ITogether Service Definition Document

Check Point Infinity XDR/XPR

Client Name: Francesca Finan
Date: 01/05/2024

Detailed Description

Check Point Infinity XDR (Extended Detection and Response) is a comprehensive cybersecurity platform designed to provide advanced threat detection, investigation, and response capabilities across hybrid IT environments. Here's an overview of its key components and functionalities:

1. **Unified Security Platform**: Infinity XDR integrates multiple security capabilities into a single platform, including endpoint protection, network security, cloud security, and security orchestration. This unified approach enables organizations to consolidate their security tools and streamline security operations.
2. **Advanced Threat Detection**: Infinity XDR employs advanced detection techniques, including machine learning, behavioral analysis, threat intelligence, and signature-based detection, to identify known and unknown threats across endpoints, networks, and cloud environments. It correlates security events and indicators of compromise (IOCs) to uncover sophisticated cyber attacks and malicious activities.
3. **Continuous Monitoring and Analysis**: Infinity XDR continuously monitors and analyzes security telemetry data from endpoints, network traffic, cloud workloads, and applications in real-time. It leverages AI-driven analytics to detect anomalous behavior, suspicious activities, and indicators of compromise (IOCs) that may indicate potential security threats.
4. **Automated Incident Response**: Upon detecting a security incident, Infinity XDR automates incident response processes, including containment, investigation, and remediation, to minimize the impact of cyber threats. It orchestrates response actions across endpoints, networks, and cloud environments to contain and neutralize threats before they can cause damage.
5. **Threat Hunting Capabilities**: Infinity XDR empowers security analysts to conduct proactive threat hunting activities by providing them with advanced search and query capabilities, threat intelligence feeds, and customizable playbooks. This enables them to proactively identify and mitigate hidden threats and security vulnerabilities before they are exploited by attackers.
6. **Rich Context and Visualization**: Infinity XDR enriches security alerts and incidents with contextual information, including asset information, user behavior, network traffic, and threat intelligence. It provides visualizations, timelines, and interactive dashboards to help security analysts understand the full scope of security incidents and make informed decisions.
7. **Integration and Orchestration**: Infinity XDR seamlessly integrates with existing security tools and infrastructure, including SIEM (Security Information and Event Management) systems, SOAR (Security Orchestration, Automation, and Response) platforms, threat intelligence feeds, and third-party security products. It orchestrates security workflows and response actions across heterogeneous environments to improve security operations efficiency.
8. **Scalability and Flexibility**: Infinity XDR is designed to scale to meet the evolving security needs of organizations, regardless of their size or industry. Whether deployed on-premises, in the cloud, or in hybrid environments, Infinity XDR offers scalability, flexibility, and customization options to adapt to the dynamic threat landscape.
9. **Comprehensive Threat Protection**: By combining advanced threat detection, automated incident response, threat hunting, and integration capabilities, Infinity XDR provides organizations with

comprehensive protection against a wide range of cyber threats, including malware, ransomware, phishing attacks, zero-day exploits, and insider threats.

Overall, Check Point Infinity XDR empowers organizations to enhance their cybersecurity posture, improve threat visibility, and respond to cyber threats effectively by leveraging advanced detection and response capabilities across hybrid IT environments.

Business Benefits

1. **Unified Security Platform**: Infinity XDR brings together endpoint protection, network security, cloud security, and security orchestration capabilities into a single platform. This unified approach enables organizations to manage and monitor their security posture holistically from a centralized dashboard.
2. **Advanced Threat Detection**: The platform employs advanced threat detection techniques, including machine learning, behavioral analysis, threat intelligence, and signature-based detection, to identify known and unknown threats across various endpoints, networks, and cloud environments.
3. **Continuous Monitoring**: Infinity XDR continuously monitors security telemetry data from endpoints, network traffic, cloud workloads, and applications in real-time. It correlates security events and indicators of compromise (IOCs) to detect suspicious activities and potential security threats.
4. **Automated Incident Response**: Upon detecting a security incident, Infinity XDR automates incident response processes, such as containment, investigation, and remediation, to minimize the impact of cyber threats. It orchestrates response actions across different security layers to neutralize threats quickly and efficiently.
5. **Threat Hunting Capabilities**: The platform empowers security analysts to conduct proactive threat hunting activities by providing them with advanced search and query capabilities, threat intelligence feeds, and customizable playbooks. This enables them to uncover hidden threats and security vulnerabilities before they are exploited by attackers.
6. **Rich Contextual Information**: Infinity XDR enriches security alerts and incidents with contextual information, including asset details, user behavior, network activity, and threat intelligence. This contextual information helps security analysts understand the full scope of security incidents and make informed decisions.
7. **Integration and Orchestration**: Infinity XDR seamlessly integrates with existing security tools and infrastructure, including SIEM systems, SOAR platforms, threat intelligence feeds, and third-party security products. It orchestrates security workflows and response actions across heterogeneous environments to improve security operations efficiency.
8. **Scalability and Flexibility**: The platform is designed to scale to meet the evolving security needs of organizations, regardless of their size or industry. Whether deployed on-premises, in the cloud, or in hybrid environments, Infinity XDR offers scalability, flexibility, and customization options to adapt to the dynamic threat landscape.
9. **Comprehensive Threat Protection**: By combining advanced threat detection, automated incident response, threat hunting, and integration capabilities, Infinity XDR provides organizations with comprehensive protection against a wide range of cyber threats, including malware, ransomware, phishing attacks, zero-day exploits, and insider threats.

Standard Service Components
Minimum deal size is 50 users.

Optional Service Components
Upgrade of service hours

Service Exclusions
Professional Services for setup and configuration

Standard Support Services
8x5 support, Monday to Friday 9am to 5pm

Assumptions
Any and all information will be provided by the customer to enable the full onboarding of the product without hinderance

Contact

Name	Role	Tel	Email
Tim Ripper	Account Director	0113 341 0123	tim@itogether.co.uk
Simon Richardson	Director	0113 341 0123	simon@itogether.co.uk