DATA SHEET

Zscaler Professional Services

Deception Deployment Offerings:

Essentials and Advanced

Zscaler Deception is a simple, faster, and more effective targeted threat detection solution built on the Zscaler Zero Trust architecture.

Deception uses advanced lures and decoys to detect and disrupt sophisticated threats that consistently bypass traditional defenses, such as advanced persistent threats (APT), exploits, reconnaissance, lateral movement, active directory, supply chain, human-operated ransomware, supervisory control and data acquisition (SCADA), and industrial control system (ICS) attacks. As an integral part of the Zscaler Zero Trust Exchange, Deception integrates with zero trust, tracking the full attack sequence and initiating automated response actions across the Zscaler platform.

Our Professional Services (PS) Consultant will work with your organization to deploy Deception and unlock the benefits of this product for your environment.

Benefits of Professional Services:

- **Valuable Zscaler Experience** Our PS Consultants bring deep architectural and operational experience, bolstered by thousands of implementations, that help you reduce risk and increase project success
- **Bridge Resources and Knowledge Gaps** Access Zscaler's expertise to efficiently fill potential skill or resource gaps, without having to hire additional resources
- **Leading Practice Guidance** Achieve your business objectives quickly by leveraging our years of experience and knowledge of leading practices
- **Accelerate ROI** Feel confident knowing your deployment has been set up for success, by relying on Zscaler's proven project methodology

Deception Essentials – Detailed Professional Services Scope	

Scope	Review customer environment and validate Deception use cases. Apply leading practices to design and deploy Deception technologies in a scalable environment. Implementation limited to a maximum of 20 decoys and one landmine policy.
	
	*** Deployment of Zscaler Client Connector, ZIA or ZPA setup must be completed prior to engagement**
	
	Platform Setup:
	• Admin Account Access
	• Admin SSO Integration
	• Configuration of up to two (2) enrichment integrations
	Use Cases Deployed:
	• Reconnaissance:
	  • Up to three (3) Perimeter Decoys (Threat Intelligence or Cloud Decoys)
	• Credential Access and Collection*
	  • One Corporate wide landmine policy redirecting users to Decoys
	  – Browser Lures
	  – Session Lures
	  – File set lures using local files
	  • AD Decoys in one (1) domain and up to seven (7) decoy objects
	  • AD Kerberoasting detection through AD decoys
	• Lateral Movement
	  • One decoy connector in one location
	  • Up to six (6) Zero Trust Network Decoys
	  • Up to three (3) Network Decoys
	• Data and Collection access
	  • One (1) File Share Decoy
	  • Leveraging existing pre–configured file dataset

Pilot Rollout	• Deployment and testing of landmine policy up to 25 users • Reachability and email alerting for deployed Decoys
Production Rollout	• Landmine policy deployment to up to 100 users • One Alert and optimization Session
Project Closure	• Deployment Overview and deliverables due at project completion
Deliverables	• Design Document • Operationalization Guide

Deception Advanced – Detailed Professional Services Scope	

Scope	Review customer environment and validate Deception use cases. Apply leading practices to Design and deploy advanced Deception technologies in a scalable environment. Implementation requires a Deception Advanced entitlement and is limited to deploying up to 40 decoys.
	
	*** Deployment of Zscaler Client Connector, ZIA or ZPA setup must be completed prior to engagement**
	
	Platform Setup:
	• Admin Account Access
	• Admin SSO Integration
	• Configuration of up to two (2) enrichment integrations
	• Integration with a supported SIEM/Syslog
	
	Use Cases Deployed:
	• Reconnaissance:
	  • Up to five (5) Perimeter Decoys (Threat Intelligence or Cloud Decoys)
	• Credential Access and Collection*
	  • Up to three (3) landmine policies redirecting users to Decoys
	  – Browser Lures
	  – Session Lures
	  – File set lures using local files
	  • AD Decoys in up to two (2) domains and up to seven (7) decoy objects per domain
	  • AD Kerberoasting detection through AD Decoys
	  • MITM Detection (LLMNR, NBT-NS, mDNS)
	• Advanced Landmine Features
	  • Privilege Escalation Landmine Policy
	  • Defense Evasion (configuration of up to one (1) fake security processes)
	• Lateral Movement
	  • Addition of up to three (3) remote sessions lures to landmine policy
	  • One decoy connector in one location
	  • Up to six (6) Zero Trust Network Decoys
	  • Up to six (6) Network Decoys
	• Data and Collection access
	  • Up to two (2) File Share Decoys
	  • Leveraging existing pre-configured file dataset
	  • Up to two (2) Storage Account or Private Account Storage Cloud Decoys
	• Impact and Containment
	  • Activation of Impact limitation capabilities (Ransomware detection, suspicious process and powershell execution detection.
	  • Up to three (3) containment rules
	  – ZIA Containment rule
	  – ZPA Containment rule
	  – Up to one (1) third-party containment rule

Pilot Rollout	• Deployment and testing of landmine policy up to 25 users • Reachability and email alerting for deployed Decoys
Production Rollout	• Landmine policy deployment to up to 1000 users • Up to two (2) Alert and optimization sessions
Project Closure	• Deployment Overview and deliverables due at project completion
Deliverables	• Design Document • Operationalization Guide

Deception Deployment Offerings – Engagement Details		
PS Credit Value	• Deception Essentials: **26 PS CR** • Deception Advanced: **40 PS CR**	Redemption of sufficient credits for fulfillment of service offering per unit required
Maximum # of Units recommended	1	The maximum number of units recommended for this offering to be implemented in parallel. For organizations requiring more than stated recommended units, there are alternative SKUs that may better align to your needs
Resource Allocation	One (1) Professional Services Consultant assigned	
Staffing	Resource assignment may take up to 2 weeks	
Duration	• Deception Essential: **Up to 4 weeks** • Deception Advanced: **Up to 8 weeks**	Upon the start of the project, all efforts should be completed within 12 weeks. In total the project will not exceed 3 months of engagement from Professional Services, based on the service start date.
Delivery Method	Remote	Assigned PS Resources will be remote for the duration of the engagement
Non-Technical Prerequisites	• This project covers the deployment of Zscaler Deception only. Additional Zscaler product offerings may be purchased to increase the value of the solution. Additional advisory, deployment, and consulting activities not contained in this project definition are deemed out of scope. • Zscaler is not responsible for the installation, configuration, or validation of any third-party software, tools, or utilities. • Zscaler is not responsible for executing tests within the customer environment. • The customer will provide and assume all risk when testing devices, lures, sandbox, and decoys within the environment. • The customer must provide appropriate lead resources and subject matter experts to attend technical kick-off and design sessions on the project commencement date. • The customer must provide Zscaler Professional Services with information and resources to successfully execute the project. This can include, without limitation, access, and credentials to systems, completing installation prerequisites, providing project resources, and attendance in planning, execution, or training meetings. • The customer will ensure resources are available in a timely manner to conduct tasks such as authentication system integration, client software deployment, change control, and documentation review. • The customer must ensure it has the necessary escalation and communication channels available to resolve any blockers in a timely manner, including dependencies on third parties and customer's other vendors, suppliers, and consultants. • The customer must provide a target list of Pilot users and groups to the project team within 2 weeks of the project start date.	
Technical Prerequisites	• Supported Identity Providers (IdP) must be in production use by the customer with SCIM/SAML based Admin & User Authentication and Provisioning capabilities. • Zscaler ZIA, ZPA, and Deception tenants must be provisioned, ready for administration and confirmation received from Zscaler Support. • Deception administrator access must be provided to Zscaler PS for the duration of the project. • ZIA, ZPA, and Deception tenant administrator access must be provided to Zscaler PS for the duration of the project. • Zscaler Client Connector 4.1 or later must be deployed within the customer environment prior to the start of the Deception project. • Customer must identify and provide a list of the critical applications and infrastructure to protect. • Customer must provide a group of users to deploy landmine policies • Identify Workstations with Windows 10 or Mac OSX operating systems. • Zscaler will assist the customer with identifying required Network/Firewall Access Control and Zscaler Client Connector process and access control lists on user machines • The customer will identify User/Groups for security policy definitions. • Directory groups and attributes must align with identified use cases. If authentication frameworks do not align with use cases, new groups will be created.	

Deception Deployment Offerings – Engagement Details (Cont.)	
Project Expectations	• Delivery of Zscaler licenses/subscription is outside, separate, and independent from the scope of the project and the services rendered hereunder, therefore resolution of any Zscaler licensing concerns will not affect, delay, or alter the completion or acceptance of this project. • Unexpected product behaviors will be managed separately through Zscaler Support. Support cases unrelated to the deliverables of this engagement or those dependent on Customer environment changes will not affect, delay, or alter the completion or acceptance of this project. • Upon the commencement of efforts hereunder, the Customer will have current, valid subscription licenses to all required third party software applications, necessary or appropriate for the configuration and implementation services contemplated by this service description document, including, but not limited to the Zscaler product suite. • Any product features or capabilities desired by the customer, but not available in the related software will be addressed separately and independently from the services rendered hereunder, through an Enhancement Request (ER). ERs will be managed separately and communicated between the Customer and the Zscaler Sales team, and do not affect, delay, or alter the completion or acceptance of this project. • The customer will identify and provide user groups, critical target URLs and collaboration applications for which security policies will be applied as required for the project. • The customer will provide the appropriate functional and technical resources to support Zscaler in the work effort outlined in this document. • Customer functional and technical management resources are responsible for coordinating and driving the decision-making process within the customer's organization. Delays in the decision-making processes may result in incomplete deliverables. • All materials will be provided in the English language unless otherwise specified. • It is assumed that the project will be delivered by Zscaler in a contiguous fashion. Both Parties (Customer and Zscaler) maintain joint responsibility for maintaining this time. • Should any additional services be required or requested beyond those noted to address the scope outlined in this service description, Zscaler will collaborate with the Customer to mutually agree upon and define such services as part of an additional SOW. • Base Professional Service deployment package has already been delivered previously, or is part of the same order and requires ZIA and ZPA for containment purposes • ZCC configuration has been completed and successfully tested
Project Constraints	• Zscaler will not be responsible for or be liable for any work completed by the customer. • Zscaler Professional Services will not work on any third-party or non-Zscaler devices, services, or software. • Zscaler Professional Services resources do not provide break-fix support or support case management. For incident resolution the customer agrees to contact Technical Support at their expense provided that an existing contract for Technical Support services is not maintained by the customer. • Zscaler does not honor any warranties expressed or implied by scripts or documentation provided as a result of this project. • Any exceptions to scope must be presented to Zscaler Professional Services Leadership for approval. • This Project covers the deployment of only Zscaler licensed solutions. Additional product offerings may be purchased as add-ons, otherwise additional professional services not contained in this Project are deemed out of scope. • Zscaler is not responsible for impacts to schedule caused by customer internal processes.
Disclaimer:	Zscaler Deployment and Professional Services Disclaimer