DEFENDER COMPANION

DefCom

Defender Companion

Your SOC, taking faster security decisions with better quality security context!

DefCom continuously provides actionable context for each Defender for Endpoint onboarded device by integrating data from sources like asset management solutions, IP address management solutions, Active Directory, Entra ID etc.

This information is consolidated through Defender for Endpoint Tags, creating a comprehensive contextual timeline for every device, ensuring that when an alert is triggered, analysts have a complete understanding of the device's role and criticality. This proactive approach streamlines threat identification, reduces investigation time, and strengthens overall security posture.

- No need for another console; context is consolidated into your existing EDR/SIEM solutions.
- Customizable context enrichment based on your organization's criticality definition.
- Reducing repetitive manual tasks.
- Streamlining detection use case lifecycle by leveraging contextual data for more precise rule scope and rule exception management.
- Risk-centric alert prioritization; prioritize alert investigation based on impacted entities' criticality.

Gather

Continuous gathering of contextual data by integrating with your existing tools.

- Azure Graph API
- Active Directory / Entra ID
- Asset inventory
- IP address management
- Vulnerability management

+ custom integrations

Process

Correlating gathered context data with real-time Defender for Endpoint telemetries.

- Extensive historical context enables accurate incident analysis
- Context is continuously kept up to date.
- DefCom processing capabilities can be configured to address your unique needs.

Consolidate

Defender for Endpoint Tags are added/removed based on configured logic.

- Standardized naming convention for Tags
- Seamless SIEM integration
- Fully utilize native Defender for Endpoint features, leveraging Tags for: custom RBAC definitions, Device Discovery policies, Device Score etc.

www.cyberhorses.io

info@cyberhorses.io