Privia SECURITY

Incident Response Service

Professional Forensic Services

"Rapid Response in Cyber Crises!

The information contained in this document pertains to the Forensic 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

"Organizations intervening promptly against cyber threats is the most critical step in eliminating those threats. With rapid response, the impact of threats is swiftly reduced, preventing attacks such as data leaks and breaches."

The Incident Response Service has been designed to provide a fast and effective response to any cybersecurity breaches an organization may face. Various techniques are used to stop the spread of attacks and restore systems to normal operation. For every type of cyber incident, our expert teams activate the appropriate response and action plans.

The Incident Response Service offers solutions for critical events such as ransomware attacks, data leaks, DDoS attacks and malware detection. With real-time intervention capabilities, it minimizes the impact of attacks and ensures uninterrupted business operations. To safeguard the organization's assets, audit trails, system logs and user activities are analyzed. Based on these analyses, the source of any cyberattack is identified and the relevant teams are informed. During the incident response process, coordination is maintained with both internal and external stakeholders. Actions are taken in compliance with legal regulations and all necessary notifications are made according to applicable laws. Additionally, reporting processes are managed to ensure compliance with national and international regulations.

Through the training and awareness programs provided under this service, organizations' resilience against threats is strengthened. Incident response teams are continuously trained -supported by simulations- to adapt to emerging threats. Technical teams are reinforced to face potential future threats more effectively.

Components of the Service

Incident Monitoring/Investigation

Enables detection of anomalies in systems and provides early warnings. Continuous monitoring of log records allows threats to be noticed at an early stage. Suspicious activities occurring on the system are reported to the incident response team. Robust monitoring tools make it difficult for attackers to operate without leaving traces.

Cyber Incident Response Team

Our Cyber Response Team is available 24/7 to take rapid action against cyber threats. Each team member specializes in specific types of incidents. During active incidents, teams work in a coordinated manner to bring the crisis under control as quickly as possible. They also manage the post-incident recovery process, facilitating the restoration of systems to their prior state.

Forensic (Digital Forensics) Analyses

This is the process of collecting and analyzing digital evidence after an incident. The integrity and legal validity of the data are preserved while tracing attacker's footprints. Forensic experts conduct detailed examinations to determine how the attack occurred. The collected evidence is documented in reports for use in legal proceedings.

Crisis Management and Communication Plan

Crisis management plans are implemented to ensure effective communication with stakeholders during incidents. Internal and external communication processes are kept under control. When necessary, the management and/or legal team issues public statements. Strategic actions are taken to protect the organization's reputation.

Post-Incident Reporting

At the end of the incident response process, detailed reports are prepared on the cyberattacks that occurred. The report includes the type of attack, its impacts and the actions taken. These reports are submitted for evaluation at both technical and management levels. With improvement recommendations, measures are adopted to guard against similar threats in the future.

Cybersecurity Drills

Cybersecurity drills are comprehensive exercises organized to ensure that organizations are prepared for cyberattack scenarios. The drills include attack scenarios similar to real-world threats and test how organizational teams will respond in a crisis. Conducted at various levels, these drills involve everyone from executives to technical staff in a unified training process. Drills allow both technical vulnerabilities and process deficiencies to be identified. By repeating these exercises regularly, the cybersecurity team's continuous development is supported and they remain prepared against current global threats.

FAQ

What is an Incident Response Plan (IRP)?

An Incident Response Plan outlines the procedures an organization will follow when responding to security incidents such as cyberattacks or data breaches. The plan ensures that threats are quickly identified, their impact is contained and normal operations can resume. The IRP aims to prepare the organization for threats. Within the plan, roles and responsibilities are defined, communication protocols are established and technical remediation steps are specified.

Why is the incident response process important?

A timely and coordinated response to cyber incidents minimizes the damage caused by attacks. Without an effective response plan, data loss and operational disruptions can occur. By implementing an IRP, businesses can protect sensitive information and ensure legal compliance.

Who should be involved in developing an incident response plan?

Representatives from various departments—such as cybersecurity, the Cyber Incident Response Team (SOME), data protection officers, IT, legal, human resources and public relations—should participate in preparing the plan. Support from upper management also provides strategic contributions to the incident response process and helps ensure smooth execution of procedures.

What are the steps of the incident response process?

The main steps are preparation, identification, containment, eradication, recovery and post-incident review. During the preparation phase, response plans are developed. Identification determines the source of the attack. Containment focuses on preventing the threat from spreading. Eradication removes the threat from the environment. Recovery restores systems to their prior state and carries out post-incident remediation efforts. Post-incident review analyzes and documents lessons learned.

What is the role of the Cyber Incident Response Team (SOME) in responding to cyber incidents?

The Cyber Incident Response Team analyzes threats during a crisis and implements response strategies. SOME teams both respond to predefined incident types and provide solutions against emerging global threats. Through forensic investigations, they collect legal evidence to support any potential legal proceedings.

Which systems and tools are used in incident response?

Tools such as Intrusion Detection/Prevention Systems (IDS/IPS), firewalls, SIEM, DLP, Endpoint Protection Platforms (EPP), Endpoint Detection and Response (EDR) and SOAR software are critically important. Log management systems are also used to monitor and report incidents. These tools enable early visibility of threats and allow for an effective response.

Why are cybersecurity drills important for organizations?

Drills simulate real attack scenarios to ensure that teams are prepared. They test the effectiveness of security systems and reveal any deficiencies. Regular drills support team development and improve incident response processes.

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