InfoSec Service Offerings

Identify and reduce risk with the ExtraHop platform

ExtraHop Solutions Architecture InfoSec service offerings help you to apply the power of the ExtraHop platform and mature your security program.

Benefits

- Maximize the value from your existing ExtraHop investment
- Achieve InfoSec goals without adding extra burden on your staff
- Improve your teams' proficiency on the ExtraHop platform
- Enable the business to operate as needed while minimizing risk

Yes, I Want to Engage!

If you have questions about the InfoSec offerings or other ExtraHop Solutions Architecture services, contact your designated ExtraHop sales representative or fill out the web form at:

www.extrahop.com/contact

Put wire data to work for your InfoSec program. Whether you just want to get a handle on what's going on in your environment or need to fill a particular gap in visibility, the ExtraHop Solutions Architecture team has you covered. Choose from our targeted service offerings below.

Policy Assessment and Compliance

Authentication Monitoring

Historical and real-time data to track privileged user logins, failed login attempts, and authentication methods used by applications.

Business Process Compliance

Whitelists to monitor ingress and egress traffic. Alert on potential fraud or other policy violations.

Encryption and Certificate Analysis

Simplify audits and reporting with detailed analysis on certificate expiration, SSL cipher strength, SSL versions used, etc.

Egress Traffic Compliance

Ensure outbound traffic for specific zones and networks goes through a content-screening proxy or use approved ports, protocols, and services.

Availability

Baseline system activity to monitor and alert on availability and detect DDoS attacks in real time.

Historical Auditing

Compliance reporting for portions of PCI-DSS, HIPAA, SOX. Examples: Record access attempts to sensitive assets or track the movement of data between a PCI-compliant area and non-compliant area.

Detect Policy Violations and Respond Faster

Targeted Anomaly Detection

Examples: Whitelist users or devices allowed to access specific databases and alert on increased failed login attempts for devices that provide access to sensitive information.

Targeted Data Exfiltration Detection for 3-Tiered Application

Create logical boundaries for L7 communications (storage/database access, large data transfers), build EXA queries, and integrate with SIEM or alerting workflows.

Ransomware Detection

Triggers, dashboard, and alerts to detect ransomware activity by monitoring known file extensions, variances from a file-extension whitelist, WRITE activity thresholds, and other observed data.

Targeted Vulnerability Detection

Find Shellshock, Heartbleed, HTTP.sys, Turla, and others based on observed behavior on the network, not signatures or logs.

IP Blacklist

Dashboards and alerts for monitoring when known bad IPs attempt to access your network.

Integrate with Security Infrastructure

SIEM Integration

Stream real-time, observed events and metrics to SIEM platforms for correlation with log data.

Custom Integration

Pull data into ExtraHop or stream data out to other systems for alerting, automated workflows, dashboards, reporting, and more.

Precision PCAP for Policy Violations

Triggers to gather the forensic evidence needed to fulfill Chain of Custody requirements.

Custom Engagements

In addition to the service offerings listed above, our Solutions Architects are also available for custom engagements, such as detecting brute-force attacks, integrating with next-generation firewalls, and assisting with incident response and forensic investigation using the ExtraHop platform.

> “We can now answer questions like, ‘Why are non-Accolade IPs trying to access the Admin page?’ or ‘Why are non-US IPs trying to login when all of our customers are in the US? Not only does ExtraHop allow us to see and alert on that activity as it happens, we have the data we need to drill down to the source, get the answer, and protect our assets.”
>
> Mike Sheward
> Principal Security Architect, Accolade