A Day in the Life of a

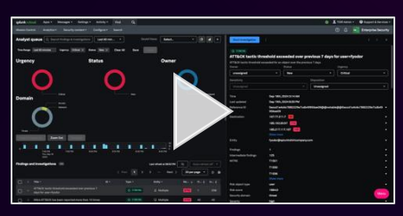
SOC Analyst

A SOC analyst typically starts their day by reviewing the alerts that have been generated overnight by various security tools in the analyst queue.

The analyst reviews the finding(s) from a detection in the analyst queue. The findings are classified based on the *Risk* scores, helping the analyst to prioritize the criticality of the alerts.

T Threat

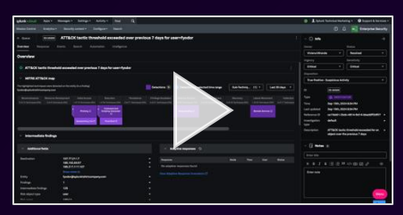
Splunk customers can see a reduction of "*their false positive rates from an average of 48% to 26%, a 46% improvement on average* [1]



D Detection

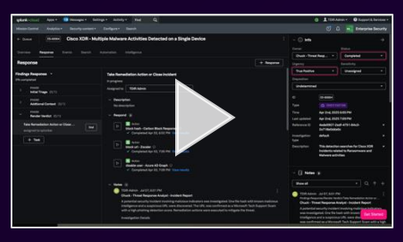
Having identified a high-priority alert, the analyst proceeds with an in-depth investigation to understand the scope and impact of the potential threat by analyzing indicators of compromise (IoC). For example, the security practitioner can run SPL searches to enrich the investigation.

"Travis Perkins PLC was able to reduce security incident investigation time from 3 weeks to 3 hours." [2]



I Investigation

The analyst can now take informed actions such as triggering Adaptive Response actions and /or playbooks based on the IoCs to isolate the infected endpoint and prevent the attack from spreading to other systems. Once the threat has been resolved and the disposition has been marked as true positive or false positive, the soc analyst generate a report on the actions taken and its response Lastly, the expert can proactively hunt for potential threats that may have bypassed initial security controls.



R Response

At the end of the day, Splunk's users obtain an unified platform that *"speeds up incident response (59%) and cuts down on tool maintenance (53%).*[3]

1 IDC The Business Value of Splunk Security: A Unified TDIR Platform; 2 Travis Perkins PLC Adopts Analytics-Driven SIEM to Enable Hybrid Cloud Transition; 3 State of Security 2025: The Stronger, Smarter SOC of the Future