imperva

Service Description: SKU# DSTL-MGS-10

Security Analyst Services for Online Fraud Prevention (OFP)

Managing Sophisticated Automated Threats

Bot operators present unique and crippling challenges for businesses. Security and development teams often lack the expertise and know-how to protect their applications against the automated threat landscape, where mistakes mean lost revenue and brand damage, and complex tooling comes with steep learning curves. Behind the front lines, business stakeholders require deeper levels of technical and analytical insight, to understand how bot operators affect their applications and know when attacks happen on their most critical services. Imperva Security Analyst Services are designed to provide this ever present vigilance where it matters most, along with best practices and ongoing guidance for managing the Imperva Online Fraud Prevention solution suite consisting of Advanced Bot Protection, Account Takeover Protection and Client-Side Protection **(In-Scope Products)**. Imperva security analysts provide dedicated operational support structured around phases of the attack lifecycle.

Attack Readiness

Imperva's Security Analyst Services work collaboratively with your team and can provide autonomous management of your Imperva Advanced Bot Protection environment and operational setup. This includes the creation of custom signatures, building enforcement policies, and auditing configurations for areas of improvement.

Security Analyst Services customers receive exclusive access to our full OFP reporting package that highlights security posture, maturity score, strengths, threats with actionable insights, custom security rules for protection and in-depth traffic analysis.

- **Best Practices:** The Best Practices Monthly Report provides a maturity score of your OFP environment, calculated from quantified SAS best practices.
- **Know Where You Stand:** The Threat Mitigation Monthly Analysis Report highlights top OWASP Automated Threats (OAT) as well as other exploits in your environment for the last 30 days and provides recommendations including customised security rules and conditions.
- **Track What's Happening:** The Monthly Traffic Analysis Report provides in-depth analysis of traffic hitting your environment. It explores statistical and aggregate measurements of a multitude of parameters related to your traffic.

HIGHLIGHTS

- **Advanced Reports & Dashboards**
  Advanced reports provide monthly insights into security posture, best practices, and top OWASP threats to your assets.
- **OFP Reviews**
  Ongoing recurring review of OFP settings & configuration includingmonthly traffic analysis, adaptingyour security setup to defend against evolving malicious actors.
- **Proactive Monitoring**
  Proactive Monitoring provides notifications of surges in suspicious traffic on your critical assets followed by an investigation by security analysts. Regular health checks ensure traffic is flowing smoothlyand your servers are up and running.
- **Web Application Security Advisory**
  Imperva Security Analysts can examine your web application security to provide advice about how to harden your defences against abusive traffic beyond just automated attacks from bot operators.

Attack Response

When sophisticated bots are targeting your application, Imperva security analysts are ready on demand to dive into traffic, assess anomalous signatures, and apply mitigation controls to stop advanced actors. Advanced Bot Protection has machine learning capabilities that our analysts leverage to implement the accurate Machine learning models. These mitigation models or signatures are measured and vetted to comprehensively target and hold off malicious activity while avoiding false positives against your legitimate user base.

Custom Attack Alerting: Get real-time peace of mind as our algorithms and analysts monitor and investigate surges in suspicious and anomalous traffic patterns of your critical scoped paths.*

Traffic Healthchecks: We proactively monitor the flow of traffic and highly suspicious traffic across all your assets and alert you when traffic drops abruptly or surges with malicious activity.

** Endpoints or critical scoped paths should be identified and communicated by customers to SAS for enrollment in attack alerting.*

Attack Review

Imperva security analysts can supply ad-hoc incident and traffic analysis reports related to bot activity, for distribution to security and business units as well as your executive leadership. Bringing the expertise of Security Analyst Services into the equation allows your teams to focus on the mission critical projects that matter most for growing your business.

SAS also provides a guided approach to custom reports and dashboards creation based on your requirements and unique use-cases to monitor trends.

Premium Support SLAs

Security Analyst Services entitles you to Imperva's Premium Support SLAs for the In-Scope Products. Security Analyst Services customers get the combined benefits of access to the global Security Analyst team for all deliverables available under the Security Analyst Services program, plus 24×7 access to the Imperva Support team for any critical or time-sensitive inquiries. Tickets may be routed **to or from the Premium Technical Support team depending on nature and priority as submitted.**

First Response SLA Comparison

Support Delivery	Standard Support	Premium Support
Critical Impact	< 2 hrs	< 30 min
Major Impact	< 4 hrs	< 1 hr
Low Impact	< 1 Business Day	< 8 hrs

* Critical Impact situation = loss of service

Duration; Assumptions and Exclusions

Delivery of this service will not exceed a total of **120 hours of effort delivered as up to 10 hours per month over a 12-month period**. Unused hours from any month shall not carry over to the next month and will be deemed forfeited. No credit or refund will be due, including in connection with any unused hours. The Services will be performed remotely.

Service Terms

This description of services constitutes the Statement of Work for the Security Analyst Services described in this document. This offering is governed by the terms and conditions of the Imperva Professional Services Agreement which can be found at: https://www.imperva.com/legal/imperva_professional_services_agreement/, except to the extent the customer has a mutually signed contract in effect with Imperva or Incapsula that covers these services (the "Terms"). All capitalized terms used in this service description, but not otherwise defined, will have the meaning assigned to them in the Terms. In the event of a conflict between this service description and the Terms, this service description shall take precedence.

Payment and Validity

This offering is fixed price, inclusive of expenses, and willbe billed upon receipt of an acceptable purchase order or order form. Acceptance of Services occurs upon Imperva's performance of the Services. Acceptance of deliverables, if any, occurs upon delivery. This offering is non-cancellable and non-refundable.