Privia SECURITY

Defensive as a Service

Professional Defensive Security Services

"Complementary Strength for Operations Centers!"

The information contained in this document pertains to the Defensive Services performed by Privia Security Information Technology and Consultancy Services Inc. and is of a **general** nature. All information in this document is publicly available.

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

“Complementary element for Security Operations Centers to rapidly detect security vulnerabilities and respond to incidents.”

Our Professional Defensive Services (Defensive as a Service) constitute a comprehensive offering designed to help organizations strengthen their cybersecurity infrastructures and enhance their defensive capabilities against potential threats. By securing SOC (Security Operations Center) infrastructures, these services ensure that cyber threats are detected and addressed promptly. Our Professional Defensive Services consolidate all security operations, enabling organizations to continuously assess and improve their cybersecurity posture.

Services such as SOC maturation, threat intelligence integration, EDR, SIEM and SOAR management cover every component of an organization’s defense system. Organizations can achieve proactive protection by analyzing potential threats and can mature their incident management processes. Another key feature of this service is the integration of threat intelligence into the enterprise framework. Data obtained from global threat intelligence networks are analyzed and made applicable to the organization’s specific needs. Integrating threat intelligence accelerates decision-making processes, enabling faster response to attacks.

Defensive as a Service also provides SIEM optimization, ensuring that security data are analyzed regularly and meaningfully. SIEM systems help security teams identify real-time threats and, based on historical data, even predict future threats. By protecting organizations’ electronic/digital assets, Defensive as a Service aims to make security operations more efficient. Our service detects vulnerabilities, responds to threats in real time and minimizes risks, providing organizations with sustainable, long-term protection against cyberattacks.

Service Components

L1-L2 and L3 Level Analysis Service

This process ensures that threats detected in the Security Operations Center (SOC) are analyzed at different levels of expertise. L1 covers basic security monitoring and rapid response; L2 involves more detailed threat investigation and resolution of complex incidents; L3 offers advanced forensic analysis and root-cause investigations, providing strategic solutions against sophisticated attacks.

L1 Level Analysis Service

The L1 level analysis service forms the first stage of the cybersecurity monitoring process, enabling the quick detection of incidents and preliminary analysis. L1 Analysts are responsible for evaluating basic cybersecurity events and escalating them to the next level (L2) when necessary. By examining low-risk incidents and filtering out false positives, they direct more complex cases to higher-level analyses.

L2 Level Analysis Service

The L2 level analysis service deepens the analytic process for security events that require a more detailed examination. An L2 analyst assesses incidents forwarded from L1 in depth, performing risk analyses and initiating response procedures when necessary. L2 analysts investigate the root causes of incidents to develop permanent solutions for recurring threats. They also undertake tasks such as analyzing more complex attacks and identifying the sources of those threats.

L3 Level Analysis Service

The L3 level analysis service represents the highest tier of security analysis, encompassing advanced investigations and root-cause examinations. L3 analysts evaluate sophisticated attack scenarios and offer strategic solutions against advanced threats. The L3 analysis focuses on using forensic analysis and threat intelligence to examine attackers' methods and motivations in detail.

Product and Technology Operation (MDR)

Product and Technology Operation encompasses the management and operation of various security products that support an organization's cybersecurity infrastructure. By ensuring that security operations run sustainably and continuously, it provides constant protection against threats. Following an MDR (Managed Detection and Response) approach, this service ensures the effective operation of security solutions such as Tenable, Picus, ThreatMon, Trellix (McAfee and FireEye), Wazuh, Palo Alto, DarkTrace and Burp Suite. The service helps cybersecurity teams derive maximum benefit from these technologies.

SOC Maturation

SOC maturation aims to strengthen the Security Operations Center (SOC) infrastructure and develop its capabilities according to international standards. Throughout this process, the capacity of SOC teams, the effectiveness of technological tools and operational workflows are evaluated to identify areas in need of improvement. SOC Maturation Service enhances the organization's ability to respond quickly and accurately to security incidents. A SOC structure customized to the organization's needs improves the success of attack detection and response processes.

SIEM Management and Optimization

SIEM management is used to monitor and analyze security events in order to detect threats. Effective operation and management of the SIEM system are critical for corporate security. Through SIEM optimization, data can be analyzed more accurately and false positives (F/P) are minimized. A well-managed SIEM system enables real-time analysis, allowing swift detection and response to threats.

Threat Intelligence Integration

Threat intelligence integration enables the analysis of internal and external threats and incorporates that intelligence into security operations. Data collected from global threat networks are processed to develop a defense strategy specific to the organization. Threat intelligence helps SOC teams understand the nature of attacks and contributes to taking preventive measures.

Network Security Monitoring

Network security monitoring allows organizations to detect threats in their network infrastructure in real time. Using real-time monitoring tools, intrusion attempts can be identified and addressed immediately. Network security management facilitates regular traffic analysis and the identification of attack patterns. This process is particularly effective for early detection of threats such as DDoS attacks and data breaches. A robust network security infrastructure reduces vulnerabilities and enhances the organization's overall security.

Incident Response

Incident response is planned to provide a swift and effective reaction in cases of attacks or security breaches. The service includes analyzing the security incident's impact and executing response procedures promptly to minimize damage. Incident response may also involve post-incident forensic analysis. During this process, security teams analyze threats and minimize risks to the organization.

Training and Awareness

Comprehensive training programs are organized to enhance the skills of security teams and raise awareness throughout the organization. Employees are educated on potential threats, making them better prepared for security incidents. Awareness training aims to reduce human-originated security risks, such as social engineering attacks. Training programs also keep security teams updated on the latest threats and attack methods.

SIEM Local Maintenance Support Consulting

SIEM Local Maintenance Support Consulting provides the necessary maintenance and support services to ensure SIEM systems operate continuously and perform optimally. On-site support addresses any issues that may arise with SIEM products, ensuring security operations continue without interruption. During maintenance, system updates, patches and performance optimizations are carried out to keep the SIEM running at maximum efficiency.

SIEM Maturation Consulting

SIEM Maturation Consulting aims to optimize SIEM solutions for more effective use within the Security Operations Center (SOC). During the maturation process, the SIEM system's data collection, analysis and correlation capabilities are evaluated. Customized correlation rules and security alerts are developed to meet the organization's specific needs.

Correlation Rule Effectiveness Testing

Correlation Rule Effectiveness Testing is a service that verifies the functionality of correlation policies defined in the SIEM system. Periodic audits are conducted to ensure these policies generate correct alerts. By correcting faulty or misconfigured policies, threat detection improves and false positives (F/P) are reduced. Correlation rule effectiveness is regularly monitored and improvements are made as needed. These audits help ensure security events are detected promptly and accurately.

Log Collection Architecture and Log Maturation Consulting

Log Collection Architecture and Log Maturation Consulting provide the necessary configuration to effectively monitor corporate security infrastructure. The service aims to ensure accurate log collection from servers, networks, applications and other electronic devices for forensic purposes—facilitating the illumination of any incident. During the maturation process, log data are optimized to reduce storage costs and accelerate analysis processes. This shortens the time security teams need to analyze incidents and enables faster threat response.

Patch Analysis

Patch Analysis is a security process that identifies the update and patch requirements for an organization's digital assets. Analyses are conducted periodically to ensure that systems are protected with the latest security patches. Missing or faulty patches can lead to vulnerabilities, so correct patches are applied based on analysis results. Patch analysis helps prevent threats and cyberattacks by ensuring that security measures are up to date.

Asset Visibility Analysis

Asset Visibility Analysis is a security process that maps all of an organization's digital assets to increase their visibility. Through these analyses, security teams gain a clearer understanding of which assets need protection and the threats they face. Improving asset visibility reduces the likelihood that attackers can exploit vulnerabilities. The analysis also evaluates whether assets operate in compliance with security policies.

Segmentation Analysis

Segmentation Analysis is a security process that verifies whether security segments in the network infrastructure are correctly configured. Analyses of different network segments' access restrictions help minimize security risks. Ensuring that each segment is isolated according to its security requirements reduces the attack surface. Segmentation is one of the most important processes in maintaining network security because it prevents threats from spreading across segments. This service also optimizes segmentation policies in line with the current threat environment.

Remote Access Analysis

Remote Access Analysis evaluates an organization's external access points to ensure a secure access infrastructure. These analyses inspect the security of VPNs, remote desktop connections and other external access methods. Particularly given the increased demand for remote work since COVID-19, Remote Access Analysis is crucial for preventing cybersecurity risks. Insecure access points are identified and unauthorized entry attempts are detected. Additionally, recommendations are provided for updating remote access policies and implementing strong authentication methods.

Authentication Infrastructure Analysis

Authentication Infrastructure Analysis evaluates an organization's user authentication mechanisms and assesses their effectiveness. The analyses measure the efficacy of security measures such as multi-factor authentication (MFA) and robust password policies. A strong authentication infrastructure controls user access and prevents unauthorized entry. During the analysis, any deficiencies in authentication systems are identified and aligned with current security policies.

Enterprise SOME Consulting

Enterprise SOME (Security Operations and Monitoring) Consulting provides professional advisory services to help organizations respond swiftly and effectively to cyber incidents. SOME develops a strategic plan for responding to security breaches and ensures immediate action. Tailored to the organization's internal dynamics, SOME Consulting matures incident response capabilities and trains teams on relevant topics. The service includes the creation of incident response procedures and communication plans. By enhancing SOME team effectiveness, it also establishes policies for post-incident remediation.

Regulation-Compliant Data Destruction Consulting

Regulation-Compliant Data Destruction Consulting ensures that organizations destroy sensitive data in compliance with national and international regulations. By developing data destruction policies that meet regulatory requirements, this service guarantees data security. Secure disposal of sensitive information minimizes the risk of data breaches. During the destruction process, reliable software and physical destruction methods are used to render data irrecoverable. After data destruction, destruction reports are provided to document and record the completion of the process.

Vulnerability Management Consulting

Vulnerability Management Consulting offers a comprehensive solution for identifying and remediating security vulnerabilities in an organization's electronic assets. Throughout this service, security vulnerabilities are regularly detected, eliminating weak points that attackers might exploit. Security scans and analyses ensure continuous monitoring of the organization's risk posture. Necessary patches and updates are applied to remediate identified vulnerabilities. During the vulnerability management process, threats are prioritized, ensuring that critical vulnerabilities are addressed first.

Cybersecurity Policy and Procedure Development Consulting

Cybersecurity Policy and Procedure Development Consulting helps organizations create customized security policies and procedures, thereby strengthening their overall security strategy. Structuring security processes systematically and ensuring organizational compliance is crucial for robust cybersecurity. Developing policies and procedures encourages all employees to adhere to security standards. The security policies developed cover areas such as access control, data protection and incident response. Regular updates to procedures ensure alignment with the evolving threat landscape. Security policies are also essential for raising employee awareness and fostering a culture of security within the organization.

FAQ

How does MDR service provide an advantage in security operations?

MDR (Managed Detection and Response) is a comprehensive security service that enables the detection of threats and rapid response. Our MDR Service, integrated with systems such as SIEM, SOAR, DLP, EPP, sandboxed EDR and NDR, plays a vital role in the instant identification and prevention of security incidents. Continuous threat monitoring, immediate response and the operation of security technologies within the organization are among MDR Service's greatest advantages. The MDR Service provides uninterrupted protection during security operations and with systems updated by threat intelligence, vulnerabilities are quickly remediated. MDR Service helps reduce the workload on security teams, enabling them to focus on critical incidents.

What steps are followed during the incident response process and what are the benefits?

Incident response is a service that begins with the detection of incidents and is completed through analysis, isolation, eradication and remediation steps. In the first step, threats are detected using SIEM and other security technologies. During the analysis phase, our cybersecurity experts conduct a detailed examination of the threat's source and potential impact. Then, in the isolation and eradication phases, malicious elements are removed from the systems. Throughout the response process, security teams work collaboratively to prevent the threat from spreading. The remediation phase includes the necessary adjustments to prevent similar incidents from occurring in the future.

How does SIEM optimization play a role in security operations?

SIEM optimization accelerates the analysis of security events, enabling effective response to threats. By optimizing SIEM technologies to improve system performance and reduce false positives (F/P), the productivity of security teams is enhanced. Regular and meaningful analysis of data helps in the quicker identification of security gaps. Optimizations enable retrospective threat analysis and prediction of future threats. Keeping SIEM updated and well-integrated is critically important for the sustainability of security operations.

What is the contribution of threat intelligence integration to security operations?

Threat intelligence integration plays a critical role in the effective management of security operations. By integrating up-to-date threat information into security technologies, it provides a robust defense against threats. SOC teams can analyze the origins and methods of threats more effectively with integrated intelligence data. As a result, the organization gains protection against external threats while also anticipating internal risks. This process accelerates decision-making, enabling faster response to incidents. Evaluations based on threat intelligence data enable the

organization to develop long-term security strategies. Faster decision-making helps close security gaps more rapidly.

How does the SOC maturation process work and what benefits does it offer organizations?

The SOC maturation process includes improvements that make the Security Operations Center more effective against threats. By increasing incident detection and response capabilities, the SOC's efficiency is enhanced. The maturation process is managed according to frameworks such as SOC-CMM or NIST to ensure compliance with international standards. Throughout the process, SOC team skills are developed and their rapid-response capabilities are strengthened. Detection times decrease and response times shorten. A robust SOC structure establishes a stronger defense against attacks and ensures greater preparedness. Over the long term, the SOC maturation process optimizes the organization's security posture. Continuous improvement and evaluation enhance the SOC's capabilities.

How do L1, L2 and L3 level analysis services differ and what does each level contribute?

L1, L2 and L3 level analysis services are designed to investigate threats at different depths of detail. L1 level analysis provides basic monitoring and rapid response services, assessing low-risk incidents and escalating them to L2 when necessary. L2 level analysts conduct a detailed analysis of incidents, perform root-cause investigations and develop solutions for recurring threats. L3 level analysis delivers strategic solutions for complex attacks and conducts forensic analysis. Advanced analysis identifies the origin of attacks and tracks attackers' footprints, helping to close security gaps and address root problems.

What advantages do MDR solutions offer in product and technology operation processes?

MDR solutions increase threat-detection and response capabilities in product and technology operation processes. By automating the management of security products through MDR, threat detection becomes more effective. MDR Service prevents threats from escalating and raises the organization's overall security level. Additionally, MDR continuously improves security policies with up-to-date threat intelligence. By reducing the workload of security teams, it increases operational efficiency. Rapid detection and response to threats minimize security risks.

Why is SIEM and SOAR integration important?

Integrating SIEM and SOAR is crucial for analyzing security events and activating automated response mechanisms. While SIEM analyzes events, SOAR triggers automated response procedures based on predefined rules. Integration enables faster and more effective responses to security incidents. It reduces the workload on security teams, allowing them to focus on critical events. SOAR's automated processes enable immediate incident response and help reduce the number of false positives (F/P). Together, SIEM and SOAR solutions contribute to rapid threat detection and neutralization.

How does post-incident forensic analysis contribute to security operations?

Post-incident forensic analysis is a comprehensive investigation process that identifies the source and traces the attacker's path. By determining where security vulnerabilities originated, it assesses the full scope of the incident. Forensic analysis uncovers methods that attackers used to exploit vulnerabilities. The findings collected during this phase help guide preventive measures against future attacks. Additionally, the reports generated from forensic analysis contribute to the maturation of the organization's security policies.

How does Network Detection and Response (NDR) work and what benefits does it provide?

Network Detection and Response (NDR) aims to detect anomalous activities by analyzing an organization's network traffic in real time. It enables early detection and response to threats such as data exfiltration, backdoors and DDoS attacks. Real-time monitoring allows security teams to identify and respond to threats immediately. Continuous traffic analysis is used to uncover attack techniques and security vulnerabilities. With these monitoring tools, security teams can manage potential threats more effectively. Regular network security monitoring ensures that threats are kept in check and prevents them from spreading to other network segments.

Your Trusted Partner in Cybersecurity

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

Global and Local Cybersecurity Solutions

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East and the Americas. Our specialized teams in Offensive, Defensive and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions and military organizations, it bridges the gap between training and real-world readiness.

A Secure Future Through Advanced Technology

With R&D centers located in Istanbul, Ankara, London and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "**Privacy For You**" we bring a fresh, innovative perspective to security and privacy—ensuring that our clients' digital futures are secure.

Privia
SECURITY