CHARITH (21BCE1872)

What is SOC?

The function of the security operation center (SOC) is to monitor, prevent, detect, investigate, and respond to cyber threats around the clock. SOC teams monitor and protect the organization’s assets, including intellectual property, personnel data, business systems, and brand integrity. The SOC team implements the organization’s overall cybersecurity strategy and acts as the central point of collaboration in coordinated efforts to monitor, assess, and defend against cyberattacks.

What does a SOC do?

Although the staff size of SOC teams varies depending on the size of the organization and the industry, most have roughly the same roles and responsibilities. A SOC is a centralized function within an organization that employs people, processes, and technology to continuously monitor and improve an organization’s security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

- **Prevention and detection:** When it comes to cybersecurity, prevention will always be more effective than reaction. Rather than responding to threats as they happen, a SOC works to monitor the network around the clock. By doing so, the SOC team can detect malicious activities and prevent them before they can cause any damage.

  When the SOC analysts see something suspicious, they gather as much information as they can for a deeper investigation.
- **Investigation:** During the investigation stage, the SOC analyst analyzes the suspicious activity to determine the nature of a threat and the extent to which it has penetrated the infrastructure. The security analyst views the organization’s network and operations from the

perspective of an attacker, looking for key indicators and areas of exposure before they are exploited.

The analyst identifies and performs a triage on the various types of security incidents by understanding how attacks unfold, and how to respond before they get out of hand effectively. The SOC analyst combines information about the organization’s network with the latest global threat intelligence that includes specifics on attacker tools, techniques, and trends to perform an effective triage.

- **Response:** After the investigation, the SOC team then coordinates a response to remediate the issue. As soon as an incident is confirmed, the SOC acts as a first responder, performing actions that such as isolating endpoints, terminating harmful processes, preventing them from executing, deleting files, and more.
  In the aftermath of an incident, the SOC works to restore systems and recover any lost or compromised data. This may include wiping and restarting endpoints, reconfiguring systems, or, in the case of ransomware attacks, deploying viable backups to circumvent the ransomware. When successful, this step will return the network to the state it was in before the incident.

SOC Challenges

SOC teams must constantly stay one-step ahead of attackers. In recent years, this has become more and more difficult. The following are the top three challenges that every SOC team faces:

- **Shortage of cybersecurity skills:** Based on a survey by Dimensional Research, 53% of SOCs are having difficulties hiring skilled personnel. This means that many SOC teams are understaffed and lack the advanced skills necessary to identify and respond to threats in a timely and effective manner. The (ISC)² Workforce Study estimated that the cybersecurity workforce needs to grow by 145% to close skills gap and better defend organizations worldwide.
- **Too many alerts:** As organizations add new tools for threat detection, the volume of security alerts grows continually. With security teams

today already inundated with work, the overwhelming number of threat alerts can cause threat fatigue. In addition, many of these alerts do not provide sufficient intelligence, context to investigate, or are false positives. False positives not only drain time and resources, but can also distract teams from real incidents.

- **Operational Overhead:** Many organizations use an assortment of disconnected security tools. This means that security personnel must translate security alerts and policies between environments, leading to costly, complex, and inefficient security operations.

Addressing SOC Challenges

For many Security Operations Center (SOC) teams, finding malicious activity inside the network is like finding a needle in a haystack. They are often forced to piece together information from multiple monitoring solutions and navigate through tens of thousands of daily alerts. The results: critical attacks are missed until it's too late.

Designed to address SOC challenges, Check Point Horizon enables security teams to expose, investigate, and shut down attacks faster, and with 99.9% precision. Easily deployed as a unified cloud-based platform, it increases security operations efficiency and ROI.

Horizon SOC goes beyond XDR with AI-based incident analysis augmented by the world's most powerful threat intelligence and extended threat visibility, both inside and outside your enterprise. By providing easy access to exclusive threat intelligence and hunting tools it enables faster and more in-depth investigations.

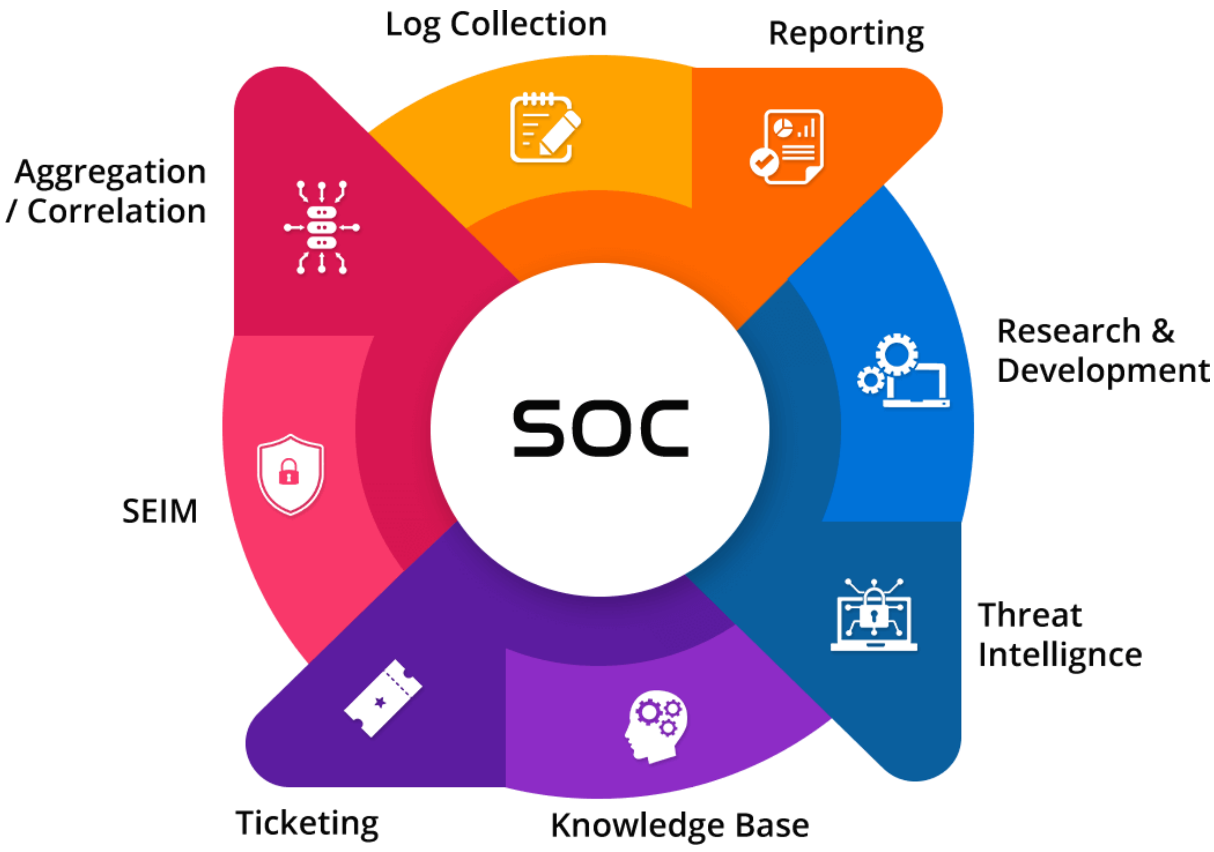
Check Point Horizon helps enterprises protect their networks by delivering:

Unrivaled accuracy to quickly detect and shut down real attacks

Rapid incident Investigations

Zero-friction deployment

CHARITH (21BCE1872)



SIEM

Security information and event management (SIEM) is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. SIEM systems collect log data from a wide range of sources across an organization's entire network, including firewalls, intrusion detection systems, servers, and applications. This data is then analyzed in real time to identify suspicious activity and potential security threats.

SIEM systems typically use a variety of techniques to detect security threats, including:

- Correlation: SIEM systems correlate events from different sources to identify patterns and anomalies that may indicate a security threat. For example, a SIEM system might correlate a failed login attempt from a foreign country with a successful login attempt from the same country a few minutes later. This could indicate that an attacker is attempting to gain access to the network using a brute-force attack.
- Rule-based alerting: SIEM systems can be configured to generate alerts based on predefined rules. For example, a SIEM system might be configured to generate an alert if it detects 10 failed login attempts from the same IP address within a 15-minute period.
- Machine learning: SIEM systems can also use machine learning to identify suspicious activity and potential security threats. For example, a SIEM system might be trained to identify patterns in network traffic that are associated with known malware infections.

Once a security threat is detected, a SIEM system can take a variety of actions, including:

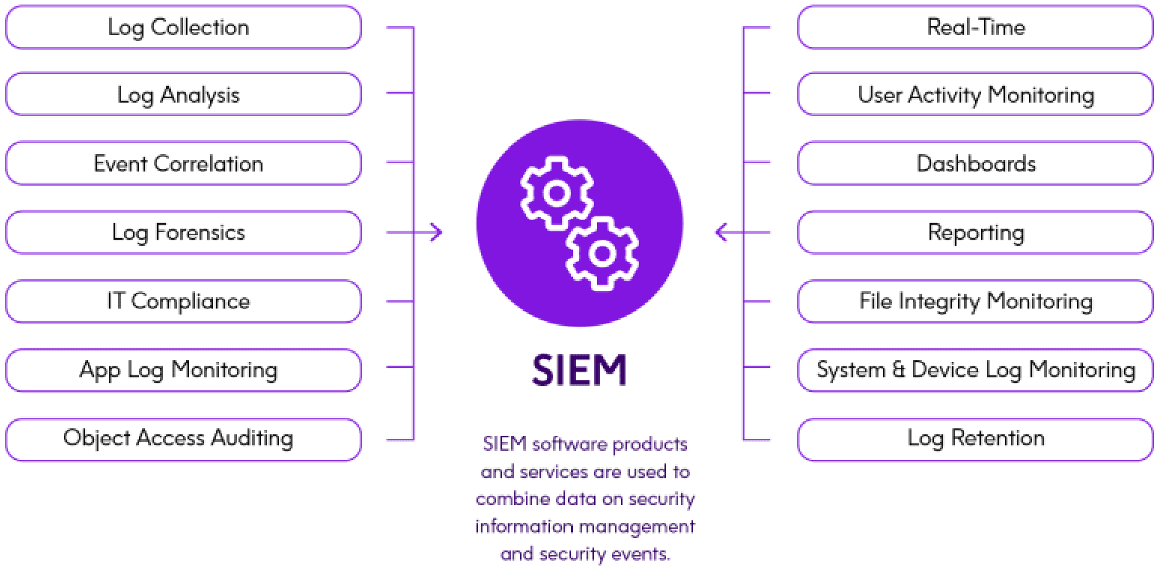
- Generate an alert: SIEM systems typically generate alerts that are sent to security analysts for further investigation.
- Block suspicious activity: SIEM systems can be configured to block suspicious activity, such as traffic from a known malicious IP address.
- Quarantine infected systems: SIEM systems can also be configured to quarantine infected systems to prevent them from spreading malware to other systems on the network.

SIEM systems play an important role in helping organizations to protect themselves from a wide range of security threats. By providing real-time visibility into network activity and automating security tasks, SIEM systems can help organizations to detect and respond to security threats more quickly and effectively.

Here are some of the key benefits of using a SIEM system:

- Improved security posture: SIEM systems can help organizations to improve their security posture by providing real-time visibility into network activity and identifying potential security threats before they can cause damage.
- Reduced response time: SIEM systems can help organizations to reduce their response time to security incidents by automating security tasks and providing security analysts with the information they need to quickly investigate and resolve incidents.
- Improved compliance: SIEM systems can help organizations to comply with a variety of industry regulations and standards that require organizations to monitor their networks for security threats.

SIEM systems are an essential tool for any organization that is serious about protecting its data and systems from security threats.



Qrader

IBM Security QRadar is a security information and event management (SIEM) platform that provides organizations with a comprehensive view of their security posture. QRadar collects and analyzes data from a variety of sources, including network and security devices, logs, and threat intelligence feeds. It uses this data to identify and prioritize security threats, and to automate responses.

CHARITH (21BCE1872)

QRadar is a modular platform, which means that organizations can choose the components that best meet their needs. The core components of QRadar include:

- Log management: QRadar collects and stores logs from a variety of sources, including network devices, security devices, and applications.
- Security event correlation: QRadar analyzes logs and other data to identify security threats. QRadar uses a variety of techniques to correlate events, including rule-based correlation, anomaly detection, and machine learning.
- Asset management: QRadar automatically discovers and profiles assets on the network. This information is used to enrich security events and to provide context for investigations.
- Incident response: QRadar provides a variety of tools to help organizations respond to security incidents. These tools include incident management tools, playbooks, and integrations with other security products.

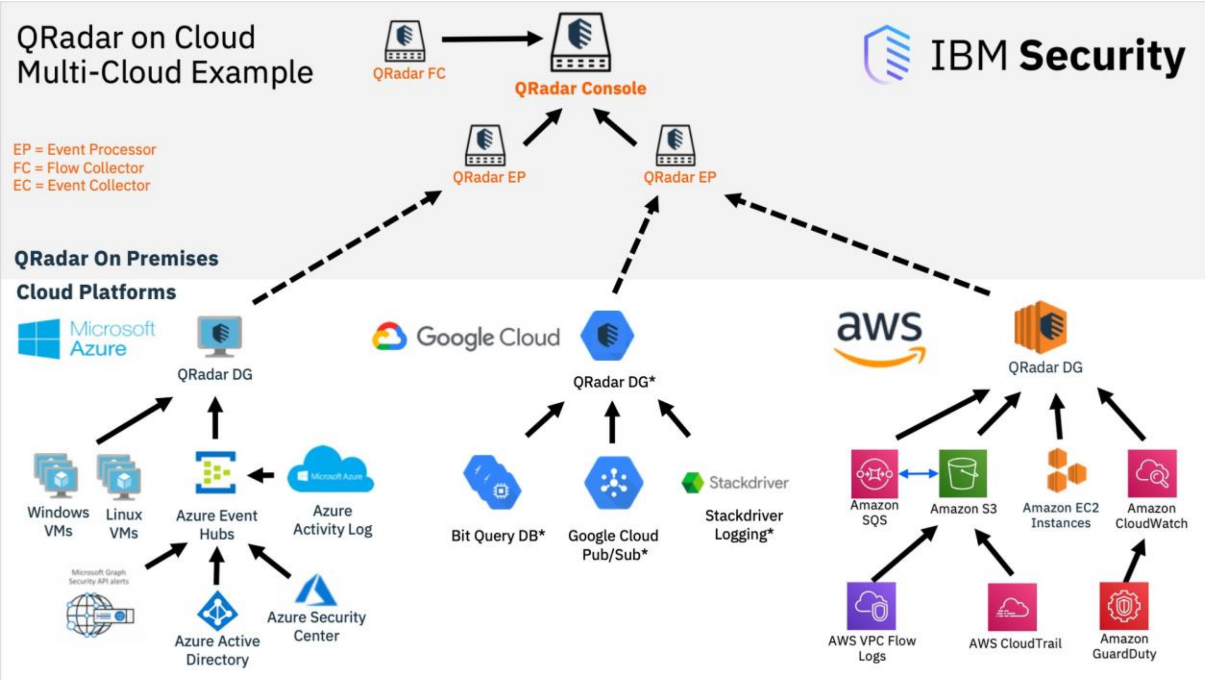
QRadar is a powerful SIEM platform that can help organizations of all sizes to improve their security posture. It is used by a wide range of organizations, including financial institutions, government agencies, and healthcare providers.

Here are some of the key benefits of using QRadar:

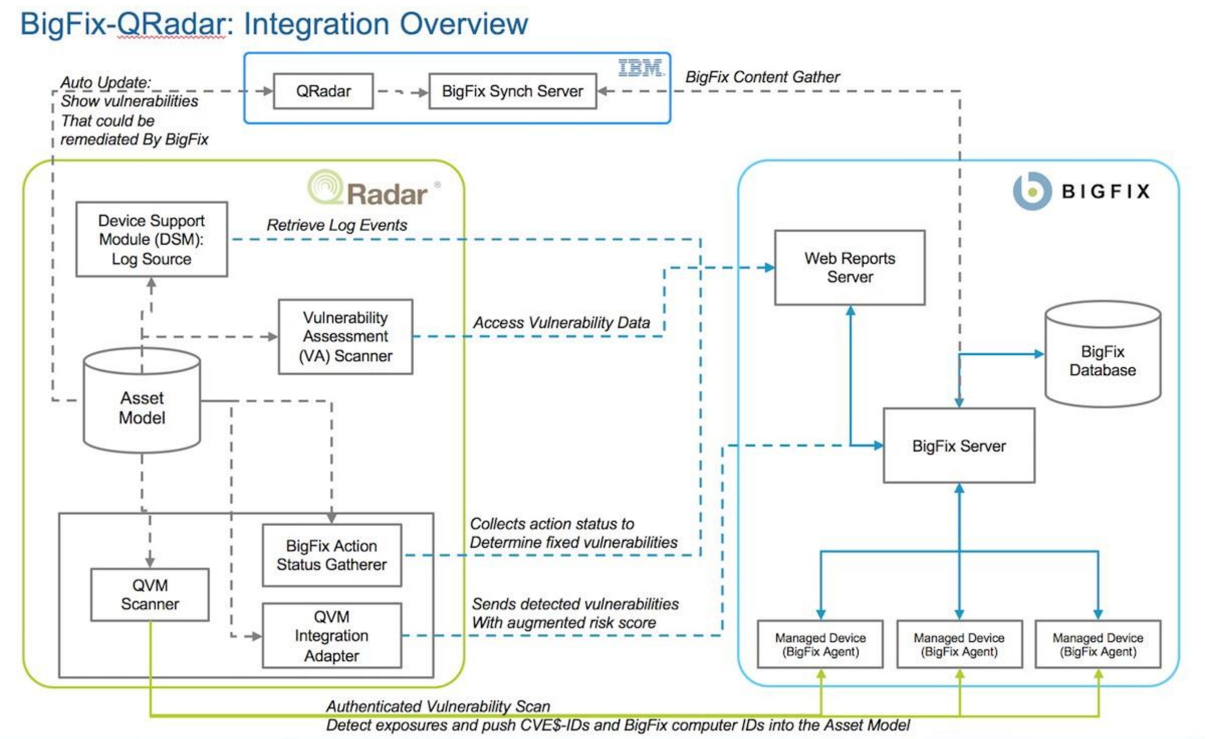
- Improved security visibility: QRadar provides a single view of security events from across the organization. This gives security analysts a better understanding of the organization's security posture and helps them to identify threats more quickly.
- Reduced risk: QRadar can help organizations to reduce their risk of security breaches by identifying and prioritizing threats early on. QRadar can also automate responses to threats, which can help to reduce the damage caused by a breach.
- Improved compliance: QRadar can help organizations to comply with a variety of security regulations. QRadar provides a variety of reports that can be used to demonstrate compliance.

CHARITH (21BCE1872)

QRadar is a complex platform, but it is also a very powerful one. It can help organizations of all sizes to improve their security posture and to reduce their risk of security breaches.



CHARITH (21BCE1872)



BigFix-QRadar: Integration Overview

IBM
QRadar
BigFix Synch Server
Auto Update:
Show vulnerabilities
That could be
remediated By BigFix
BigFix Content Gather
QRadar
Device Support Module (DSM): Log Source
Retrieve Log Events
Vulnerability Assessment (VA) Scanner
Access Vulnerability Data
Asset Model
BigFix Action Status Gatherer
Collects action status to
Determine fixed vulnerabilities
QVM Scanner
QVM Integration Adapter
Sends detected vulnerabilities
With augmented risk score
BIGFIX
Web Reports Server
BigFix Database
BigFix Server
Managed Device (BigFix Agent)
Managed Device (BigFix Agent)
Managed Device (BigFix Agent)
Authenticated Vulnerability Scan
Detect exposures and push CVE$-IDs and BigFix computer IDs into the Asset Model