Turn Data Into Doing

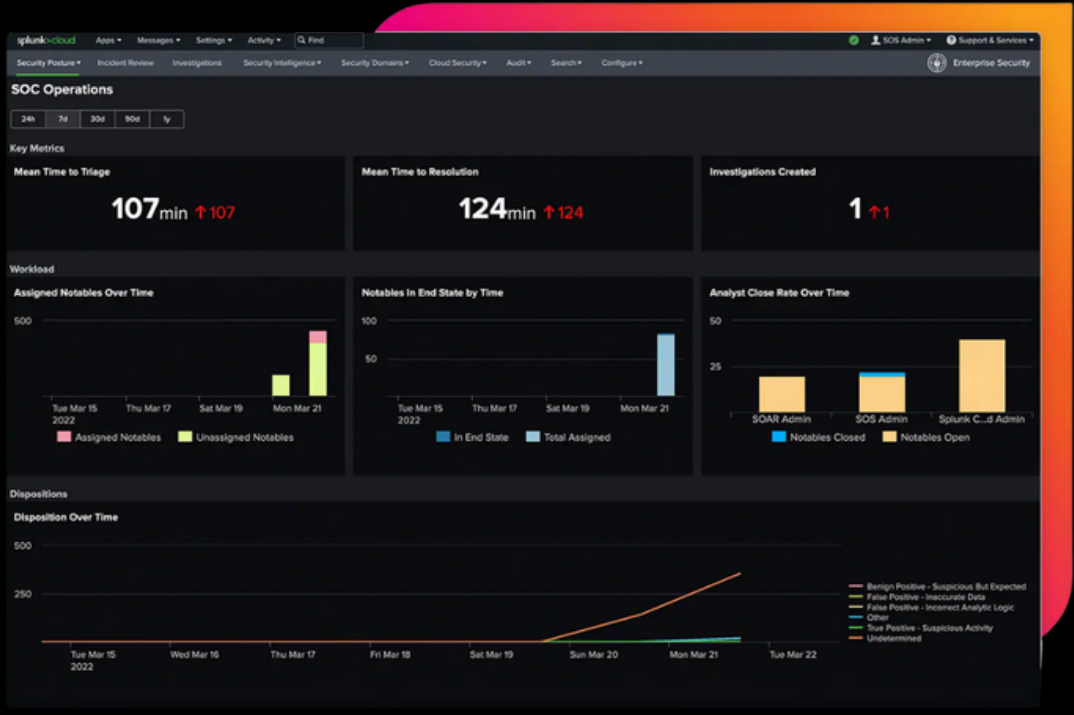
True Zero's Services Team has been purpose-built with seasoned industry experts, possessing the necessary Splunk certifications to deliver quality and repeatable solutions.

Splunk and True Zero have partnered closely to bring high-value and high-impact services to organizations that have predictable outcomes and enable customers to innovate and re-envision their security and operations programs through the power of Splunk.

Powered By

"We have developed and cultivated an environment and culture where highly skilled technologists and engineers thrive while also enabling the consistent capture of lessons learned across our entire customer base, that are then embedded into our solutions and methodologies we take to market."

-Jonathan Cooper, CTO



True Zero's Services Team has been purpose built with seasoned industry experts, possessing the necessary Splunk certifications to deliver quality and repeatable solutions. Splunk and True Zero have partnered closely to bring high value and high impact services to organizations that have predictable outcomes and enable customers to innovate and re-envision their security and operations programs through the power of Splunk. In addition to Splunk Cloud expertise, True Zero's Splunk team members possess deep skills in other tools commonly integrated with Splunk, including Tanium, ZScaler, Crowdstrike, CRIBL, and GitLab. As a result, True Zero consultants can advise you on your broader vision in addition to Splunk for greater value.

YOUR TARGET OUR MISSION

True Zero's long history of successfully executing on many cybersecurity projects has fine-tuned a success methodology that ensures a rapid path to value while maintaining an agile flexibilty for organization-specific customization.

Success Methodology

SCOPE

Our seasoned consultants will work closely with you to identify core requirements and necessary resources in order to develop a tailored implementation plan that accounts for performance, budgets, and end state success to optimize your return on investment.

DESIGN

Our team will design the best possible architecture including all deployment steps, prerequisites, and level of effort needed to ensure a smooth best practice deployment of your Splunk environment.

DEPLOY

Utilizing our best practice deployment methodologies, including options for completely automated implementations, our team of consultants will rapidly install, configure, and operationalize your Splunk environment, while providing cross training for your internal engineering teams.

EVALUATE

Working alongside your stakeholders, our team will evaluate success against use case requirements to ensure Splunk is performing optimally and that all teams are getting the value expected from Splunk.

TUNE

Based on feedback and observations, our consultants will tune and adjust content to ensure actionable and accurate results are generated and support the expectations of success from all stakeholders.

EXPAND

As use cases mature, identification of additional data sources and use cases is inevitable. Our consultants have a wide range of experience performing an array of integrations and custom content development, and our team will support the identification and evolution of content and integrations needed.

ENTERPRISE DEPLOYMENT SERVICES

True Zero's consultants have been implementing, deploying, and upgrading enterprise and agency wide Splunk solutions across the federal, civilian, Department of Defense, State and Local Governments, and Commercial business entities collectively for over 10 years. True Zero's Services Team has been purpose built with seasoned industry experts, possessing the necessary Splunk certifications to deliver quality and repeatable solutions.

True Zero offers three deployment service packages to ensure appropriate scoping and to achieve rapid time to value. If project requirements dictate broader scoping parameters than the packaged offerings below, please contact us directly so one of our experts can work with you on the best approach designed for your specific needs.

PHASES	TASKS	STANDARD	PLUS	PREMIUM
SCOPE	Detailed scoping session with customer, build a tailored implementation plan, capture use cases, and required data sources, as well as success criteria	✓	✓	✓
DESIGN	Design and document "to-be" solution	✓	✓	✓
DEPLOY	Implement design according to Splunk best-practices	✓	✓	✓
	Apply security hardening configurations	✓	✓	✓
	Implement data management strategy and access control	✓	✓	✓
	On-board data sources	✓	✓	✓
	Implement Splunk apps & add-ons for enhanced features/use cases	SplunkBase	+ Custom (1)	+ Custom (3)
	Automate deployment (CICD Methodology)		✓	✓
EVALUATE	Perform functional testing of content, evaluate against success criteria, solicit feedback from stakeholders and document next steps/recommendations.	✓	✓	✓
TUNE	Adjust and modify content based on evaluate phase		✓	✓
EXPAND	Identify and expand use cases based on new requirements			✓

Visit Our Website
www.truezerotech.com

Contact Us
info@truezerotech.com

ENTERPRISE SECURITY SERVICES

True Zero specializes in Enterprise Security deployments, enhancements, tuning, and advanced security content development. Our experience building large scale security programs from both a technical and strategic perspective has heavily influenced what we see as a superior path to success as it relates to SIEM deployments. Our methodology is based on a cyber resilience strategy where we view the end state of a SIEM deployment as being a mechanism by which actionable content is promoted based on a threat actor perspective tied to our customer's business context. This ensures that throughout the deployment process, our team is consistently influencing the path based on traditional cybersecurity market trends, best practices, and also taking into account the specificity of each customer's threat profile. We have found that this approach has far more positive impacts on our customers security programs as it truly enables capturing the correct data for the proper use case.

True Zero offers three Enterprise Security service packages to ensure appropriate scoping and to achieve rapid time to value. If project requirements dictate broader scoping parameters than the packaged offerings below, please contact us directly so one of our experts can work with you on the best approach designed for your specific needs.

PHASES	TASKS	STANDARD	PLUS	PREMIUM
SCOPE	Detailed scoping session with customer, build a tailored implementation plan, capture use cases, and required data sources, as well as success criteria	✓	✓	✓
DESIGN	Design and document "to-be" solution	✓	✓	✓
DEPLOY	Implement design according to Splunk best-practices	✓	✓	✓
	Apply security hardening configurations	✓	✓	✓
	Implement data management strategy and access control	✓	✓	✓
	On-board data sources	✓	✓	✓
	Common Information Model (CIM) Compliance Check	✓	✓	✓
	CIM Mapping		2 Custom Data Sources	4 Custom Data Sources
	Correlation Search Use Case Identification	✓	✓	✓
	Correlation Search Enablement	✓	✓	✓
	Custom Correlation Searches		4 Custom Use Cases	6 Custom Use Cases
	Asset/Identify/Threat Integration	LDAP/CMDB	✓	✓
	Automate deployment (CICD Methodology)		✓	✓
EVALUATE	Perform functional testing of content, evaluate against success criteria, solicit feedback from stakeholders and document next steps/recommendations.	✓	✓	✓
TUNE	Adjust and modify content based on evaluate phase		✓	✓
EXPAND	Identify and expand use cases based on new requirements			✓

Visit Our Website
www.truezerotech.com

Contact Us
info@truezerotech.com

CLOUD MIGRATION SERVICES

Migrations to the cloud are accelerating at a rapid pace across all industries. Software as a Service (SaaS) options are plentiful and present an easy-to-use platform that is almost "turnkey". True Zero understands that when it comes to enterprise migrations, whether native cloud or hybrid solutions, nothing is ever "turnkey". The same applies to customers who seek to migrate their on-premises Splunk environments to Splunk Cloud, Splunk's SaaS offering.

True Zero offers three cloud migration service packages to ensure appropriate scoping and to achieve rapid time to value. If project requirements dictate broader scoping parameters than the packaged offerings below, please contact us directly so one of our experts can work with you on the best approach designed for your specific needs.

PHASES	TASKS	STANDARD	PLUS	PREMIUM
SCOPE	Detailed scoping session with customer, build a tailored implementation plan, capture use cases, and required data sources, as well as success criteria	✓	✓	✓
DESIGN	Design and document "to-be" solution	✓	✓	✓
DEPLOY	Implement design according to Splunk best-practices	✓	✓	✓
	Apply security hardening configurations	✓	✓	✓
	Implement data management strategy and access control	✓	✓	✓
	Configure LDAP or SAML authentication	✓	✓	✓
	High availability planning		✓	✓
EVALUATE	Perform functional testing of content, evaluate against success criteria, solicit feedback from stakeholders and document next steps/recommendations.	✓	✓	✓
TUNE	Adjust and modify content based on evaluate phase		✓	✓
EXPAND	Identify and expand use cases based on new requirements			✓

Visit Our Website
www.truezerotech.com

Contact Us
info@truezerotech.com

SOAR DEPLOYMENT SERVICES

True Zero has developed this specific SOAR deployment service offering to ensure a stable, expandable, and performant solution that meets your success criteria. Through True Zero's decades of collective experience enabling large-scale security programs to automate response actions to emerging threats, we have the skills and knowledge to develop custom playbooks within the SOAR platform to meet your needs, improve mean time to detection (MTTD) and mean time to resolution (MTTR).

True Zero offers three Splunk SOAR Deployment packages to ensure appropriate scoping and to achieve rapid time to value. If project requirements dictate broader scoping parameters than the packaged offerings below, please contact us directly so one of our experts can work with you on the best approach designed for your specific needs.

PHASES	TASKS	STANDARD	PLUS	PREMIUM
SCOPE	Detailed scoping session with customer, build a tailored implementation plan, capture use cases, and required data sources, as well as success criteria	✓	✓	✓
DESIGN	Design and document "to-be" solution	✓	✓	✓
DEPLOY	Implement design according to Splunk best-practices	✓	✓	✓
	Apply security hardening configurations	✓	✓	✓
	Perform platform integration with customer tooling such as Splunk Enterprise, Splunk Enterprise Security, or any other enterprise solution based on customer requirements	✓	✓	✓
	Enable external application API integration into Splunk SOAR	✓	✓	✓
	Build playbooks to automate standard operating procedures (SOPs) and tier 1 tasks.	3	5	8
	Enable external application API integration into Splunk SOAR	✓	✓	✓
	Identify security use cases and form SOPs		✓	✓
EVALUATE	Perform functional testing of content, evaluate against success criteria, solicit feedback from stakeholders and document next steps/recommendations.	✓	✓	✓
TUNE	Adjust and modify content based on evaluate phase		✓	✓
EXPAND	Identify and expand use cases based on new requirements			✓

Visit Our Website
www.truezerotech.com

Contact Us
info@truezerotech.com