# **Maslach Burnout Inventory – Cybersecurity Edition (MBI-CS)**

## **Introduction**

The **MBI-CS** is designed specifically for **cybersecurity professionals, analysts, engineers, SOC personnel, and IT security teams** who operate in high-stress environments. These roles often require handling cyber threats, responding to incidents, and enduring long hours of intense concentration.

The survey measures burnout across three key dimensions:

* **Emotional Exhaustion:** Feeling drained by continuous security alerts, cyber incidents, and workload.
* **Depersonalization (Detachment):** Developing cynicism or detachment from security responsibilities, end users, and management.
* **Personal Accomplishment:** A sense of effectiveness in mitigating threats, securing networks, and defending against cyberattacks.

## **Survey Items**

### **Emotional Exhaustion**

☑ I feel emotionally drained from responding to cybersecurity incidents.  
☑ I feel used up at the end of a long day monitoring security alerts.  
☑ I feel fatigued knowing I have another shift defending against cyber threats.  
☑ Working in cybersecurity is mentally and emotionally exhausting.  
☑ I feel burned out from the constant need to stay ahead of attackers.  
☑ I feel frustrated when I see repeated security failures despite my efforts.  
☑ I feel I am working too hard to maintain security with little organizational support.  
☑ The 24/7 nature of cybersecurity operations puts too much stress on me.  
☑ I feel like I’m at the end of my rope when dealing with security incidents.

### **Depersonalization (Cynicism & Detachment)**

☑ I sometimes view end users as careless and part of the problem rather than people I need to protect.  
☑ I’ve become more cynical about leadership’s commitment to cybersecurity.  
☑ I worry that this job is making me emotionally detached.  
☑ I feel indifferent about new security policies or initiatives.  
☑ I sometimes feel that no matter what I do, security issues will never improve.

### **Personal Accomplishment**

☑ I can effectively analyze and mitigate security threats.  
☑ I feel confident in my ability to prevent cyber incidents.  
☑ I have positively influenced the security posture of my organization.  
☑ I feel a sense of achievement when I successfully defend against an attack.  
☑ I can educate others about security risks in an engaging way.  
☑ I am proud of my contributions to cybersecurity.  
☑ My work in security is meaningful and rewarding.  
☑ I feel energized when solving complex security challenges.