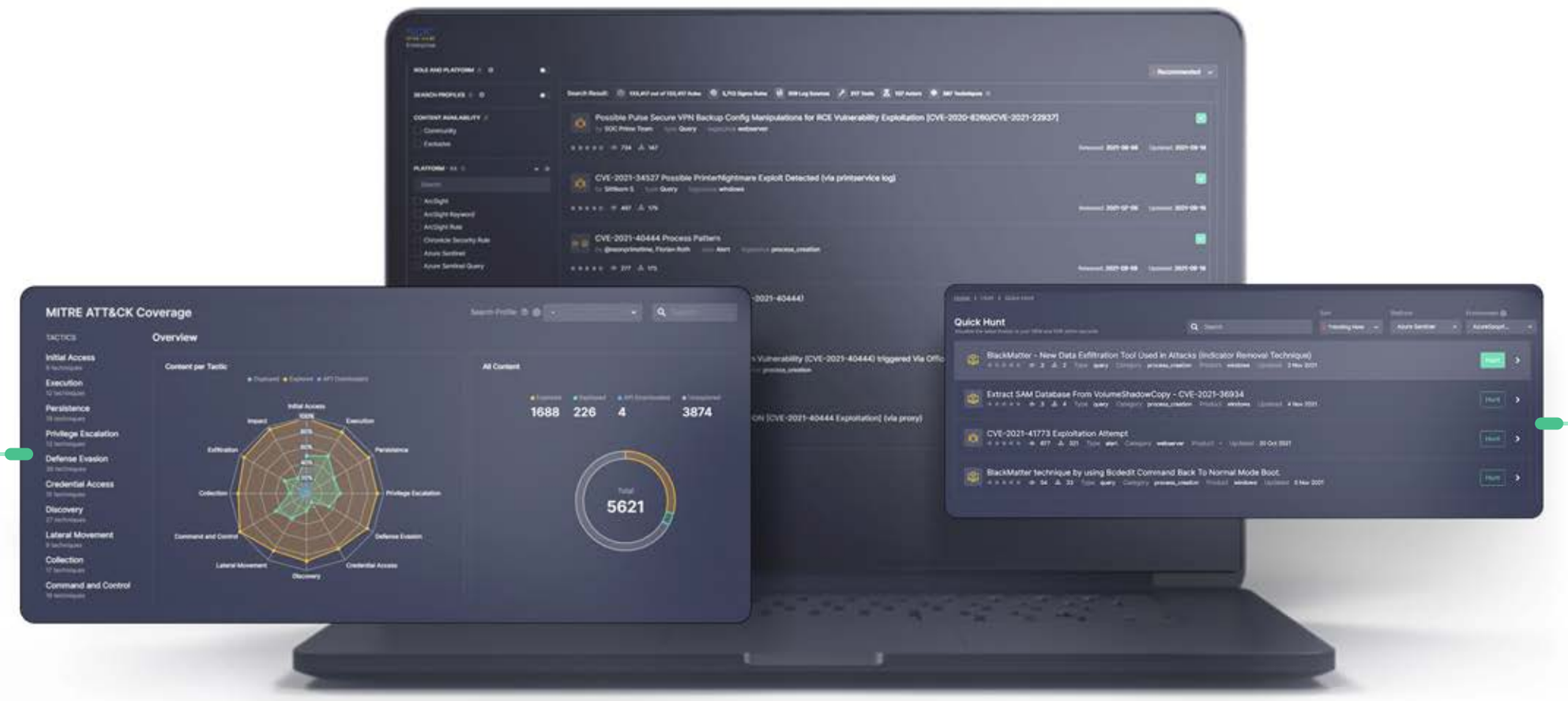
# SOC Prime Technologies for Collective Cyber Defense: Tools and Methodologies for the Global SOC

The war against Ukraine breaks out in five domains embracing land, sea, air, space, and cyberspace. The latter is the very domain that has spread beyond the Ukrainian borders since the cyber war broke out on a global scale. Nowadays, the main goal of Ukraine is to be the “shield of cyber defense” for the entire world, which will remain a crucial mission even after the Ukrainian victory in the ongoing war.

The constantly growing volumes of attack vectors and ever-increasing threat landscape complexity pose a significant menace to cyber defenders. The only way to successfully withstand offensive intrusions is to leverage the principles of collective cyber defense, acting as a global SOC.

**Collective cyber defense** is a novel approach that enables information-sharing on existing and emerging threats, including key metadata, context, and detection algorithms in real time.

SOC Prime is a pioneer developer of the world’s first technology applying collective cyber defense in action.



# SOC Prime Technologies: Instruments, Methodologies, and Practical Approaches to Collective Cyber Defense

**The course objective** is shaping students' knowledge and practical approaches to collective cyber defense, and mastering the instruments and methodologies based on SOC Prime technologies.

SOC Prime technologies are backed by innovative Detection as Code practices, Sigma language, and the MITRE ATT&CK® methodology.

### SOC Prime Platform:

the industry-first and most advanced platform for collective cyber defense aggregating the world's largest collection of over 250,000 detection algorithms ready-to-deploy to 25+ SIEM, EDR, and XDR solutions. To automate detection content search & streaming, the Platform provides dedicated integration & customization modules.

### Uncoder.IO:

the free online tool for on-the-fly conversion of Sigma rules to the native formats of 25+ SIEM, EDR, and XDR systems.

### CTI.Uncoder.IO:

the free online tool for automated generation of performance-optimized IOC-based search queries for log analysis in the native SIEM, EDR & XDR format.

### Quick Hunt:

the online tool for automated threat hunting in the selected SIEM, EDR, or XDR environment.

## What We Offer

- **Guest lectures by seasoned SOC Prime experts**
- **Self-advancement materials available online**
- **Direct access to SOC Prime resources to hone practical skills**

The best students might be offered grants for Sigma rules and MITRE ATT&CK Defender (MAD) certifications, an internship at SOC Prime, and other educational grants.

SOC Prime has established the world's largest and most advanced platform for collective cyber defense that enables cybersecurity practitioners to detect critical threats and defend against emerging attacks faster, simpler, and more efficiently than ever before. SOC Prime Platform is based on the flexible and innovative Detection-as-Code principles connecting over 30,000 cyber defenders worldwide. SOC Prime's innovation and cutting-edge cyber defense technologies with access to the world's largest repository of Sigma rules, which is continuously enriched and updated in real time, are recognized by industry leaders. SOC Prime is credited by the market-leading SIEM, XDR & MDR vendors and trusted by 8,000+ organizations, including 42% of Fortune 100 and 21% of Forbes Global 2000.

EXPLORE SOC PRIME ↗