![Fortinet]

We're With You on the Journey
Services to Support Your Cybersecurity Planning

Change in the enterprise is a reality. Digital transformation, mergers and acquisitions, turnover in staff and employees, and threat landscape evolution all affect an organization's readiness to withstand attack. Maintaining a resilient cybersecurity program is an ongoing journey. It requires maintaining staff security skills and employee awareness, regularly updating network (virtual, physical, or cloud) defenses, and always including a review of processes—in addition to your technology investments. Where staff isn't available or skills can't be maintained, outsourcing options help augment your team, provide 24×7 coverage, or otherwise assist in protecting the enterprise.
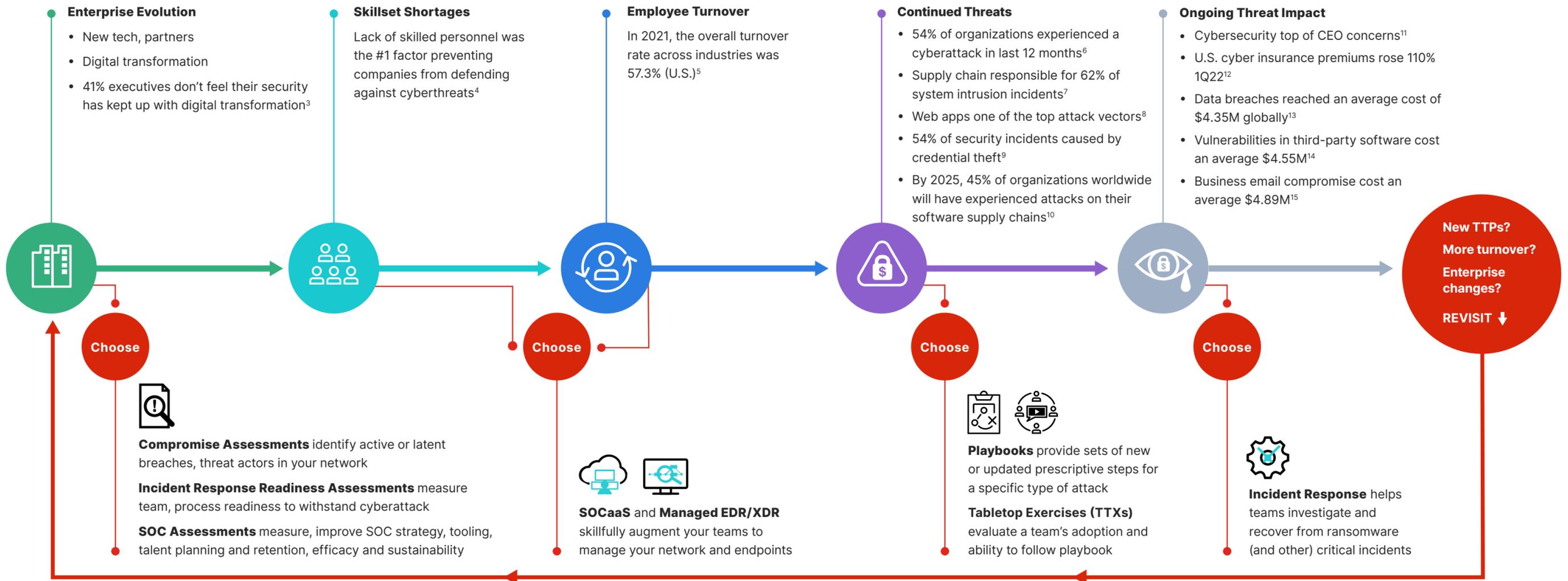
Upon any significant change, regularly updated assessments, playbooks, and tabletop exercises help to provide an up-to-date view of your readiness. They also help identify and address gaps before they become liabilities.

Did you know:

"A risk assessment can quickly identify and prioritize cyber vulnerabilities so that you can immediately...protect critical assets...while immediately improving overall operational cybersecurity."[1]

"The number one reason organizations did not have an incident response plan was due to lack of skilled internal resources."[2]

Fortinet has expert resources available to help you address these common challenges.

Enterprise Evolution
- New tech, partners
- Digital transformation
- 41% executives don't feel their security has kept up with digital transformation[3]

Skillset Shortages

Lack of skilled personnel was the #1 factor preventing companies from defending against cyberthreats[4]

Employee Turnover

In 2021, the overall turnover rate across industries was 57.3% (U.S.)[5]

Continued Threats
- 54% of organizations experienced a cyberattack in last 12 months[6]
- Supply chain responsible for 62% of system intrusion incidents[7]
- Web apps one of the top attack vectors[8]
- 54% of security incidents caused by credential theft[9]
- By 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains[10]

Ongoing Threat Impact
- Cybersecurity top of CEO concerns[11]
- U.S. cyber insurance premiums rose 110% 1Q22[12]
- Data breaches reached an average cost of $4.35M globally[13]
- Vulnerabilities in third-party software cost an average $4.55M[14]
- Business email compromise cost an average $4.89M[15]

New TTPs? More turnover? Enterprise changes? REVISIT ⬇

Choose

Compromise Assessments identify active or latent breaches, threat actors in your network

Incident Response Readiness Assessments measure team, process readiness to withstand cyberattack

SOC Assessments measure, improve SOC strategy, tooling, talent planning and retention, efficacy and sustainability

Choose

SOCaaS and **Managed EDR/XDR** skillfully augment your teams to manage your network and endpoints

Choose

Playbooks provide sets of new or updated prescriptive steps for a specific type of attack

Tabletop Exercises (TTXs) evaluate a team's adoption and ability to follow playbook

Choose

Incident Response helps teams investigate and recover from ransomware (and other) critical incidents

---

[1] Chuck Brooks, "A Cybersecurity Risk Management Strategy for the C-Suite," Homeland Security Today, May 11, 2022.
[2] "The 2021 Ransomware Survey Report," Fortinet, November 3, 2021.
[3] "Cybersecurity Solutions for a Riskier World," ThoughtLab, accessed August 18, 2022.
[4] "2022 Cyberthreat Defense Report," CyberEdge Group, accessed August 18, 2022.
[5] "19 Employee Retention Statistics That Will Surprise You (2022)," Apollo Technical, January 6, 2022.
[6] "The State of Cybersecurity and Third-Party Remote Access Risk," Ponemon Institute, July 20, 2022.
[7] "2022 Data Breach Investigations Report," Verizon, June 2022.
[8] Ibid.
[9] "The State of Cybersecurity and Third-Party Remote Access Risk," Ponemon Institute, July 20, 2022.
[10] "7 Top Trends in Cybersecurity for 2022," Gartner, April 13, 2022.
[11] "Cyberthreats: A year in retrospect," PwC, accessed October 15, 2022.
[12] "Global Insurance Market Index," Marsh, 2022.
[13] "Cost of a Data Breach Report 2022," IBM Corporation, July, 2022.
[14] Ibid.
[15] Ibid.