

CYBERSECURITY ANALYTICS AND OPERATIONS HAS EVOLVED

To accommodate data growth while enriching, contextualizing, and acting upon security intelligence in real time, CISOs are moving towards a tightly integrated security operations and analytics platform architecture (SOAPA).

Too Many Tools

On average, organizations are using between **25 AND 30 DIFFERENT SECURITY TECHNOLOGIES AND SERVICES.**



Security Analytics and Operations Challenges

Some of the biggest challenges that organizations face have to do with time – focusing too much time on tactical issues and not enough on strategy and process improvement, and the length of time it takes to remediate security incidents – the lack of tools and processes to operationalize threat intelligence, and the skills and resources required to focus on security analytics and operations.



27%

Too much time spent addressing high priority/emergency issues and not enough time on strategy and process improvement



23%

It takes too long for my organization to remediate security incidents



21%

We don't have the appropriate skills or staff size to keep up with all of the tasks associated with security analytics and operations

Security Analytics Processes



99% report that **security analytics is done in a siloed way**

81% are moving to a **consolidated and integrated approach**



Priorities for Security Analytics Automation and Orchestration



Integrating external threat intelligence with internal security data collection and analysis

35%



Adding custom functionality that sits above existing security tools

30%



Automating basic remediation tasks

29%



Correlating and contextualizing security data from multiple tools

28%

The Bigger Truth

Splunk's Adaptive Response enables security teams to address the Security Analytics and Operations challenges by enabling the automation of information retrieval, sharing, and response in multi-vendor security and IT environments to speed the time to make decisions and take actions, remaining essentially unchanged.

[Learn More](#) about Adaptive Response.

splunk >