
- break functions into maturity levels to improve resource allocation and development

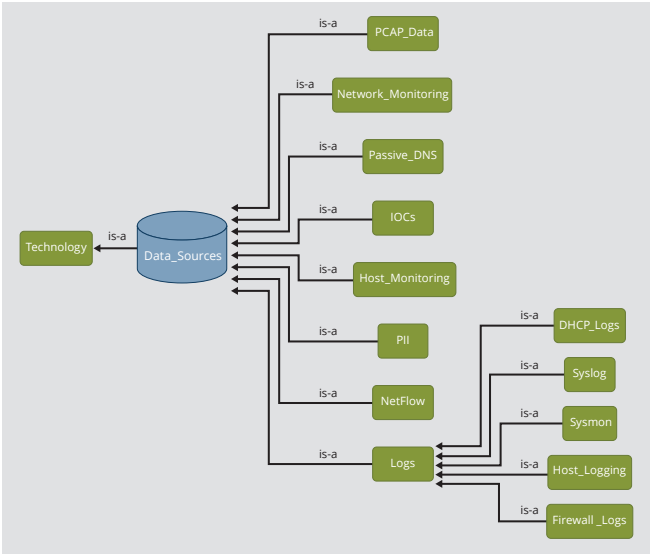
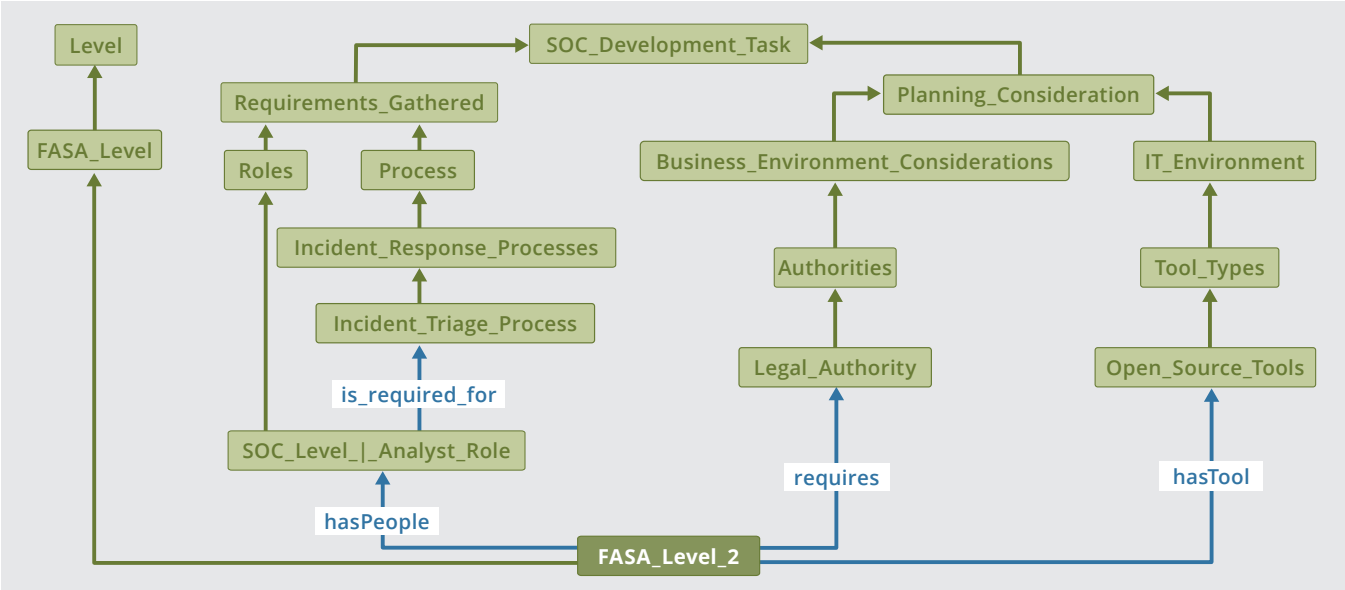


Figure 1 - Example SOC Knowledge Class Hierarchy



- 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.

Figure 2 - Forensic Analysis Service Area

OWL Entity Description Editor: ICSA_Level_5

```
1  Class: ICSA_Level_5
2
3        Annotations: [in root-ontology]
4            rafs: 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
```

Figure 3 - Axiom Defining a Service Level

OSCAR will be used to create a knowledge base that will be part of an expert system that DoD organizations can use. It will partially replace or supplement human experts (i.e., consultants), thereby decreasing costs and reducing the time required to develop and deploy SOC capabilities.

Our main goal is to align OSCAR with the needs of core DoD mission partners. Later, we may expand OSCAR to address the concerns of a more extended set of partners, including the defense industrial base and foreign allies.

As part of follow-on SEI applied research, we will integrate OSCAR into an expert system that we will create to operationalize SOC development.

These research efforts align with the SEI's technical objective to provide DoD organizations with capabilities that make new missions possible and/or improve the likely success of existing ones.

About the SEI

Always focused on the future, the Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We lead research and direct transition of software engineering, cybersecurity, and artificial intelligence technologies at the intersection of academia, industry, and government. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and are based at Carnegie Mellon University, a global research university annually rated among the best for its programs in computer science and engineering.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu

©2024 Carnegie Mellon University | 6350 | C 09.03.2024 | S 10.31.2024 | DM24-1362 | [DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.