BOOST YOUR
SIEM EXPERIENCE

YOU SHOULD:

1. **Keep up with the changing threat landscape**
2. **Track, measure, and visualize alert coverage**
3. **Continuously refine the rule base**
4. **Enforce preventative and detection layer improvements across the organization**

HOW QUICKLY CAN YOU DEVELOP
DETECTION RULES?

7 Hours

Average time required to develop a detection rule*

A 2020 survey by Picus Customer Success Team found out that it takes **7 hours** on average to write a detection rule.

"DETECTION AS CODE" SUPPORTED BY
BREACH AND ATTACK SIMULATION (BAS)

"Detection as Code" is a recent concept laid out by **Anton Chuvakin** aiming to develop or obtain high-quality detection rules consistently as an organizational capability. **3 key benefits of BAS for implementing detection as code:**

Automated gap analysis help correctly prioritize **detection engineering efforts**

Offers proper quality assurance through in-depth validation of defense capabilities

Continuous improvement to keep up with the changing threat landscape becomes an organizational capability

ACHIEVE
SMARTER SIEM ALERT MANAGEMENT

Powered by Breach and Attack Simulation Technology, Picus Security developed a **Continuous Security Control Validation** approach that helps: