# SIEMPLIFY
## THREATNEXUS™

FOR

splunk>

SOLUTION BRIEF

SIEMPLIFY FOR splunk>

## Highlights

*Siemplify ThreatNexus™ is a centralized security orchestration and incident response platform designed for the entire security operation to manage, investigate, and automate threat response from a single pane of glass.*

*ThreatNexus for Splunk enables security teams to instantly upgrade the full scope of functionality, delivering immediate productivity and security gains.*

> By applying Siemplify ThreatNexus™ platform to their existing Splunk deployment, organizations are able to transform any existing log repository into a robust platform, meeting the diverse needs of the modern SOC.

## SPLUNK AND THE SECURITY CHALLENGE

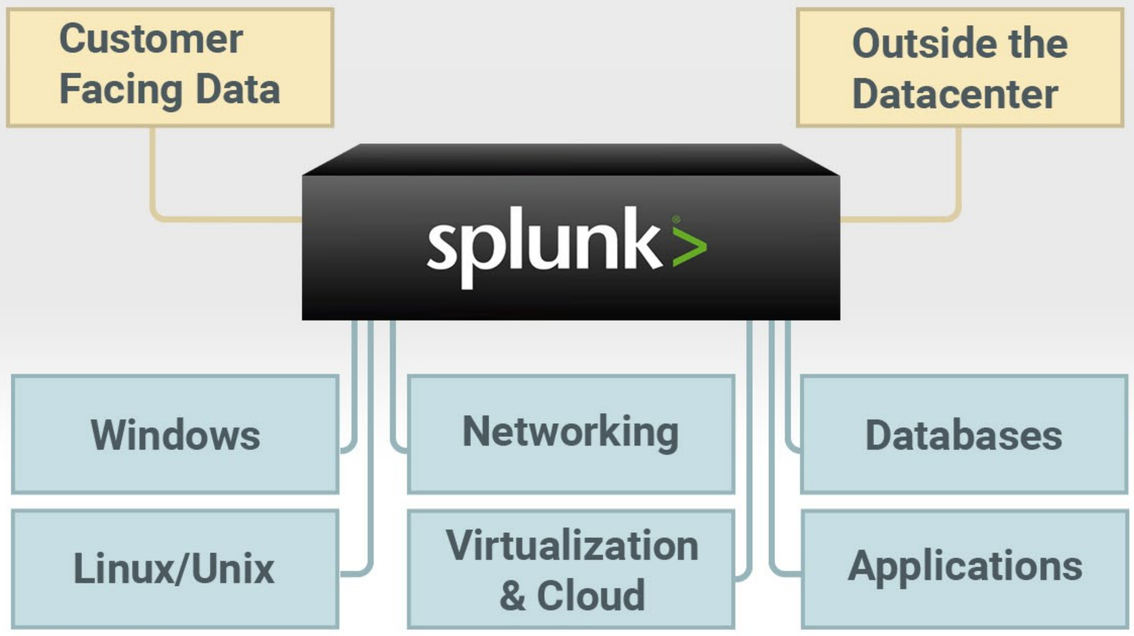
- Enterprises are attempting to leverage Splunk as a SIEM replacement, with growing frustration.
- Security teams are being asked to mature their security operations around Splunk, and while valuable as a log repository, lacks the core capabilities to power the Intelligent SOC – prioritization, contextualization, automation, among other functionality.
- Splunk Enterprise Security is often looked to as a solution, but merely offers a library of queries and doesn't solve the broader security challenges challenges.
- The result is slow painful queries driving significant manual intervention among analysts.

## BENEFITS OF SIEMPLIFY + SPLUNK

- Fuse static log data with other security tools and data to create fully contextualized cases -- driving significant ROI from legacy security investments.
- "Securitize" your Splunk to create a comprehensive SOC solution.
- Dramatically enhance analyst productivity and reduce the time to respond to threats.

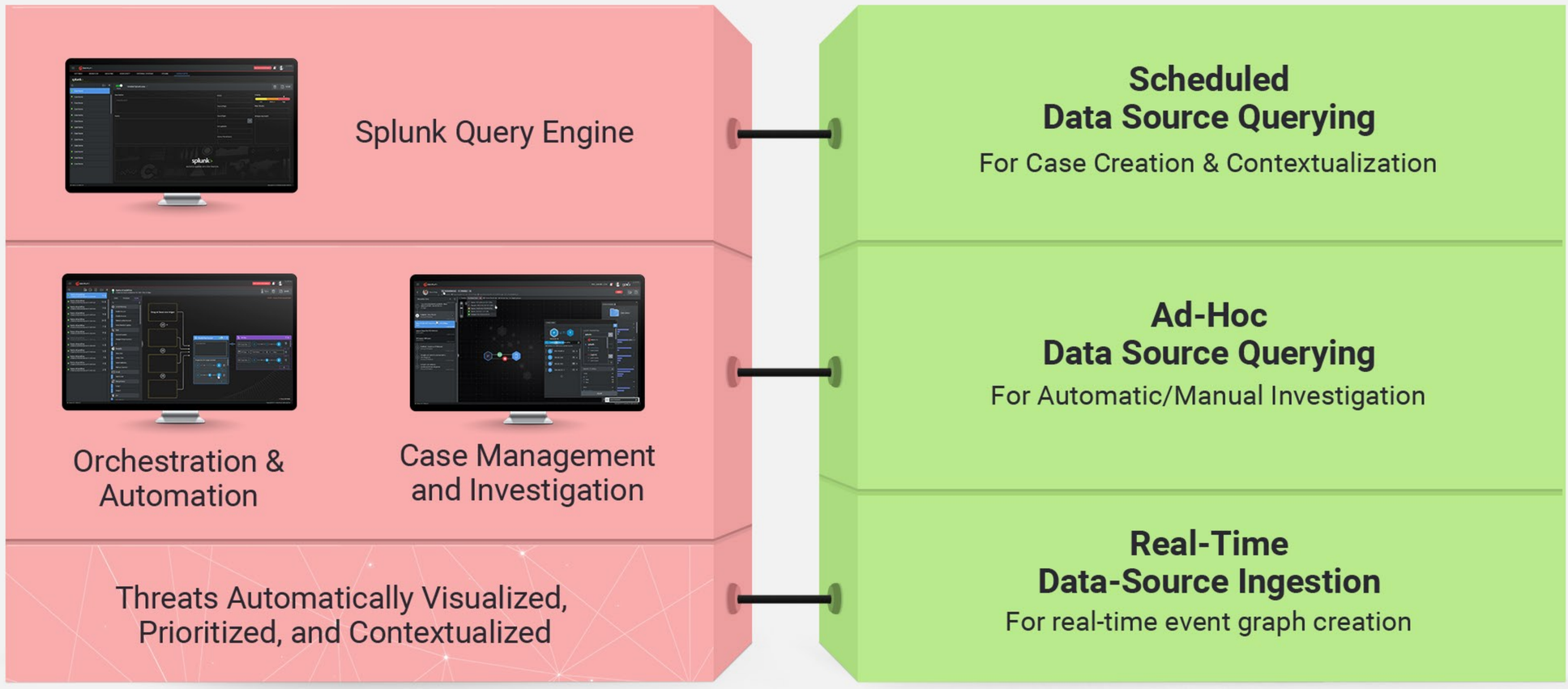
# Security Orchestration for Splunk

## SOC CHALLENGES WITH SPLUNK




While Splunk has proven to be a powerful platform in the way of log retention and data querying, It is not inherently designed to meet the diverse need of the security team.


## SIEMPLIFY INTEGRATION WITH SPLUNK




**Splunk Query Engine**

Our Splunk Query Engine allows customers to centrally create, import, and manage the execution of queries against Splunk in order to support use-cases relevant to your organization.  Siemplify enables Splunk customers to leverage existing Enterprise Security investments, or to operate more efficiently without it.

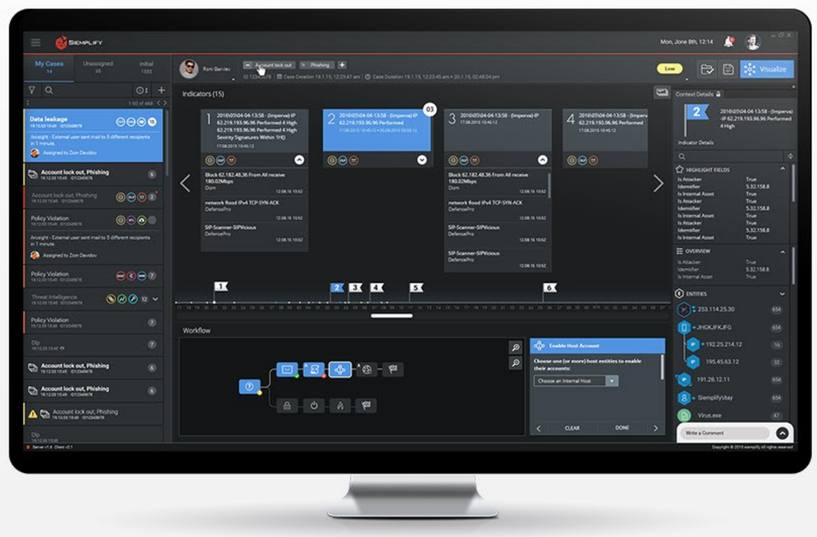
# Siemplify's ThreatNexus™

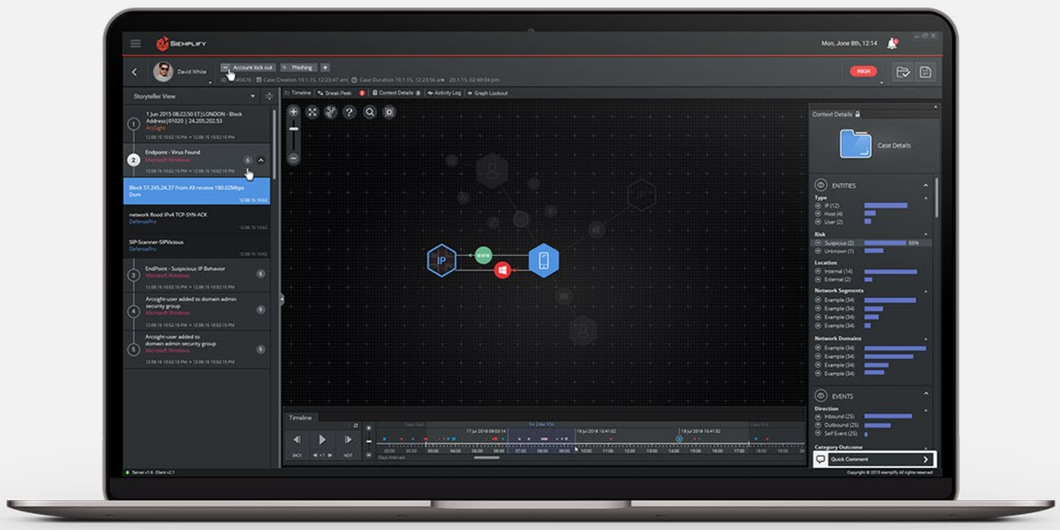
## Security Orchestration and Incident Response


- Security Operations from a single pane of glass
- Consolidate security alerts by 80 percent
- Automatically prioritize threat storylines
- Automate and Orchestrate workflows
- Triple analyst capacity
- Drive ROI from existing security investments
- Reduce time-to-remediate from months to minutes

## CASE MANAGEMENT

ThreatNexus connects the disparate tools across the security footprint to become the nucleus serving security operations. Alerts are clustered with related threat indicators into prioritized cases. Fully contextualized cases are either fed through the automation engine or presented to analysts for rapid triage and management.



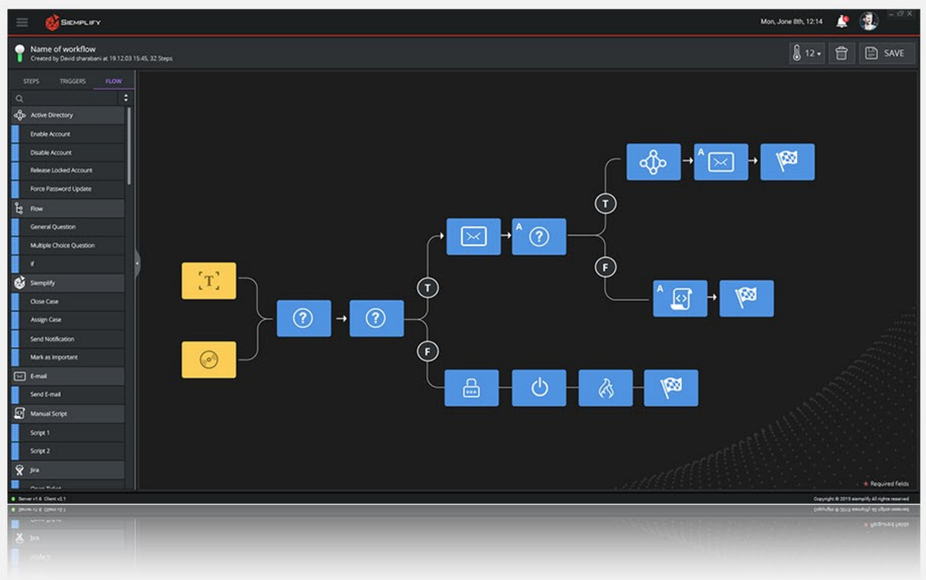


## INVESTIGATION

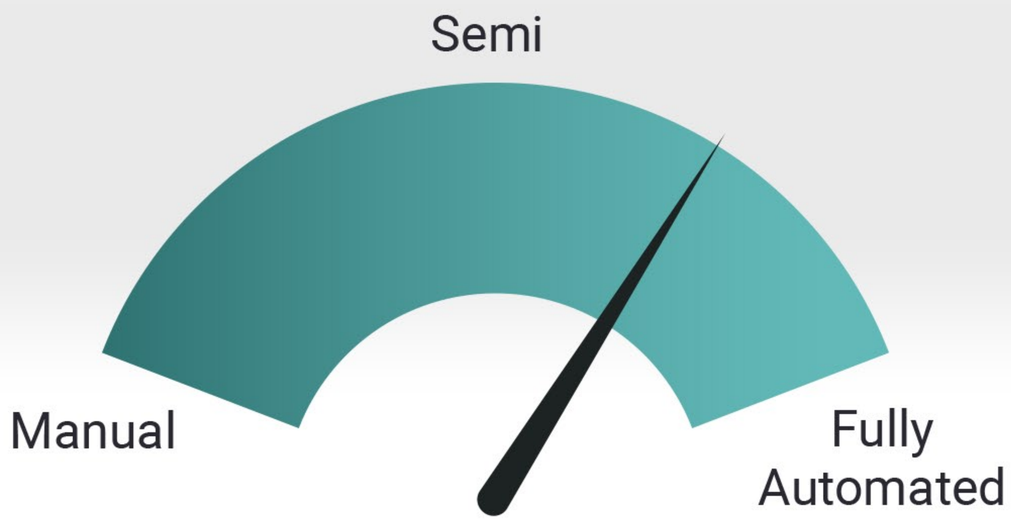
ThreatNexus provides rapid investigation for all levels of security analysts. By integrating disparate security tools throughout the enterprise, analysts can investigate incidents through a single pane of glass. Analysts can execute lightning fast root cause analysis, rapidly pivoting from threat detection to response and mitigation.

## AUTOMATION

ThreatNexus contextual based approach to orchestration and automation provides the ultimate balance between machine driven and analyst led response.



# ThreatNexus Immediately Transforms Splunk Deployments




## Machine Driven & Analyst Enabled Response

The full range of automation is at your disposal – from complete automation of incident response, to semi-automatic workflows, to playbooks to standardize incident management process.  The result is a flexible mix of automated task/flows and highly intuitive, analyst led investigation – striking the ultimate balance of machine driven and analyst led response.

## Ontology Enabled Context

Utilizing Siemplify Cyber Ontology we integrate Splunk data to the other relevant sources across the security footprint (Threat Intelligence, Vulnerability, AD, etc.) to enrich cases with the needed context to understand the complete threat storyline.  The result is prioritized cases with complete understanding of the full scope of entities and relationships involved in a threat.


## Rapid Deployment across Complex Environments

Easily deploy ThreatNexus with wizard-driven installation and integration.  Most new customers are fully operational within hours.