SIGMA

One Common Language for Cyber Defenders

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, and this will remain a crucial mission even after the Ukrainian victory in the ongoing war.

Sigma is the universal language format for creating threat detection algorithms. Such algorithms identify log events that might indicate a potential cyber attack or any other form of malicious activity.

Sigma acts as one common language for cyber defenders, which allows detecting cyber attacks in real time. Leveraging Sigma, detection algorithms are fast to share and easily convertible into the native format of the SIEM, EDR & XDR solutions. Such approach ensures an efficient and future-proof foundation for collective cyber defense on a global scale.

The Sigma language was invented in Germany by Thomas Patzke and Florian Roth who are the current advisory board members of SOC Prime, the U.S.-based company with Ukrainian roots, which is the biggest backend contributor and major evangelist of Sigma among the global cyber defender community.

Before the invention of Sigma, the cybersecurity industry was challenged with a lack of experts skilled at developing anti-virus signatures making it harder to keep up with emerging cyber attacks and proactively withstand them. The use of Sigma as a universal cybersecurity language has totally transformed the approach to cyber defense. Being armed with Sigma rules, the entire global community gained access to the detection algorithms covering TTPs that were or will be used cyber attacks. For instance, the analysis of the destructive cyber attack by Sandworm APT on the Ukrainian power facilities in April 2022 has indicated that detections addressing 9 out of 13 adversary technologies have already existed and were developed two years earlier, in 2020.

Backed by Sigma knowledge, cybersesurity practitioners gain direct access to the global industry expertise and skillset that will remain in high demand for decades. Moreover, cybersecurity professionals highly skilled at Sigma can work with any modern SIEM, EDR, or XDR tool.

Sigma is listed as one of the industry’s best cyber defense technologies and recommended by such leading cybersecurity organizations as Cybersecurity & Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), SANS Institute and Gartner.

Sigma Basics

The course objective is shaping students' knowledge of Sigma, precoditions of its invention and the stages of the language development, practical methodolofies of its application, and basic skills of writing Sigma rules.

Introduction to the Sigma language

Precoditions of its invention, the history of Sigma evolution and the stages of its development in the cybersecurity industry. The foundation of collective cyber defense (SigmaHQ, SOC Prime Platform, Threat Bounty Program).

Basics of Sigma rules development

The Sigma methodology, syntax, and taxonomy. Sigma rules development and log description, metadata description.

Standartization of log description and event sources

Mapping. Sigma rule conversion to the SIEM, EDR, and XDR formats.

Practice

The development and practical use of Sigma rules.

What We Offer

- **Guest lectures from the seasoned SOC Prime experts**
- **Self-advancement materials available online**
- **Direct access to the SOC Prime resources for mastering Sigma skills**

The best students 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 ↗