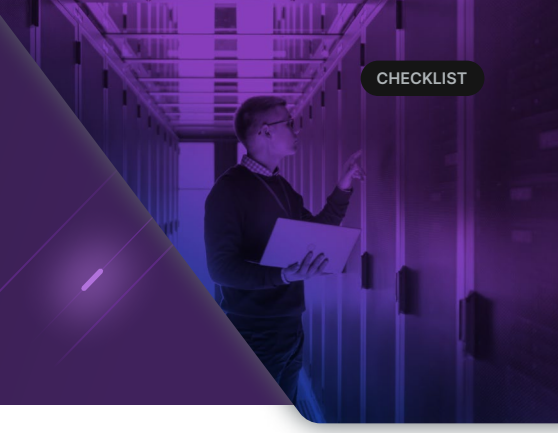
BISHOPFOX

CHECKLIST

Evaluating Offensive Security Solutions

The Top 50 Questions to Ask



To ensure your security investments offer complete visibility into your attack surface and uncover critical risks at scale, we've compiled questions to help you evaluate solutions. We focus on six key areas: attack surface discovery, exposure identification, triage, validation, remediation, and outputs.

Attack Surface Discovery	
Coverage	What assets are in scope of the discovery process?
	What focus (external, internal, 3rd party, etc.) does the provider take in the discovery process?
	How does the provider account for new, unknown, and ephemeral assets?
Method	What approach is used to identify assets across the attack surface?
	Does the process leverage automated, human, or a combined process for discovery? ◯ Automated ◯ Human ◯ Combined
	How does the provider ensure the process isn't disruptive?
Frequency	What is the cadence of the attack surface discovery process?
	How does the cadence align with different categories of assets?

Validation	To what degree are components of the attack surface being validated?
	Are validation processes automated, human driven, or a mix? ◯ Automated ◯ Human ◯ Mix
	Does the provider involve the client in the discovery and validation process and to what extent?

Exposure Identification	
Categories	What types of exposures can be identified across attack surface assets?
	What processes are used to discover exposures and are they disruptive?
Context	How does the provider keep pace with emerging threats?
	How are newly discovered exposures implemented into the identification process?
	What is the time frame from new exposure identification to implementation?
Criticality	How does the provider determine which exposures are critical?
	How does the provider consider the unique attributes of the client when determining criticality?
Frequency	What is the frequency of exposure identification discovery?
	How does the frequency pertain to different categories of exposures?

Triage

Automation	How are automated processes being utilized to enable delivery at scale?
	What are the underlying automated processes and what are their objectives?
False Positives	How is the provider reducing or eliminating false positives?
	How is the provider ensuring they are not missing true positives?
	Is the provider accomplishing this through automation, human analysis, or a combination? ◯ Automated ◯ Human ◯ Combination
Deduplication	How is the provider reducing data redundancy that could affect service quality?
Prioritization	How are exposures being prioritized for validation?
	How are the unique attributes of the client considered for prioritization?
	How are triaged leads delivered for validation?

Validation	
Method	What approach is used to validate that exposures can be exploited?
	Does the process leverage automated, human, or a combined process for validation? ◯ Automated ◯ Human ◯ Combination
	How does the provider ensure their processes are aligned to real-world attack scenarios?
Frequency	What is the cadence of the validation process?
	Is the cadence of validation process different for various types of exposures?
Extent	How is the potential business impact of the exposure determined?
	To what degree are exposures validated?
	How does the provider ensure the process isn't destructive or disruptive?
Tools and Skills	What processes and frameworks are utilized to conduct exploitation and post-exploitation activities?
	What level of expertise do the validators have in emulating real-world attacks?
	What tools and processes are utilized in the validation process?

Remediation	
Prioritization	How are validated exposures prioritized for remediation?
	Do prioritization processes consider the unique attributes of our environment? ◯ Yes ◯ No
Guidance	To what degree is remediation guidance provided for validated exposures?
	Is guidance customized for unique situations and our needs? ◯ Yes ◯ No
	Are we able to request additional guidance as needed? ◯ Yes ◯ No
Collaboration	To what degree does the provider collaborate with our client's security team?
	What limitations exist across time, access, and expertise?
	Does the collaboration team have direct knowledge of our environment and discovered exposures? ◯ Yes ◯ No
Revalidation	Does the provider validate that remediation actions were successful? ◯ Yes ◯ No
	What limitations are put on revalidation in relation to time, frequency, and extent?

Outputs	
Insights	How can we access information related to our attack surface, exposures, and findings?
	Are there limitations on the data available? ◯ Yes ◯ No (If Yes, please describe.)
Posture	How does the end-to-end service inform the improvement of the overall security posture?

About Bishop Fox

Bishop Fox is the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments. We've worked with more than 25% of the Fortune 100, eight of the top 10 tech companies, and hundreds of other organizations to improve their security. Our Cosmos platform was named Best Emerging Technology in the 2021 SC Media Awards, and our offerings are consistently ranked as "world-class" in customer experience surveys. We're an active participant in the security community and have published more than 15 open-source tools and 50 security advisories in the last five years. Learn more at **bishopfox.com** or follow us on Twitter.

Are you ready to start "defending forward"? Get in touch with our offensive security experts today to explore solutions that meet your unique business needs.

Explore Cosmos **Get Started**

8240 S. Kyrene Rd. • Tempe, AZ 85284
480.621.8967
hello@bishopfox.com • bishopfox.com