Privia SECURITY

Investigation and Incident Response

Professional Defensive Security Services

"Immediate Response to Cyber Incidents!"

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

“Instant response to cyber incidents ensures threats are quickly contained and security is restored to normal.”

Incident Response Service is a comprehensive security offering designed to enable organizations to respond rapidly to cyberattacks and security breaches they may face. Given the rapidly evolving nature of cyber threats, effective incident response plays a critical role in preserving business continuity. During a security breach, the most appropriate response strategy is determined and executed based on the scope of the incident.

In the incident response process, detecting and effectively isolating threats are among the top priorities. The security team defines the steps to follow based on identified threats and takes swift action. The technologies employed in this process allow real-time monitoring of threats and accelerate response times. To minimize the impact of an incident, isolation procedures are implemented.

Internal threats may arise from employee errors or malicious insiders, while external threats originate from cybercriminals or rival organizations. The incident response process is designed with a comprehensive perspective to address all these threat sources. After a security breach, forensic analyses are conducted to examine in detail the cause of the incident and the source of the attack. The forensic analysis process helps the security team trace the attacker’s footprints and take preventive steps against similar threats.

Incident Response Service also supports the organization’s compliance with legal requirements. In the event of a security breach, it ensures collaboration with regulatory bodies and provides necessary reporting.

Service Components

Incident Detection and Analysis

Incident detection encompasses the rapid identification and analysis of cyber threats. Using monitoring tools, the security team detects suspicious activities and potential threats. During threat detection, the attack's origins, targeted systems and the type of attack are analyzed in detail. Through these analyses, the scope and impact of the attack are determined and appropriate response steps are promptly initiated. This process helps the organization better understand the root cause of the incident and prepare for future threats.

Threat Isolation and Control

Threat isolation involves separating threats to prevent security breaches from spreading across the organization. Isolation measures allow the security team to quickly take control of compromised systems. By isolating affected systems, the spread of the attack is halted, protecting the integrity of other systems. The tools used support rapid and effective monitoring and isolation. The threat control process provides a safe environment in which the organization can manage security incidents.

Incident Response Process

The incident response process encompasses our cybersecurity team's rapid reaction to threats to bring the incident under control. During a security breach, the most suitable response steps are identified and immediately implemented. These steps are customized according to the type of incident and the organization's specific needs. Incident response helps minimize the damage caused by the attack. Our cybersecurity teams ensure that, by containing threats, the organization's business continuity is maintained.

Forensic Analysis and Trace Tracking

The forensic analysis process includes detailed examinations conducted after an incident to determine the reasons behind a security breach and trace the attacker's path. Our cybersecurity teams track the attacker's footprints to analyze which systems were affected and how. The data obtained is also used to evaluate the effectiveness of the incident response. Critical insights into the attacker's methods help guide necessary improvements to the security infrastructure. The findings serve as guidance for updating security policies.

Communication and Reporting

Effective communication during the incident response process ensures information flows smoothly during a crisis, supporting proper management of the incident. Timely and accurate communication with internal and external stakeholders plays a critical role in incident management. In the event of a security breach, the management, security teams and, if necessary, regulatory bodies are informed. Detailed reports on the incident's impact and the measures taken are prepared. These reports contribute both to evaluating the response process and to ensuring legal compliance. Communication protocols facilitate the organization's ability to act quickly during a crisis.

Preventive Measures

Following the incident response process, improvements are implemented to close security gaps and prevent similar incidents in the future. The organization uses data obtained during the post-incident phase to make necessary enhancements to its security infrastructure. Additionally, tools and protocols used in threat monitoring and analysis are updated. Security policies and procedures are regularly reviewed and adjusted in line with the evolving global threat landscape.

FAQ

Why is Incident Response Service important?

Incident Response Service enables an organization to respond quickly and effectively to cyber threats, thereby minimizing data leaks, data loss and operational disruptions. When security breaches are detected and contained immediately, the adverse effects of an attack can be mitigated. In today's environment of escalating cyber threats, incident response has become a critical component of an organization's cybersecurity posture. A rapid and effective incident response process ensures that security weaknesses are addressed and preventive measures are taken to avoid repeat attacks.

How are cyber incidents responded to?

Responding to cyber incidents begins with detection, followed by a rapid analysis phase. First, the source of the security breach and the scope of the attack are determined and efforts are made to neutralize the threat. While isolating and analyzing the threat, potential spread risks are assessed and contained. Security teams take corrective actions to minimize the damage caused by the attack. Afterward, a detailed review and reporting process is initiated to analyze the incident's impact on systems and applications.

What are the first steps to take during a cyberattack?

During a cyberattack, the first priority is to detect and isolate the attack as quickly as possible. The source and scope of the attack should be identified and affected systems must be isolated immediately to prevent further spread. From the outset, detailed log records must be maintained to document all information related to the attack. Once the full extent of the damage is understood, remediation efforts commence. Relevant departments and management are informed and the incident is reported.

What stages make up the incident response process?

The incident response process consists of threat detection, initial response, analysis, isolation, recovery and improvement stages. In the first stage, abnormal activities in systems are monitored and potential threats are identified swiftly. In the second stage, the threat is isolated to prevent spread, separating it from other systems. Next, a thorough analysis determines the source of the incident and how it occurred. Following analysis, systems are restored and security vulnerabilities are addressed.

Who is notified in the event of a security breach?

In the event of a security breach, the organization's senior management, relevant security teams and necessary regulatory bodies are informed. First, the security team assesses the incident's impact and provides detailed information to senior management. Coordination is established with other relevant departments within the organization and a continuous information flow is maintained regarding the incident. During this process, regulatory bodies are provided with necessary reports to ensure legal compliance.

How should Incident Response Service be tested and updated?

Incident Response Service should be tested regularly through drills and simulations so that teams' reactions in a crisis scenario can be measured. Tests should be based on realistic scenarios to observe security teams' coordination. After each test, any gaps in the process should be reviewed and areas requiring improvement identified. To update the service, new threats and attack techniques should be examined and necessary safeguards implemented. Additionally, new security protocols and technologies must be integrated into the service. Any shortcomings and vulnerabilities discovered during drills should be remedied and response procedures updated accordingly.

What technologies are used during incident response?

Technologies used in incident response include SIEM (Security Information and Event Management) systems, EDR (Endpoint Detection and Response), SOAR (Security Orchestration, Automation and Response) and threat intelligence tools. SIEM analyzes events in real time and helps detect security breaches quickly. EDR solutions monitor endpoints for abnormal activities and provide automated responses to threats. SOAR platforms automate incident response workflows, enabling faster reactions to security events.

What reporting processes are applied during incident response?

During incident response, a detailed reporting process is implemented to analyze the attack's impact and damages. The report details the source, type, duration and propagation method of the attack. It identifies which systems were compromised and which data were affected. Based on all collected information, evidence and findings, security weaknesses are analyzed and preventive measures are determined. Reporting is critical for guiding post-incident remediation efforts and for taking preventive measures against future threats. Furthermore, the reports serve as informative documents for regulatory bodies and senior management.

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