ITogether Service Definition Document

Check Point Infinity Events

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

Detailed Description

Check Point Infinity Events is a security platform offered by Check Point Software Technologies, a leading provider of cybersecurity solutions. This platform is designed to provide comprehensive threat visibility and protection across networks, cloud environments, and mobile devices.

Here are some key features and aspects of Check Point Infinity Events:

1. **Unified Security Management**: Check Point Infinity Events offers a unified security management interface, allowing security teams to centrally manage and monitor security policies, events, and incidents across various environments.
2. **Threat Intelligence Integration**: The platform integrates threat intelligence feeds and data from various sources to provide up-to-date information on emerging threats and vulnerabilities. This helps organizations stay ahead of evolving cyber threats.
3. **Real-Time Event Monitoring**: Check Point Infinity Events continuously monitors network traffic and system logs in real-time to detect suspicious activities and potential security incidents. It uses advanced analytics and machine learning algorithms to identify anomalies and indicators of compromise.
4. **Automated Incident Response**: In addition to detecting security incidents, the platform also offers automated incident response capabilities. It can automatically block malicious activities, isolate compromised devices, and take other predefined actions to mitigate threats in real-time.
5. **Forensic Analysis**: Check Point Infinity Events provides tools for forensic analysis and investigation of security incidents. Security teams can conduct detailed investigations to understand the scope and impact of an incident, gather evidence, and take appropriate remediation actions.
6. **Integration with Security Orchestration Platforms**: The platform can integrate with security orchestration, automation, and response (SOAR) platforms to streamline incident response workflows and automate repetitive tasks.
7. **Scalability and Flexibility**: Check Point Infinity Events is designed to scale and adapt to the evolving needs of organizations of all sizes. It can protect both on-premises and cloud-based environments and is suitable for a wide range of industries and use cases.

Overall, Check Point Infinity Events helps organizations strengthen their security posture, improve threat visibility, and respond effectively to cyber threats in today's dynamic threat landscape.

Business Benefits

Key features of Check Point Infinity Events for multi-cloud environments include:

1. **Unified Management**: The platform offers a single pane of glass management interface for managing security policies, events, and incidents across multiple cloud environments. This centralized management simplifies security administration and ensures consistent policy enforcement.
2. **Cloud-Native Security**: Check Point Infinity Events provides cloud-native security controls specifically designed to protect workloads, applications, and data in cloud environments. These controls include network security, workload protection, application security, and data loss prevention (DLP) capabilities.
3. **Integration with Cloud Platforms**: The platform integrates with major cloud platforms' native security services and APIs, allowing organizations to leverage native security features while enhancing them with additional layers of protection provided by Check Point.
4. **Compliance and Governance**: Check Point Infinity Events helps organizations maintain compliance with regulatory requirements and industry standards across multiple cloud environments. It provides tools for auditing, reporting, and enforcing compliance policies to ensure that cloud workloads meet security and regulatory standards.
5. **Scalability and Flexibility**: Check Point Infinity Events is designed to scale and adapt to the dynamic nature of multi-cloud environments. It can protect workloads deployed in public, private, and hybrid cloud infrastructures, offering flexibility to meet the evolving needs of organizations.

Overall, Check Point Infinity Events offers comprehensive security for multi-cloud environments, helping organizations secure their cloud workloads and data while maintaining visibility, control, and compliance across diverse cloud platforms.

Standard Service Components

Check Point Infinity Events is a comprehensive security platform designed to provide visibility into security events, monitor network traffic, detect threats, and facilitate incident response. While the specific components may vary depending on the deployment and configuration, here are some standard service components commonly associated with Check Point Infinity Events:

1. **Event Management**: The core component responsible for collecting, aggregating, and managing security events generated by various sources such as network devices, servers, endpoints, and security appliances.
2. **Real-time Monitoring**: A monitoring module that continuously analyzes network traffic and system logs in real-time to detect suspicious activities, anomalies, and security incidents.

3. **Threat Detection**: A threat detection engine that leverages advanced analytics, machine learning, and threat intelligence feeds to identify indicators of compromise (IOCs), malware, intrusions, and other security threats.
4. **Incident Response**: Tools and capabilities for orchestrating and executing incident response workflows, including automated response actions, alert notifications, and remediation tasks to mitigate security incidents.
5. **Forensic Analysis**: Features for conducting forensic analysis and investigation of security incidents, including the ability to search, correlate, and analyze historical security event data to understand the scope and impact of an incident.
6. **Policy Management**: A centralized management interface for defining, implementing, and enforcing security policies across the organization, including firewall rules, access controls, intrusion prevention rules, and threat prevention settings.
7. **Integration Interfaces**: APIs and integration points to enable seamless integration with other security systems, SIEM (Security Information and Event Management) platforms, threat intelligence feeds, and third-party tools for enhanced security orchestration and automation.
8. **Reporting and Analytics**: Reporting tools and dashboards for generating security reports, visualizing security event data, and analyzing trends, patterns, and metrics related to security incidents, compliance, and operational performance.
9. **Compliance and Governance**: Features and capabilities to support regulatory compliance and governance requirements, including predefined compliance templates, audit trails, and controls for data protection and privacy regulations.
10. **Scalability and High Availability**: Scalability features such as distributed architecture, load balancing, clustering, and failover mechanisms to ensure the platform can handle increasing workloads and maintain availability in large-scale deployments.

These service components collectively enable organizations to strengthen their security posture, improve threat visibility, and respond effectively to cyber threats in today's dynamic threat landscape. Depending on the specific deployment requirements and use cases, organizations can customize and configure Check Point Infinity Events to meet their unique security needs.

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