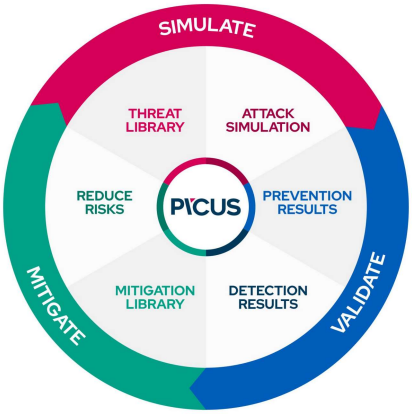
The **Picus** Complete Security Control Validation Platform **leverages Breach and Attack Simulation (BAS) technology** to validate security controls in a continuous and risk-free way. It also provides actionable **mitigation recommendations**, which enable organizations to quickly and effectively address **threat prevent** and **detection gaps**.



We offer;

- **Simulation:** Simulate real-world threats against organization's networks, endpoints, and cloud-based security controls.
- **Validation:** Validate the effectiveness of organization's prevention and detection security controls in order to identify and prioritize security gaps.
- **Mitigation:** Leveraging vendor-specific mitigations and best practices to harden security controls.

The Picus Platform offers **Detection Analytics** to **validate the effectiveness** of Security incident and Event Management (**SIEM**) and Endpoint Detection and Response (**EDR**) **tools**. Organizations can use Detection Analytics on each attack simulation module; Network Infiltration, Email, Web Application, Endpoint, Data Exfiltration. We need to deploy an integration agent to enable us to query and analyse SIEM and EDR logs and alerts generated as a result of our attack simulations.

In Security Operation Centers (SOC), Blue Teamers are responsible of managing multiple systems, monitoring all of them, looking for suspicious activities that could be indicative of health issues, security incidents, or compromises. To obtain a maturity assessment or SOC Infrastructure Management, there are three primary services stand in the core; **Log Management, Alert Monitoring, and Detection Engineering**. Thus, **these services must be healthy** and work very effectively in order to ensure and increase the maturity of Blue Teamers. **It requires too much time, effort, focus and high proficiency to have an awareness of log visibility, alert management and detection engineering.**

As The Picus Complete Security Control Validation Platform runs continuous attack simulations, it triggers the logs and alerts on organization's SIEM and EDRs. Such alerts may cause too many false positives or not triggering at all. Think about the main concerns of SOC teams/Blue Teamers experience while operating and managing these services. Advice a solution that Picus can offer while managing the enormous amounts of alerts/logs created by attack simulations or any other false positives caused by other actions.

You can proceed with **answering the following questions** leading you to solution. You can address the learnings of the **course Proactive Security Operations Center** (SOC) on **Purple Academy** while defining the problems and proposing the solution.