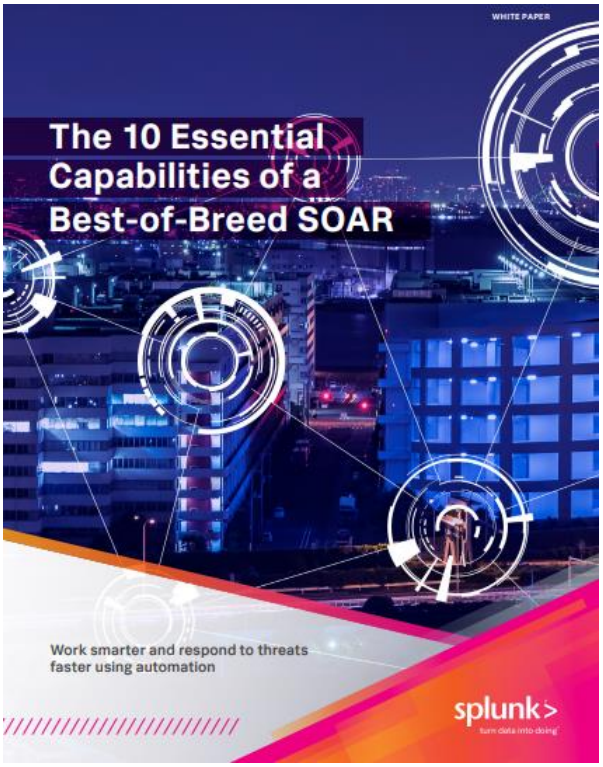
The 10 Essential Capabilities of a Best-of-Breed SOAR



Ask a group of security analysts about the challenges of working in cybersecurity, and you'll likely hear some common themes, like a high volume of security alerts, too many security point-products to manage, and a shortage of skilled cybersecurity talent. Considering these challenges, it's no surprise that security teams feel perpetually overwhelmed.
Many teams have turned to security orchestration, automation and response (SOAR) tools as a remedy. But not all SOAR solutions are created equal.

In this white paper, we'll outline 10 essential capabilities that should be top-of-mind when evaluating SOAR technology, including:

- Machine-based execution of security actions using "playbooks" to increase speed and efficiency
- Event and alert management capabilities to prioritize inbound security events
- Case management to drive holistic management of a security incident, from inception to resolution