Futurism Eagle Eye powered by IBM QRadar

Futurism

Advanced Threat Protection Package

Get ahead of advanced and sophisticated threats with our advanced threat detection package powered by IBM Security.

Did you know?

On an average, it takes 280 days to detect and contain a breach with more than 30% of organizations discovering a breach two or more years after the incident!

Our Advanced Threat Protection Package works round-the-clock to prevent, monitor, detect, analyze and respond to security incidents. Built on the fundamental pillars of people, process and technology, the advanced security service pack is aimed at fortifying your security and IT posture. Our Advanced Threat Protection package uses IBM QRadar and intelligence feeds from X-Force to provide up-to-the- minute protection from novel threats including new strands of Ransomware.

Advanced Threat Detection (QRadar SIEM)

- Real-time threat intelligence & event monitoring (powered by IBM X-Force)
- IBM QRadar incident forensics (Network scans to identify anomalous communications)
- Detecting abnormal connection behavior (volume/time/ geographic), Rogue services and systems, Malware/Worm propagation, etc.
- PowerShell Attack (Process base lining to detect anomalous/ unusual/malicious processes)
- DNS Attack (detect outbound requests to malicious sites, identify DNS trends and certificates)

Insider Threat Detection

- Privileged user monitoring
  - Preconfigured alerts and notifications for DoS attacks and hijacked accounts
  - Behavioral analytics
- Trusted Host and Entity Compromise
  - Determine risk score of an entity (e.g. disgruntled employee) using historical normal behavior and machine learning algorithms
  - Track Network Activity (Lateral movement, abnormal resource access, Browser exploits, Malware activity, suspicious file downloads, Command and control activity, beaconing, etc.)
  - Remote Access Activity (Credential theft, password sharing)
  - Identity (credential violations, account takeover, privilege escalations)
  - DNS (Tunneling, Exfiltration)
  - File Integrity Monitoring
- Abnormal Authentication Behavior
  - Real-time alerts for brute force attacks, password guessing, and misconfigured/unauthorized applications and access
  - Customize rules to detect unusual activity in your network
  - Alerts and offenses for:
    - Unauthorized access/apps
    - Multiple password attempts• Encrypt exfiltrated data
    - Same user name in multiple locations
    - Actions at unusual times
    - Credentials/VPN sharing

Cloud Discovery

- Track abnormal cloud usage and workload
- Centralized security monitoring and behavior analysis
- Cloud network visualization in real-time
- Container security
- Detect multi-vector attacks
- Identify misconfigurations
- Advanced user monitoring capabilities

Data Exfiltration

- Monitor network traffic for large data transfer
- Visibility into all network communications to avoid blind spots
- Encrypt exfiltrated data
- Alerts for:
  - Abnormal data volume transfer to external domain
  - Exfiltration – files in sensitive directories
  - Large outbound transfer
  - Emails containing sensitive files
  - Suspicious access followed by data exfiltration

Phishing Attacks

- Identify malicious code/content – including those hidden in data transmissions, SSL certificate violations, protocol obfuscation, file tags, and suspicious network flows
- Detect and extract suspicious e-mail subject lines, content an attachments
- X-Force Integration to identify Malware Family
- Record application activities, capture artifacts, and identify assets, applications and users participating in network communications

Protecting Critical Assets/Data

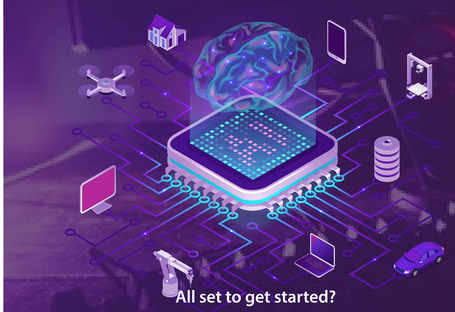
- Gain visibility and understanding of network topology and attack paths
- Protect critical assets such as financial, EMR, EHR, COVID databases, etc.
- Monitor log and source for unauthorized attempts
- Simulate attacks and impacted assets
- Prioritize remediation of assets most vulnerable to outsider and insider threats

Endpoint Detection & Response (EDR) integration

- Prioritize high-value investigation and response activities
- React faster, coordinate better, and respond smarter
- Automated escalation of offenses from IBM QRadar
- Bi-directional synchronization of notes and closed cases to ensure data integrity.

Automatic Investigation with IBM Watson AI

- Automate security analysis
- Tap into unstructured data (including security websites, blogs, and research papers, among others) and correlate with local security incidents
- Analyze large amounts of data in shorter periods of time
- Identify more attack patterns using a combination of IBM QRadar and Watson AI
- Concentrate on higher priority threats
- Determine additional suspicious behavior



All set to get started?

Schedule a FREE consultation with one of our security experts now to help us customize a security service offering that fits your business needs.

+1-512-422-4868

www.futurismtechnologies.com