



Cybersecurity Burnout: The Hidden Threat to Your Security Team

We'll explore the impact of burnout on cybersecurity teams and strategies to build long-term resilience

A GLOBAL STUDY BY NOMINET FOUND THAT OF THE
CHIEF INFORMATION SECURITY OFFICERS SURVEYED:

89%

of U.S. based CISOs
never had a two week
break from their job

88%

work more than
40 hours a week

91%

said the levels of stress
were moderate or high

18-24
MONTHS

is the average tenure
of a chief information
security officer



CYBERSECURITY
PROFESSIONALS



of IT security
professionals

CYBERSECURITY
JOB MARKET

3

MILLION

unfilled cybersecurity positions
at companies worldwide

Why This Topic Matters

Burnout isn't just a personal issue—it's a threat to your cyber resilience. With over 60% of cybersecurity professionals reporting moderate to severe burnout, the real-world costs of fatigue-induced errors, missed alerts, and disengagement pose a serious risk to organizations.

Learning Objectives



Recognize how burnout shows up in security teams

Identify emotional exhaustion, cynicism, and reduced performance in your team



Understand its measurable security impact

Explore how fatigue leads to errors, disengagement, and delayed incident response



Apply practical strategies to reduce burnout

Implement process, technology, and people-centric approaches to build team resilience



Strengthen long-term resilience in your cyber team

Foster a culture of psychological safety, shared ownership, and mental health support

A thriving security team is the foundation of long-term cyber resilience.

What is Burnout?

WHO Definition

- Chronic workplace stress not successfully managed - Leads to exhaustion, detachment, and reduced performance

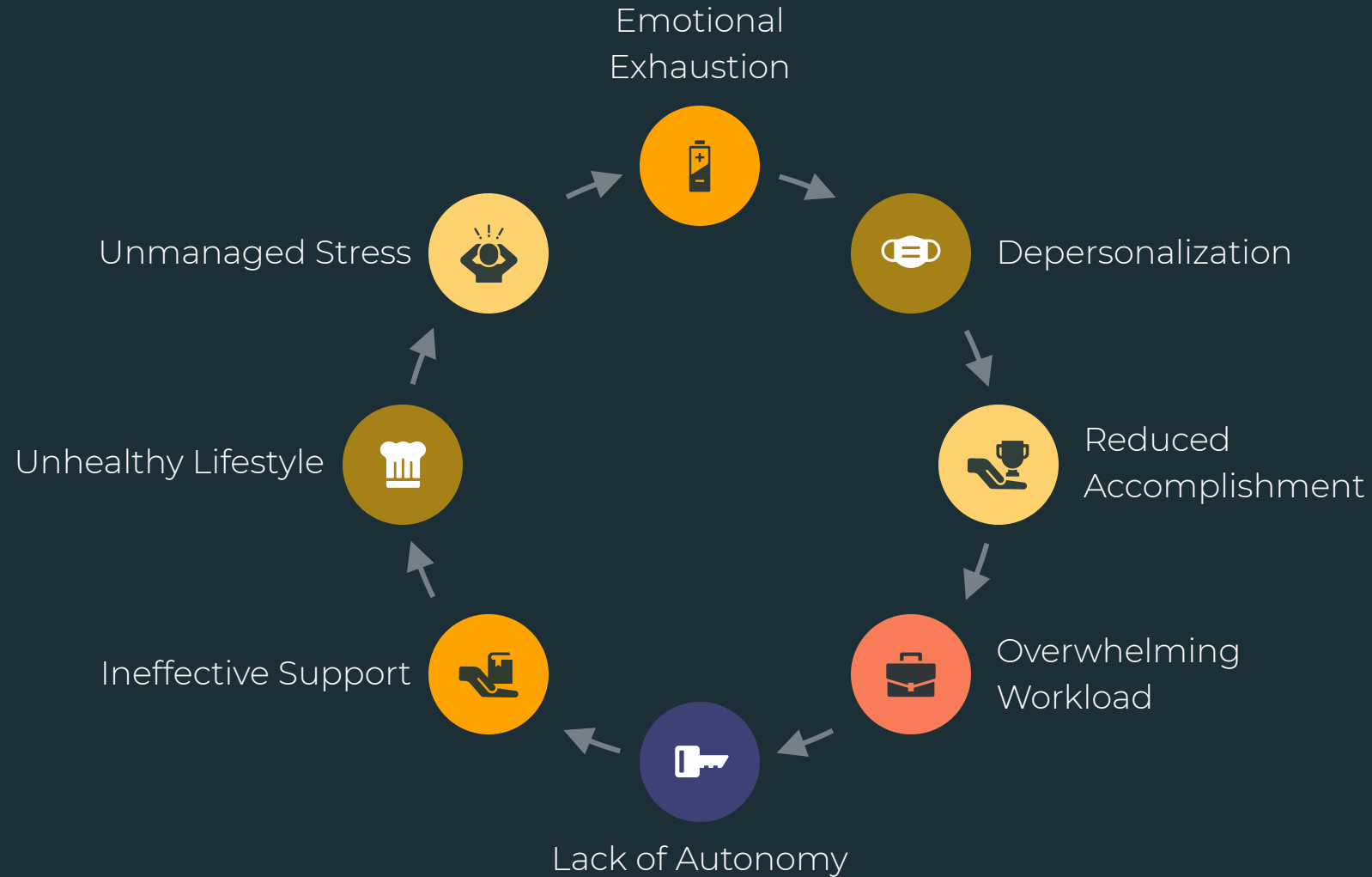
Cyber Context

- Emotional exhaustion → careless mistakes - Cynicism → disengagement from alerts - Reduced efficacy → delayed IR and misconfigurations

Excerpt from 'Psybersecurity'

"Burnout is not a byproduct—it's a breach vector in slow motion."

The Burnout Flame



Unique Stressors in Cybersecurity

- Constant on-call pressure
Security teams are expected to be available 24/7 to respond to incidents, leading to chronic stress and fatigue.
- Alert fatigue in SOC environments
Security Operations Centers (SOCs) are inundated with a high volume of alerts, causing analysts to become desensitized and less responsive.
- "Never enough" feeling due to evolving threats
The cybersecurity landscape is constantly changing, leaving teams with a sense of never being able to fully secure their environment.
- Compliance & breach anxiety
The pressure to maintain regulatory compliance and the fear of a costly data breach add significant stress to security teams.
- Skill gaps force fewer people to do more
Understaffed security teams are often forced to take on more responsibilities than they can reasonably handle, leading to burnout.

The Hidden Cost of Burnout

Poor Decision-Making

Burnout can lead to impaired judgment, resulting in suboptimal security decisions.

Slow Incident Response

Overworked and stressed teams may struggle to respond quickly and effectively to security incidents.

Incomplete Log Review

Burnout can cause teams to overlook or miss important security logs, creating blindspots.

Inconsistent Patching

Burnout can lead to inconsistent and delayed software and security updates, increasing the risk of vulnerabilities.

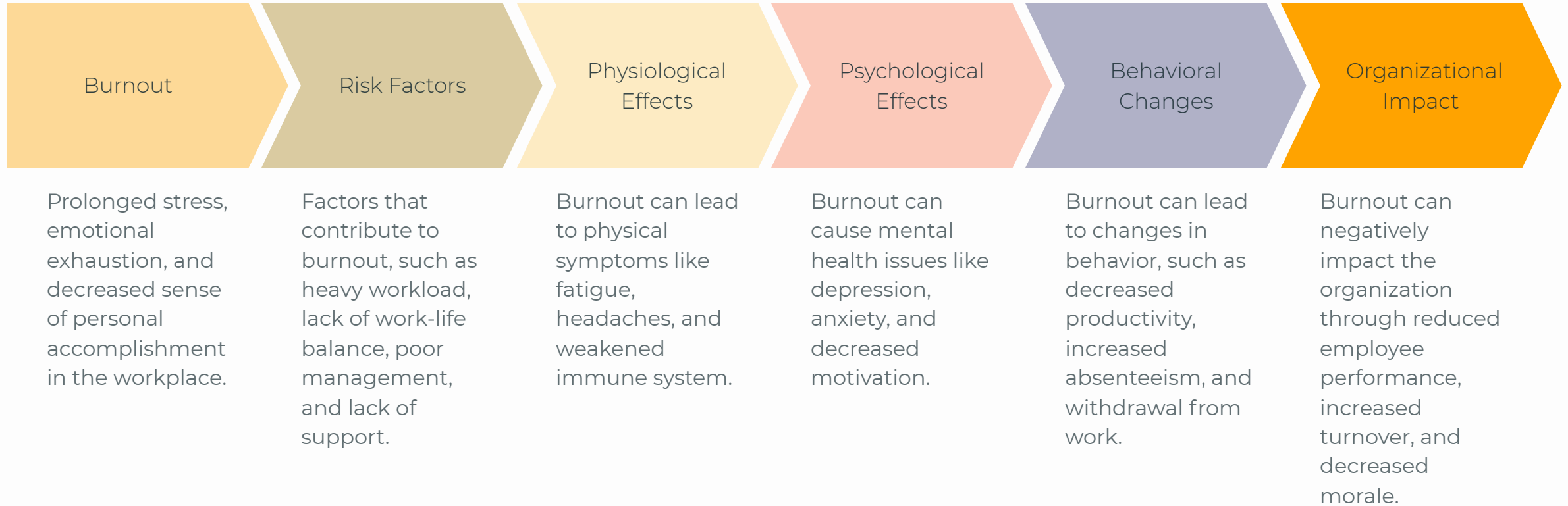
Higher Turnover

Burnout can drive team members to leave, leading to a loss of institutional knowledge and expertise.

Collapsed Team Morale

Burnout can severely impact team morale, negatively affecting collaboration and communication.

Burnout: Risk Pathway



Real-World Case

● Early 2022

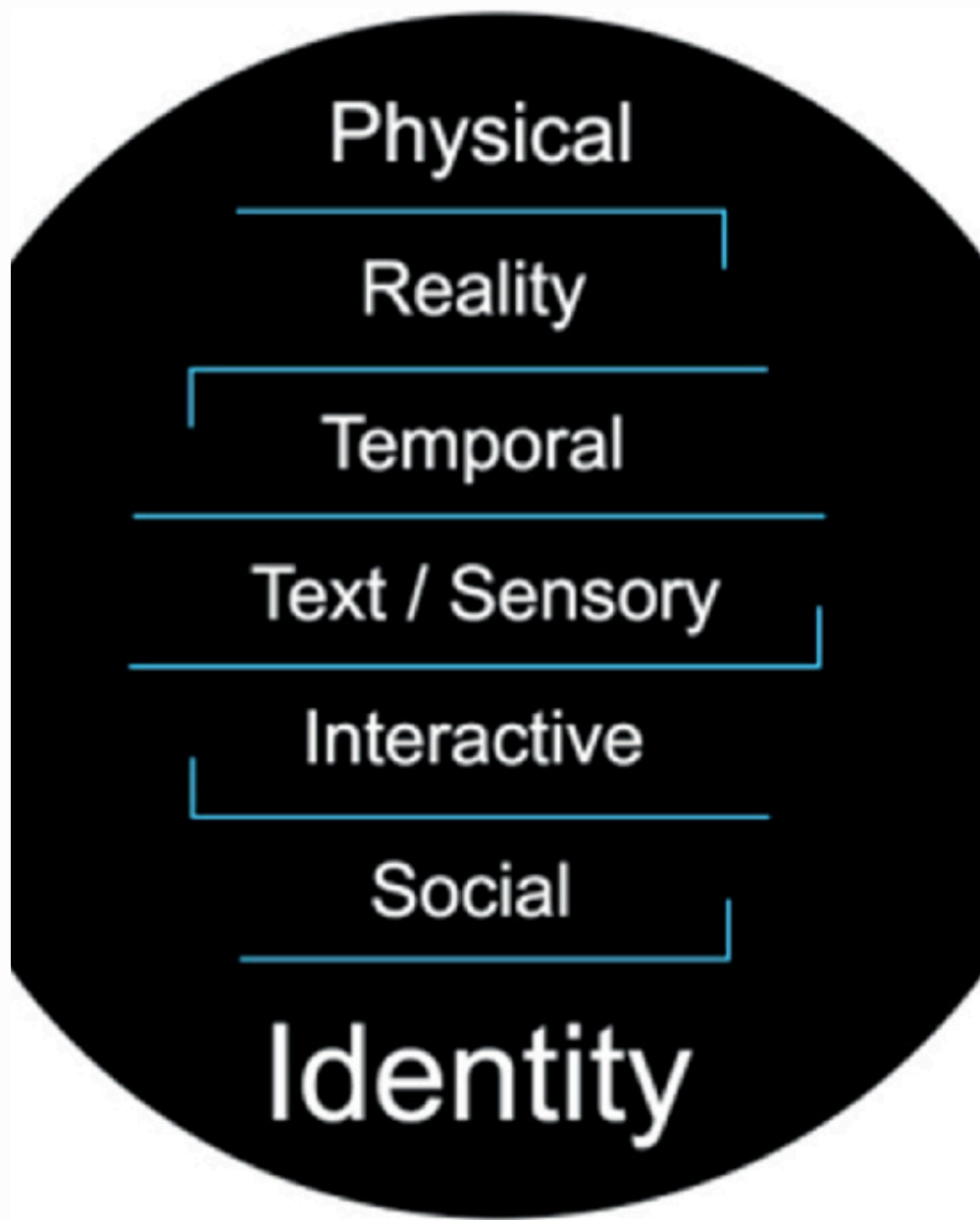
A large organization's SOC team missed signs of lateral movement within their network

● Late 2022

An \$8M breach occurred that could have been stopped with a single alert

● Mid 2022

The team was short-staffed, overworked, and rotating sleep schedules



The Psybersecurity Lens

The Psybersecurity Lens explores how psychological factors impact the cybersecurity professionals tasked with defending against evolving threats. This section delves into the cognitive and emotional strains that can lead to burnout, and how they ultimately compromise an organization's security posture.

The Psychology of Cyber Burnout

- Decision Fatigue

Reduced ability to make effective judgments after continuous hours of threat triage or compliance decisions, leading to poor prioritization, skipping of critical steps, or overreliance on automation.

- Cognitive Overload

Security environments flood analysts with alerts, logs, policies, and emerging threats, leading to burnout when there's no space to mentally 'declutter', reducing short-term memory and processing power.

- Reduced Pattern Recognition

Analysts rely heavily on pattern recognition and intuition, but under chronic stress, these intuitive signals dull, making threats blend in with the noise.

- Mental Depletion & Situational Awareness

Prolonged cognitive strain dulls an individual's ability to maintain active situational awareness, resulting in 'blindness on the battlefield' and preventing the processing of seemingly 'low-risk' anomalies that often precede larger attacks.

- Threat Anticipation Under Stress

The amygdala's dominance during chronic stress shifts the brain from strategic to reactive thinking, preventing the burned-out analyst from spotting emerging threat patterns and diminishing proactive hunting, weakening the long-term security posture.

- Shift in Risk Tolerance

Exhaustion and emotional strain unconsciously increase or decrease risk tolerance, leading burned-out analysts to ignore minor alerts or overreact to benign ones, either of which can be costly.

How to Spot Burnout in Your Team

- Disengagement from daily tasks
Reduced participation in regular security operations and a lack of enthusiasm for routine work
- Increase in avoidable errors
Security analysts making more careless mistakes or overlooking critical details due to fatigue
- Cynical comments during standups
Negative, sarcastic, or dismissive remarks during team meetings or check-ins
- Long response times, even during incidents
Delayed reaction and decision-making during security incidents and alerts
- Resistance to continued learning/training
Reluctance to engage in professional development or upskilling activities
- Absenteeism
Increased sick days, extended breaks, or disengagement from the team

Leadership's Role in Prevention

Avoid Overburdening

Piling on more work and responsibilities without providing additional resources or support will only exacerbate burnout among the security team.

Minimize Endless Incident War Rooms

Reduce the frequency and duration of high-stress incident response meetings, which can drain the team's emotional and cognitive resources.

Set Boundaries and Model Work-Life Balance

Leaders should be intentional about not contacting the team on weekends or during off-hours, setting an example of healthy boundaries.

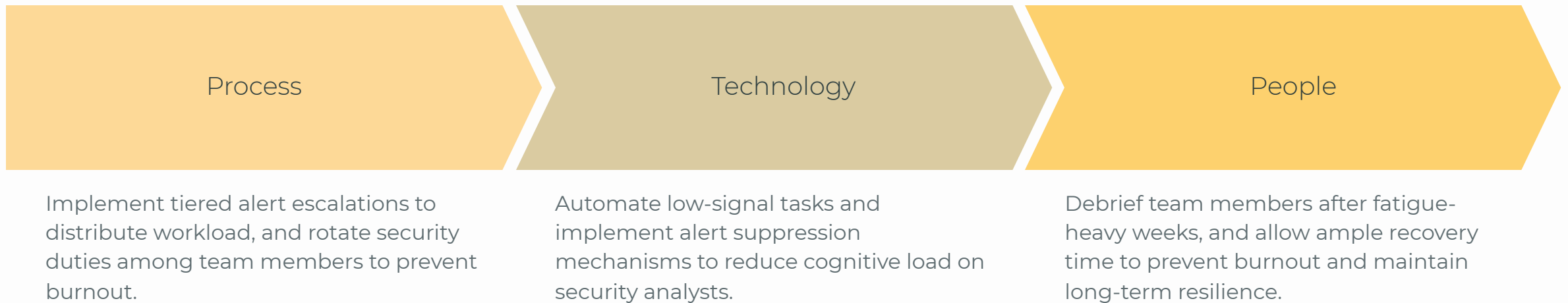
Empower Rather Than Micromanage

Give the security team autonomy and trust to manage their own workloads and workflows, rather than constantly looking over their shoulders.

Normalize Rest Cycles and Handoffs

Implement shift rotations, paid time off, and clear handoff procedures to ensure the team can recharge and avoid burnout.

Systemic Solutions



The Role of Peer Support



Encourage mental health discussions

Create a supportive environment where team members feel comfortable discussing mental health challenges and seeking help when needed



Create "cyber wellness champions"

Identify and empower team members to advocate for mental health and wellness initiatives



Anonymous feedback mechanisms

Provide confidential channels for team members to share concerns, ideas, and feedback without fear of repercussions



Weekly mental temperature checks

Regularly assess the team's well-being and identify any signs of burnout or stress

A trusted team not only talks about threat intel, but also supports each other's mental health and well-being.

Building a Resilient Culture



Psychological Safety

Team Collaboration

Leadership Empowerment

Burnout Mitigation

Designing a Culture of Shared Ownership and Psychological Safety



Shared ownership of success/failure

Encourage a culture where everyone takes responsibility for outcomes, both positive and negative. This fosters a sense of collective accountability.



Recognition of invisible labor

Acknowledge the often unnoticed efforts and contributions of team members, especially those who perform behind-the-scenes tasks. This promotes a culture of appreciation.

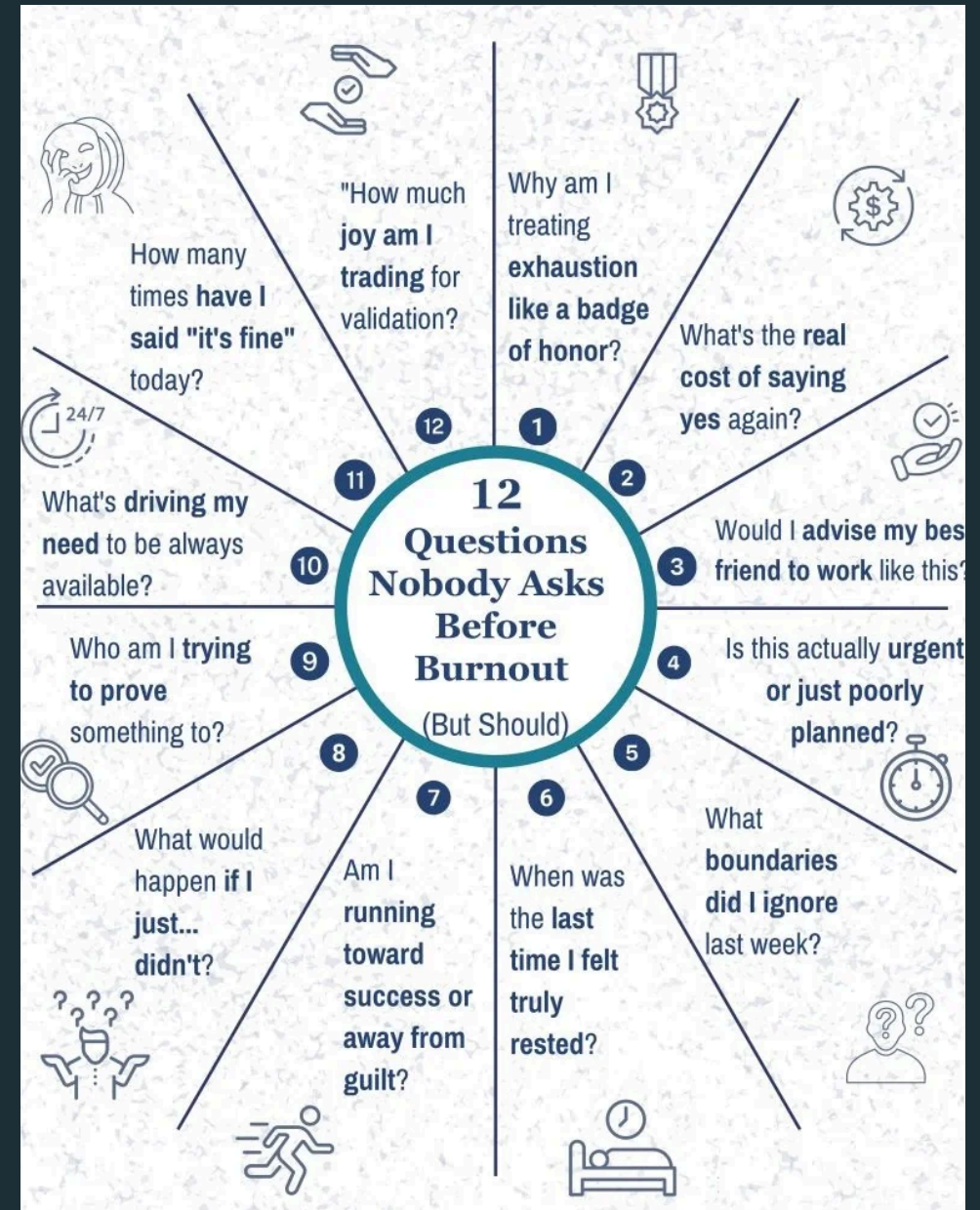


Inclusion in threat modeling & postmortems

Ensure that all relevant stakeholders, including those who may not be directly involved in a project, are included in discussions around potential risks and post-incident analyses. This promotes a culture of transparency and collective learning.

By designing these cultural pillars, organizations can foster an environment that enables collaboration, innovation, and continuous improvement, even as they leverage automation and technology to drive efficiency.

Personal Action Plan



Key Takeaways



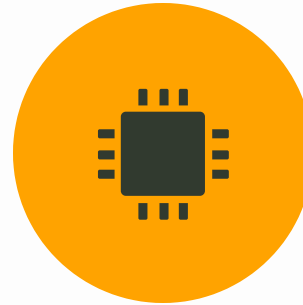
Burnout impacts risk just as much as tooling gaps

Burnout leads to fatigue-induced errors, missed alerts, and disengagement - all of which can weaken an organization's security posture.



Prevention is a shared, strategic responsibility

Addressing burnout requires a holistic approach involving leadership, processes, technology, and peer support.



Psychology helps us detect and defend better

Understanding the psychological impacts of burnout, such as decision fatigue and reduced pattern recognition, can help security teams recognize and mitigate the threat.

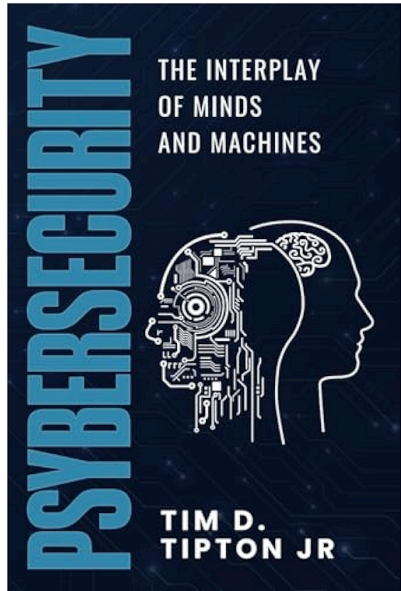


A thriving team is a resilient team

Building a burnout-resistant security culture that prioritizes mental well-being and shared responsibility leads to more sustainable, high-performing teams.

By addressing burnout as a strategic priority, security leaders can strengthen the long-term resilience of their cyber defenses.

Resources & Further Reading



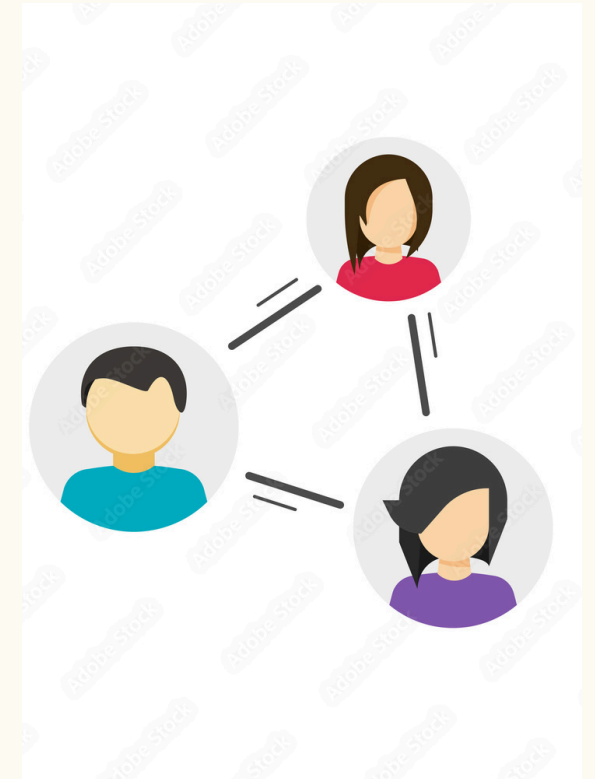
Psybersecurity: The Interplay
of Minds & Machines



Burnout Assessment Tools
Maslach Burnout Inventory, WHO-
5



Mental Health Organizations
for Cyber Pros
Cybermindz, Mental Health
Hackers



Peer Communities

Q&A



Share challenges with leadership

What do you wish leadership understood about burnout in your environment?



Discuss team dynamics

How do you see burnout impacting collaboration and trust on your team?



Explore burnout prevention

What proactive steps could your organization take to build a more resilient security culture?



Thank You + Takeaway Offer

Thank you for attending this session on the critical issue of cybersecurity burnout. As you leave, we encourage you to download the Cybersecurity Burnout Defense Toolkit, which includes practical resources to help you and your team build long-term resilience.