ExtraHop

PROFESSIONAL SERVICES

Quickstarts

Reduce Time-to-Value, Increase the Return on Your ExtraHop Investment

QuickStarts services accelerate value and platform adoption of ExtraHop through a professional services engagement.QuickStarts implement common use cases of the ExtraHop platform allowing you to greatly reduce ramp-up time and achieve desired outcomes with the aid of ExtraHop experts.

QuickStarts are predefined packages that include components such as dashboards, developed workflows, external product integrations, and configuration sets. These playbooks are then tailored to your environment. QuickStarts allow you to achieve rapid operational readiness and workflow integration to empower internal resources with enhanced ExtraHop proficiency.

Security QuickStarts

Quickly implement the most common security use cases of the ExtraHop platform. ExtraHop Professional Services bring together product plus domain expertise, extensive platform experience, and deep knowledge of customer environments to deliver solutions that empower your Security Analysts and SOC teams.

Asset Discovery and Classification

The Asset Discovery and Classification use case greatly reduces threats to your infrastructure by identifying previously unknown and unmanaged assets.

Professional services will implement the necessary configuration, integrations, and training documentation to achieve a continuous discovery program in the ExtraHop platform. Professional services will implement a technical playbook for discovering, identifying, and classifying assets on your network then moving that critical data into a management platform—such as an asset management tool. ExtraHop will perform the setup and configuration necessary to kick off the discovery process, work with you to identify critical assets and define rules for grouping critical assets, and identify potential output opportunities for the data including file-based data exports or API-based integration into an asset management platform.

Optimized Network Threat Detection

Optimized Network Threat Detection delivers extensive platform expertise to lower the barrier to operational excellence and accelerate your adoption and value of the ExtraHop platform.

ExtraHop will rapidly operationalize your ExtraHop platform tailored to your maturity level, operating capability, and goals. Professional Services will create and tune a threat detection framework focused on reducing false positive detections, highlighting critical assets, tuning monitoring capabilities on IT and security infrastructure, and reducing possibility of false negatives. The goal of the use case engagement is to significantly reduce the ramp-up time for SOC proficiency with ExtraHop and to reduce noise in the console.

Network-Based Threat Hunting

Network-based Threat Hunting rapidly operationalizes and tailors the ExtraHop platform to identify and investigate anomalous activity and advanced threat actors in your infrastructure. Rapidly identify and remediate threats in your environment to reduce attacker dwell time and potential impact from a breach.

ExtraHop professional services will tailor key components of the ExtraHop platform for a network threat-hunting focused function. Security experts will work with you to understand workflow, network topology and infrastructure, and functional maturity to facilitate effective identification of threats in the environment.

Cyberattack Surface Reduction

Continuous Attack Surface Reduction creates a workflow and accompanying technical components in the ExtraHop platform that reduce opportunity for attackers and lower technical risk to your organization in a proactive manner.

ExtraHop will implement product and workflow components that support your vulnerability management and remediation efforts by providing real-time intelligence about legacy and vulnerable network protocols being utilized on the customer's network infrastructure. ExtraHop's unparalleled network visibility gives you insight into vulnerabile network protocols and their active usage so analysts can triage and assign for remediation. In addition, this capability gives you insights into systems and applications that utilize legacy or vulnerable protocols—giving your security teams a way of prioritizing proactive security measures, getting ahead of potential exploits and targets for threat actors.

This use case delivery includes process development and optimization, dashboard development, and customization.

NPM/APM QuickStarts

Quickly implement the most common Network Performance Monitoring ("NPM") and Application Performance Monitoring ("APM") use cases of the ExtraHop platform. ExtraHop Professional Services brings the industry's leading technology platform together with extensive network and application expertise to understand how enterprise applications function at every level—mapping, diagnosing, and troubleshooting issues before they become costly.

Application Monitoring and Troubleshooting

Application Monitoring and Troubleshooting reduces the impact from poor performance or downtime in business-critical enterprise applications.

ExtraHop Professional Services will deliver a technical engagement focused on developing dashboards for rapidly identifying and isolating application and network performance issues. This engagement provides deep packet and protocol-based insights to facilitate rapid identification of trouble spots and assist in troubleshooting and issue resolution. ExtraHop will develop and build out dashboards and provide technical documentation and related usecase training for your application teams to ensure you are quickly up and running, as well as self-sufficient and operationally capable at the conclusion of the engagement.

For more information, including credit values and implementation specifics, please contact your ExtraHop representative.

ExtraHop

info@extrahop.com

www.extrahop.com