Detection Rule Automation Engine

Streamline Rule Management and Translation for Enhanced Security

SOCURA

DRAE, the Detection Rule Automation Engine, is designed to simplify the management and translation of Sigma rules across different SIEM and EDR platforms in an MSSP environment. With DRAE, you can effortlessly maintain and synchronise security rules across diverse environments, ensuring consistent and effective threat detection.

Key Features

1. **Rule Centralisation:** DRAE acts as a central repository for Sigma[1] rules, providing a unified location for rule management. Containing in-house curated content alongside community-maintained content.
2. **Multi-Platform Translation:** Seamlessly translate Sigma rules into many different languages eliminating manual rule conversion tasks.
3. **Automated Updates:** Keep your rules up-to-date across all SIEM platforms, reducing the risk of security gaps.
4. **Version Control:** Maintain a complete history of rule changes and revisions for audit and compliance purposes.
5. **Customisation:** Tailor rule translation settings to match your specific SIEM platform configurations.
6. **Rule Validation:** Validate translated rules to ensure accuracy and compatibility with your target SIEM system.
7. **Rule Collections:** DRAE introduces a powerful rule collection feature that allows you to group rules with similar objectives, making it easier to manage, organise, and maintain your security rule sets. Whether you're dealing with Sysmon configurations, firewall rules, or privilege escalation detection, DRAE's rule collections streamline the organisation of rules for specific purposes.

Key Benefits

Improved Efficiency
DRAE automates time-consuming rule management and translation tasks, freeing up security teams to focus on critical threat analysis.

Enhanced Security
Consistent rule application across SIEM platforms reduces the risk of missed threats and vulnerabilities.

Compliance Readiness
Documented rule history and version control simplify compliance reporting and auditing.

[1] Sigma - https://sigmahq.io/

MITRE ATT&CK® Mapping & Analysis

DRAE leverages DeTTECT's[2] mapping capabilities and performs gap analysis, allowing organisations to proactively strengthen their security defences, ensuring they stay ahead of evolving threats and align with industry best practices as defined by the MITRE ATT&CK® framework[3].

Enhanced Rule Development
Identify specific MITRE ATT&CK® techniques with insufficient rule coverage and develop new rules to address them.

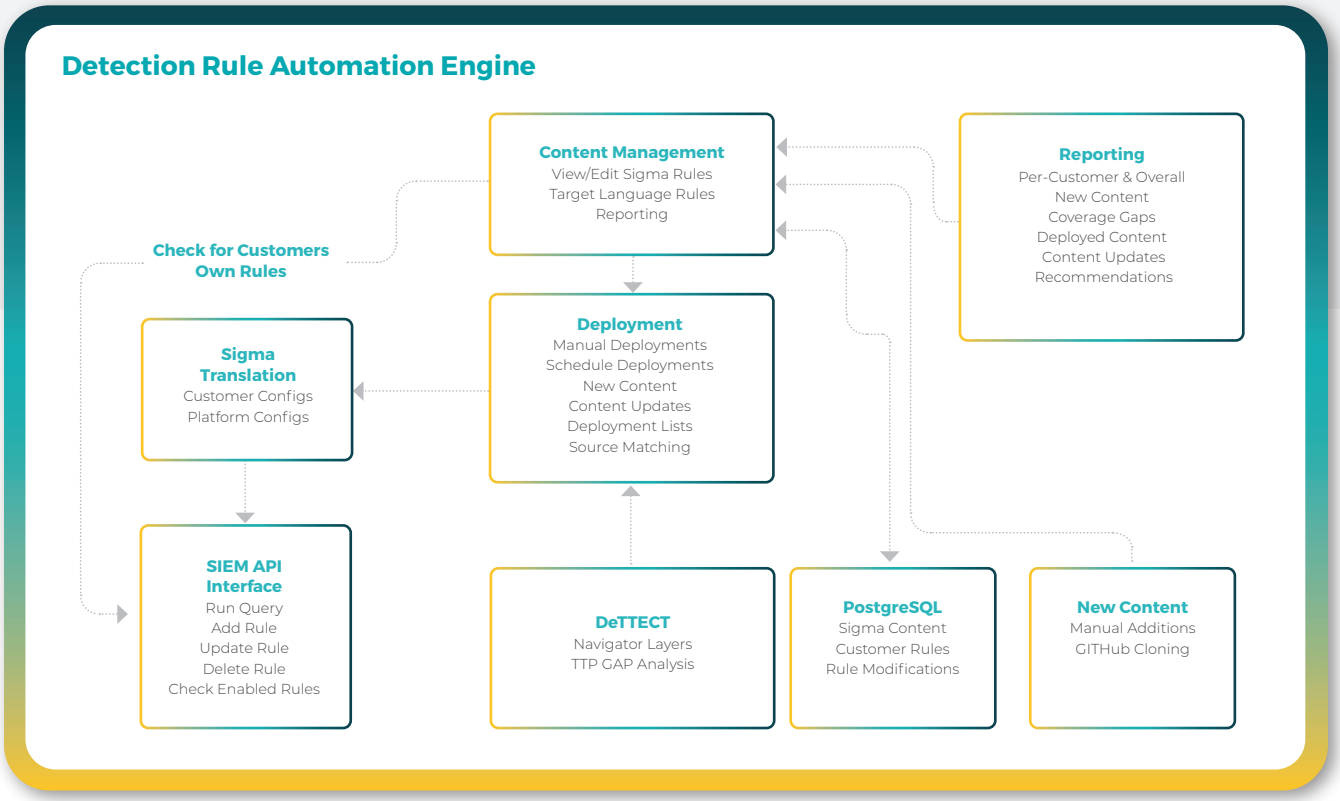
Data Source Augmentation
Determine which data sources lack coverage for critical MITRE ATT&CK® tactics and techniques and consider enhancing logging capabilities.

Rule Refinement
Improve existing rules to reduce false positives and enhance their effectiveness in detecting adversarial TTPs.

Resource Allocation
Allocate resources effectively to address the most critical gaps first, ensuring a strategic and risk-based approach to security enhancement.

Continuous Improvement
Leverage DRAE's rule version control and update automation to maintain an up-to-date and adaptive security posture.

DRAE empowers you to not only manage and translate security rules but also to evolve your security strategy in a dynamic threat landscape.



SOCURA

[2] DeTTECT - https://github.com/rabobank-cdc/DeTTECT

[3] MITRE ATT&CK® framework - https://attack.mitre.org/

socura.co.uk