F12 Managed Detection and Response (MDR)

Service Overview

F12.net™

Introduction

In today's fast-evolving threat landscape, organizations require proactive defense measures to safeguard their systems. F12.net's Managed Detection and Response (MDR) service delivers 24/7 monitoring, detection, and incident response through a collaborative partnership with Blackpoint Cyber. By combining F12's expertise with Blackpoint's cutting-edge technology, we ensure your organization stays protected against emerging threats.

F12's Security Operations Team

The F12 Security Operations Team leads incident management and response, leveraging a wealth of expertise and industry-recognized certifications, including:

- Certified Information Systems Security Professionals (CISSP)
- Certified Ethical Hackers (CEH)
- Certified Network Vulnerability Professionals (CNVP)

Our team provides expert advisory services, monitors for threats, and executes custom response playbooks tailored to your organization's unique needs.

Blackpoint's Security Operations Center (SOC)

Blackpoint's SOC provides continuous, real-time threat monitoring and response. Their specialized threat hunters use advanced detection tools to identify, analyze, and mitigate cyber threats before they escalate. This partnership ensures robust coverage, with Blackpoint's SOC escalating critical incidents to F12 for further action.

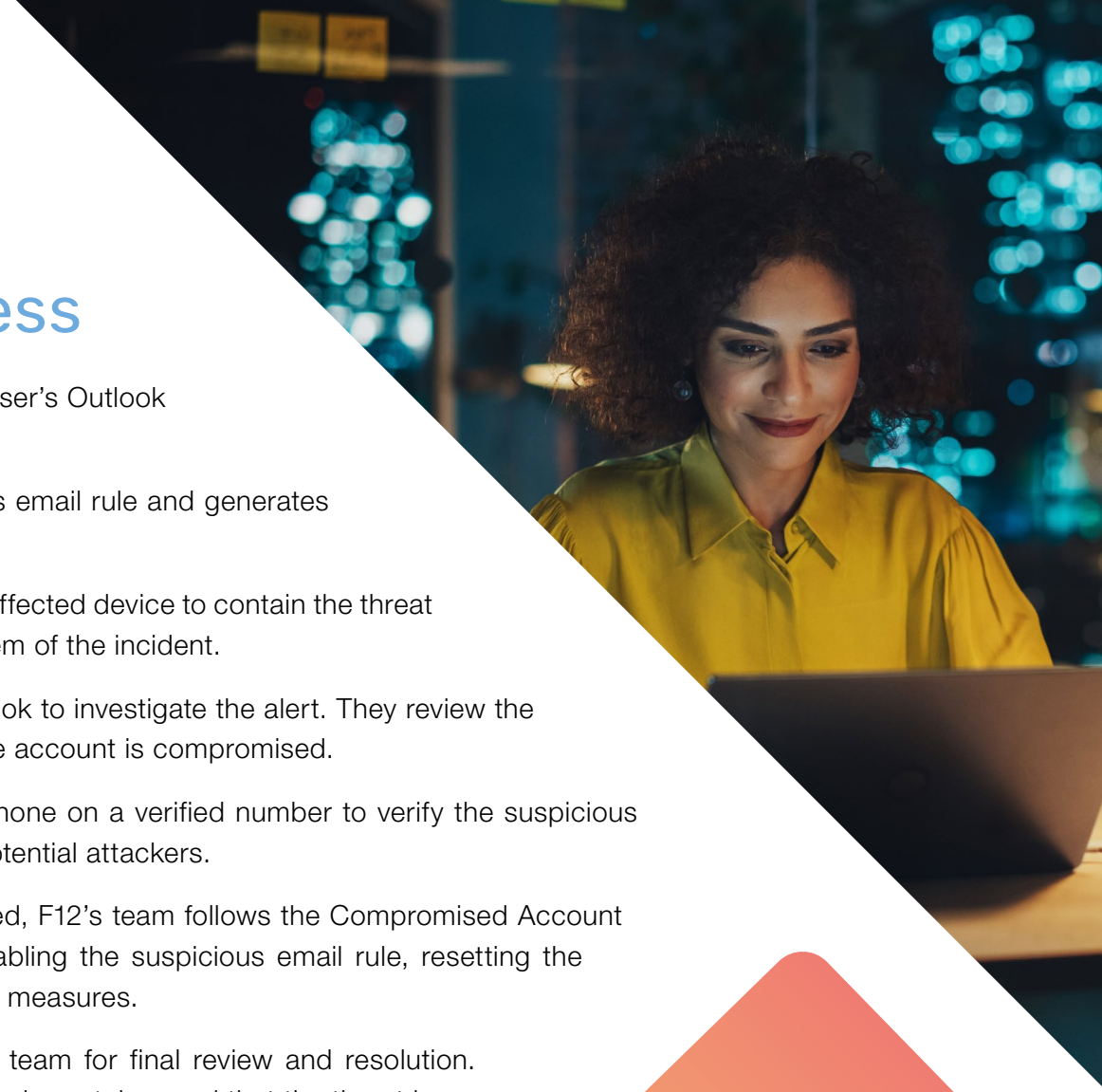
F12 MDR Alerts

1. **Detection:** Blackpoint's SOC uses advanced threat detection technologies to identify potential threats. When a threat is detected, an alert is generated.
2. **Investigation:** Blackpoint's SOC performs initial investigations to determine the severity and potential impact of the threat. They use their expertise to analyze the threat and gather relevant information, escalating identified incidents to F12's Security Operations team for tailored incident response and further analysis. High-severity incidents are escalated to F12 by phone 24/7 for faster triage.
3. **Response:** Where possible, immediate action is taken to mitigate the threat such as isolating affected systems or removing malicious files. F12's Security Operations team initiates specific actions based on their security expertise and incident response protocols, this may include executing tailored response playbooks, working with effected users, reinstating quarantined systems, or implementing additional security measures.
4. **Communication:** F12's Security Operations team gathers details of the threat and actions taken, reaching out to ensure the client is aware of the situation and of any follow-up actions required.

Handling Escalations and Using Playbooks

F12's Security Operations Team handles incidents by following a structured process. They use customized cyber response playbooks to investigate and action cyber security incidents. These playbooks are the primary guide for incident escalation and response. F12 follows unique escalation protocols informed by client-specific nuances like executive travel, trusted contacts, and organizational policies. For example, some organization's permit anonymous file shares, shared mailboxes, or international remote access. Others do not.

F12 escalates security incidents to emergency status within minutes of discovery. Emergency incidents include ransomware, active network intrusions, suspicious data transfers, suspicious authentications, and identifiable instances of privacy violations.



Example of the Escalation Process

Let's say we detect a suspicious email rule created in a user's Outlook account. Here is how the escalation process would work:

1. **Detection:** Blackpoint's SOC identifies the suspicious email rule and generates an alert.
2. **Initial Response:** Blackpoint's SOC quarantines the affected device to contain the threat and calls F12's Security Operations Team to inform them of the incident.
3. **Investigation:** F12's team follows the Malware Playbook to investigate the alert. They review the user's email activity and sign-in logs to determine if the account is compromised.
4. **Communication:** F12's team contacts the user by phone on a verified number to verify the suspicious activity. They do not email the user to avoid alerting potential attackers.
5. **Action:** If the account is confirmed to be compromised, F12's team follows the Compromised Account template to re-secure the account. This includes disabling the suspicious email rule, resetting the user's password, and implementing additional security measures.
6. **Validation:** The incident is escalated to F12's Tier 3 team for final review and resolution. The Tier 3 team ensures that all necessary actions have been taken and that the threat is fully mitigated.

Prioritization and Remediation

F12 prioritizes security incidents based on their severity and potential impact. High-priority incidents, such as ransomware attacks or active network intrusions, are escalated immediately and handled with the utmost urgency. Lower-priority incidents are addressed promptly but may not require the same level of immediate action.

While the activities described above are included in F12's MDR service, recovery and remediation of a significant breach would involve a Security Incident Response Team (SIRT). This specialized team is called in to handle complex and severe incidents, providing in-depth analysis and remediation. It is important to note that SIRT services are a billable activity and not included in the standard F12 MDR service.

Managing and Validating MDR Services

1. **Partner Selection:** F12 carefully selects their cybersecurity partners, including Blackpoint, to ensure they provide the best protection. They validate the effectiveness of these partners using third-party testing and simulated adversarial attacks.
2. **Continuous Monitoring:** F12's Security Operations Team continuously monitors the performance of the MDR services to ensure they are effective in detecting and responding to threats.
3. **Regular Reviews:** F12 conducts regular reviews of the MDR services to identify any areas for improvement. This includes reviewing the performance of Blackpoint's SOC and service agents, making any necessary adjustments to the service.
4. **Client Communication:** F12 ensures that their clients are kept informed about the status of their security. They provide regular updates and reports on the performance of the MDR services and any incidents that have been detected and responded to.

Glossary of Common Security Incidents

- **Active Network Intrusions:** Unauthorized access to a network with the intent to cause harm, steal data, or disrupt operations. This involves an attacker actively engaging with the network to exploit vulnerabilities.
- **Anonymous File Shares:** Sharing files or folders in a manner that provides open access to anyone with the link, risking data privacy and confidentiality.
- **Authentication from an Unapproved Country:** Login attempts from countries not approved or expected for access, which may indicate a compromised account.
- **Authentication from New Device or IP:** Login attempts from devices or addresses not previously used by the user, which may indicate unauthorized access.
- **Impossible Travel:** Login attempts from geographically distant locations within a short time frame, suggesting that the same user could not have traveled between those locations in the given time, indicating potential account compromise.
- **Mailbox Permissions:** Access rights granted to users or applications to read, send, or manage emails in a mailbox. Misconfigured permissions can lead to unauthorized access or data breaches.
- **Privacy Violations:** Breaches of privacy laws or policies, involving unauthorized access, use, or disclosure of personal information.
- **Ransomware:** A type of malicious software designed to block access to a computer system or data until a sum of money is paid. Ransomware attacks can cause significant disruption and financial loss to organizations
- **Suspicious Authentications:** Login attempts that deviate from normal patterns, such as multiple failed attempts, logins from unusual locations, or logins at odd hours, which may suggest unauthorized access attempts.
- **Suspicious Data Transfers:** Unusual or unexpected movement of data within or outside an organization that may indicate a security breach or data exfiltration attempt.
- **Suspicious Email Rule:** Email rules created to automatically forward, delete, or move emails in a way that could indicate malicious intent, such as hiding phishing emails or exfiltrating data.
- **Unverified Application:** Applications that have not been verified or approved by the organization, which may pose security risks if they are malicious or improperly configured.

Value of F12 MDR Services

Clients receive significant value from F12's MDR services in several ways:

- **Cost Savings:** By preventing security breaches and minimizing the impact of incidents, MDR services can save clients substantial amounts of money. For example, reducing server and network downtime by over 85% can lead to annual savings of up to $400,000 for every 100 users
- **Peace of Mind:** With 24/7 real-time vigilance, clients can rest assured that their systems are continuously monitored and protected. This proactive approach to cybersecurity reduces the likelihood of successful attacks and provides clients with confidence in their security posture
- **Reduced Downtime:** Swift detection and response to threats minimize the impact on business operations. By addressing incidents quickly, MDR services help maintain business continuity and reduce the time systems are offline
- **Improved Reputation:** Investing in MDR demonstrates cybersecurity vigilance to customers, employees, insurers, and investors. Preventing a run-away breach can avoid immense and lasting damage to brand trust and confidence.

F12's partnership with Blackpoint Cyber delivers a comprehensive MDR solution tailored to the needs of your organization. Our collaborative approach ensures effective detection, investigation, and response to emerging threats, keeping your business secure in an ever-changing digital landscape.

Clients consistently report how F12's proactive communication and swift action during incidents **provide peace of mind in challenging moments.** In some cases, ongoing infiltrations were discovered and stopped immediately upon deploy of F12 MDR.

F12.net™

Contact Us

For more information or to get started, please reach out to us using the details below:

1-866-F12-8787 | www.f12.net | info@f12.net