IDC

Building the Case for a Virtuous Cycle in Cybersecurity

JANUARY 2023

Authors:
Chris Kissel
Research Vice President, Security and Trust Products
Joel Stradling
Research Director, European Security

IDC #EUR149649622

An IDC InfoBrief sponsored by

DARKTRACE

What did the survey look at?

1

Identify barriers to achieving cyber resilience

Assess the current state of preventative security measures, and discover which, if any, are in use today, and how effective they are.

2

Gauge aspirational viewpoints

Identify any gaps in the industry that security professionals are struggling to fill as well as the aspirations of end users and what they are aiming to achieve by carrying out preventative security.

3

Identify if there are nuances in different regions in the U.K. and in North America and in industries.

Measure how people, processes, and technology vary by region and industry ...

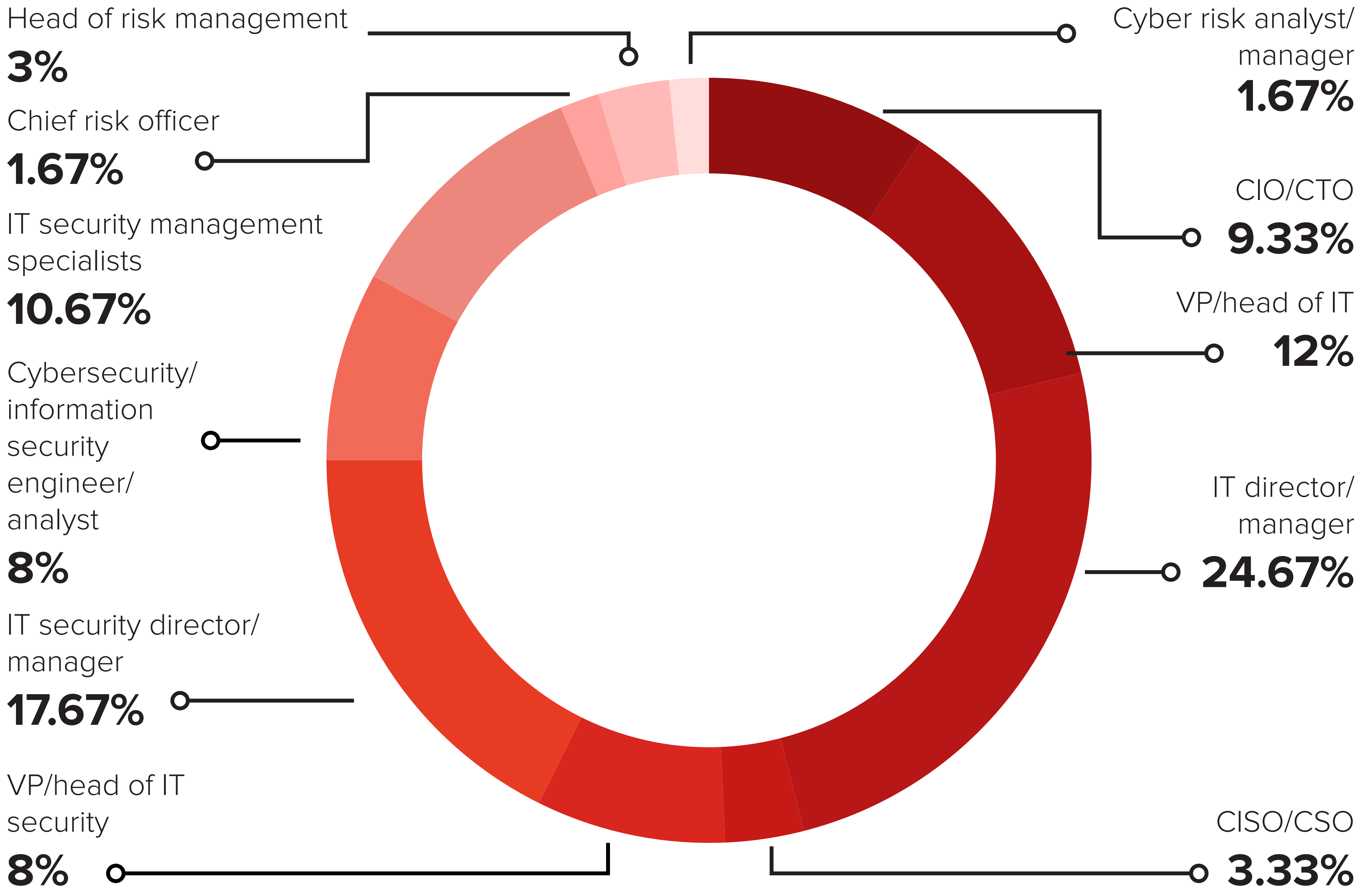
© 2023 IDC

Survey methodology

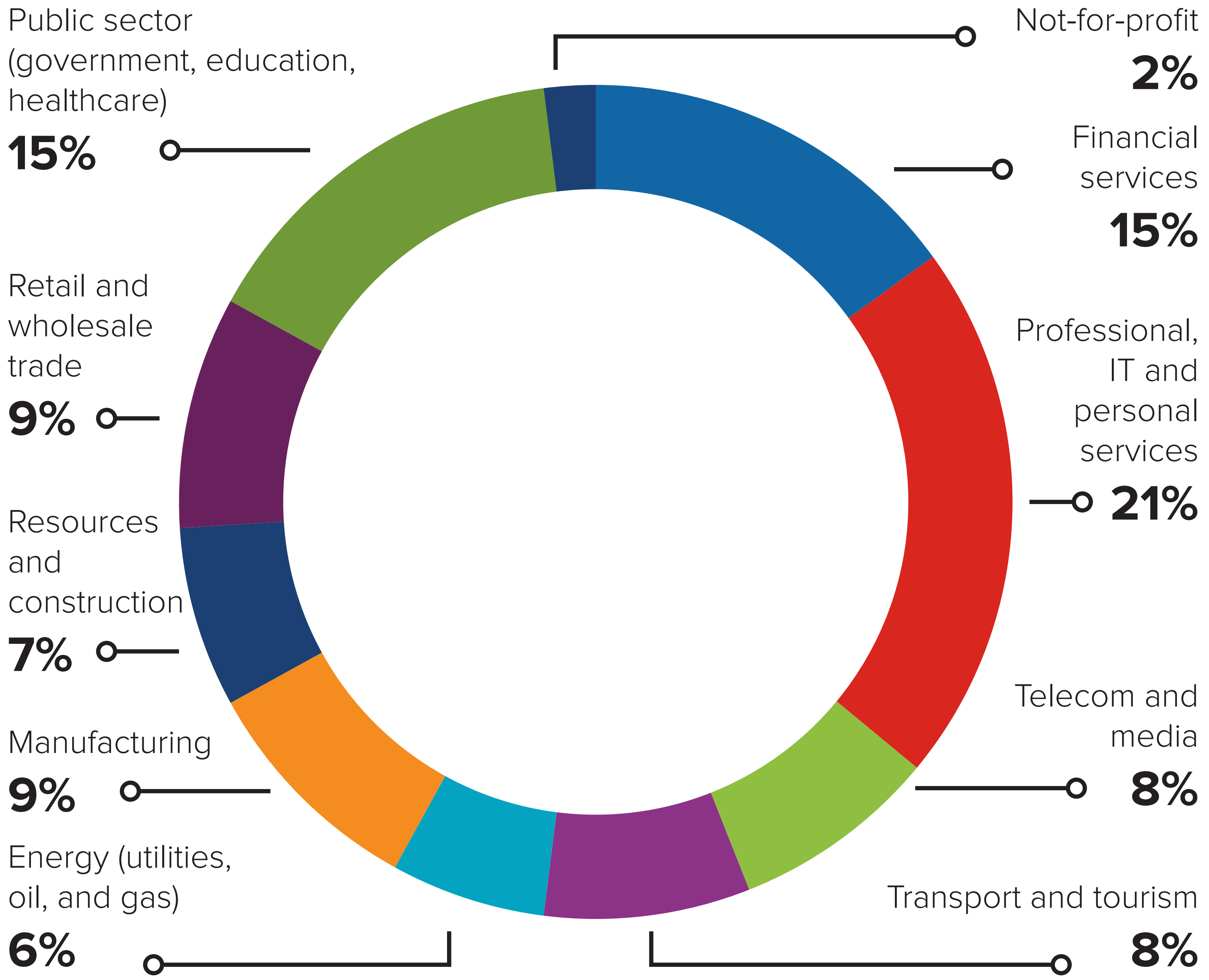
In July 2022, IDC surveyed senior security professionals at 300 companies across Europe and the U.S., looking at where security professionals are challenged in implementing preventative security measures and the gaps in their security postures that they are struggling to fill.

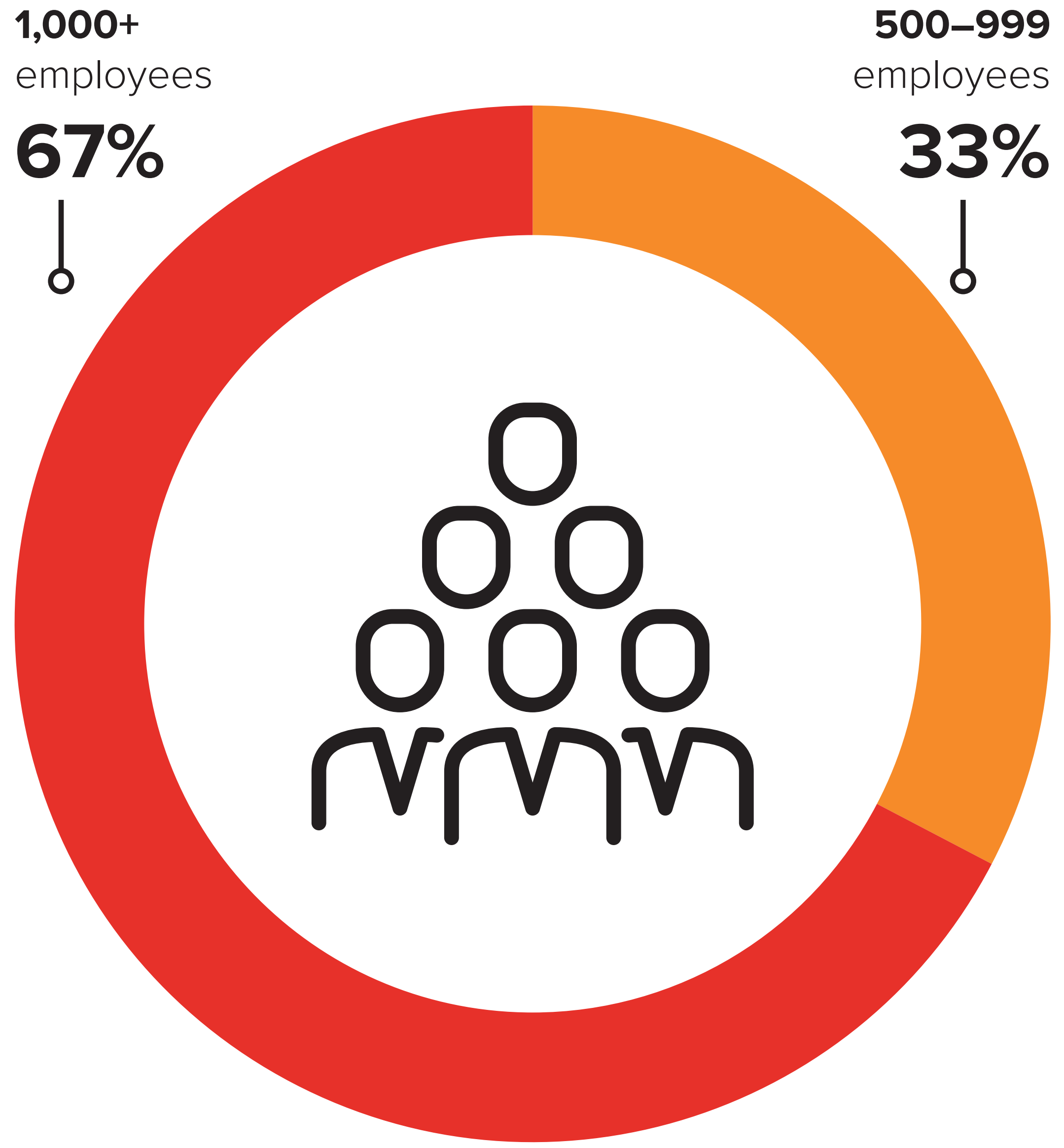
Geography

31%	19%	7%	6%	4%	5%	12%	17%
U.S	Canada	Germany	Austria	Switzerland	Ireland	U.K	Benelux



Industry verticals





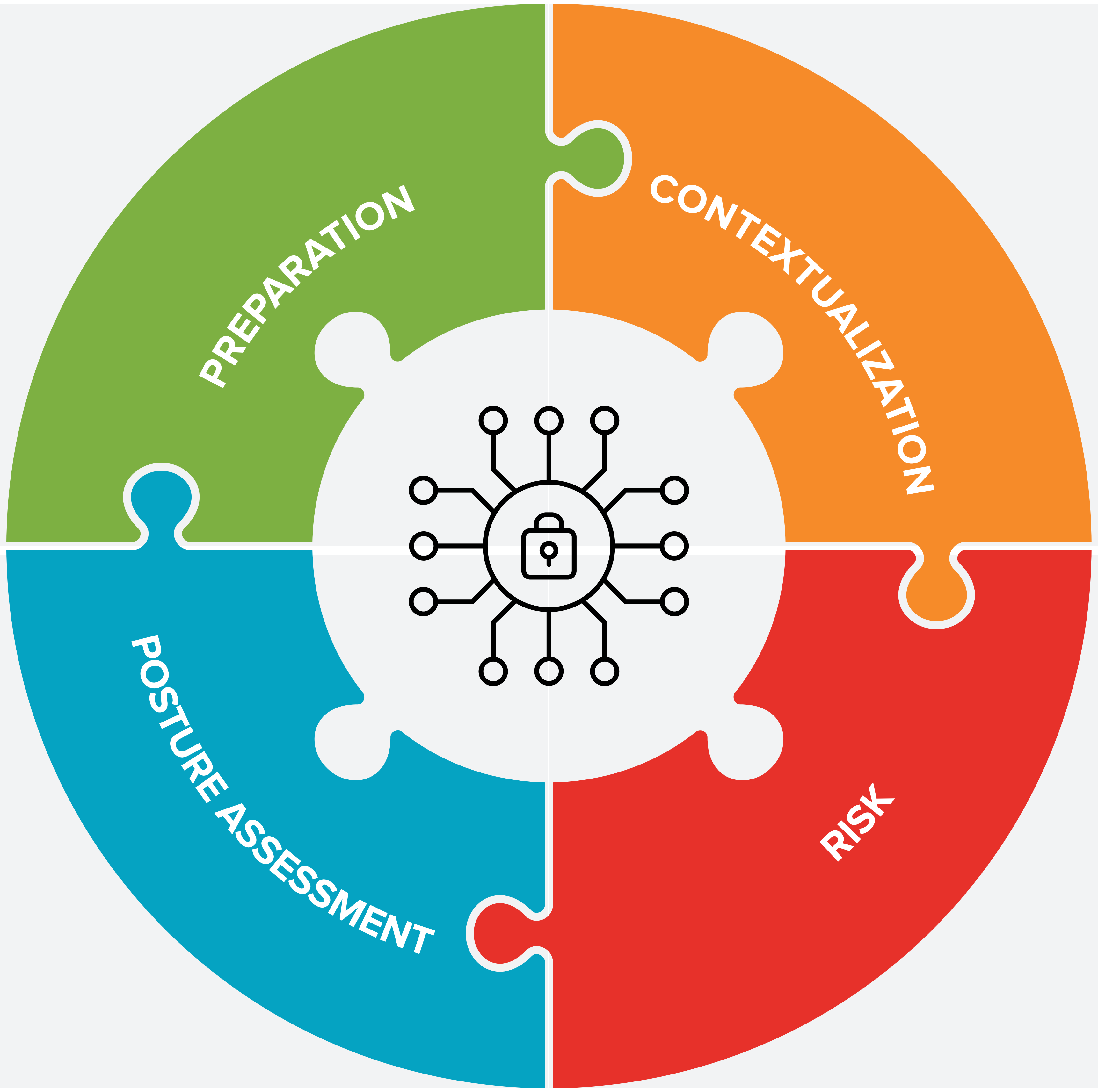
The current state of cybersecurity

Security is always challenging, and there are a number of factors that make this ever more challenging in uncertain times. Organizations already need to contend with a number of factors that threaten their resilience:

- Restrained budgets
- Limited cybersecurity talent pool
- Weight of established practices and processes
- Expanding IT estate and data ponds
- Unrelenting cyberthreats
- Strategic imperative to adapt and be resilient

© 2023 IDC

The most notable gaps in cybersecurity



Preparation

Attack vectors are evolving, making it difficult to prepare proactively.

Contextualization

Security teams have enough data; prioritizing it and making it actionable is hard.

Posture assessment

Architecture changes mean risk levels and scores quickly become out of date, meaning posture assessment needs to continuously evolve.

Risk

Without understanding the digital environment and vulnerabilities, mitigation is undisciplined.

© 2023 IDC

Source: IDC-Darktrace Survey, July 2022 (n = 300)

Organizations cannot properly prepare for evolving threats:

Challenge 1: PREPARATION

The number of organizations that can continuously run preventative exercises such as pen tests, vulnerability scans, breach attack simulation (BAS), risk scoring, and attack surface evaluation is between just **24%** and **31%** across all sectors.

Only **31%** of organizations surveyed have high confidence that their tools can continuously adjust to new configurations to identify new threats and vulnerabilities.

Just **32.7%** of organizations say they have high confidence they can investigate every incident.

Only **34%** of organizations say they have high confidence they can autonomously stop threats in real time.

Possible solutions: Automated approaches to pen testing, vulnerability scans, and BAS. An overall organization score accounts for the veracity and probability of a threat vector, the exploitability of a vulnerability, the value of the asset, and the possible blast radius. This requires an understanding of the golden state of devices and configurations and the changes that occur in a dynamic environment.

© 2023 IDC

At some point the network sees everything, but providing contextual information to inform the cybersecurity posture is still hard to do.

Challenge 2: CONTEXTUALIZATION

Just **34%** of organizations feel that pen testing/ red teaming can provide them with actionable insights on where and how to harden defenses.

69% of organizations agree that pen testing/red teaming only help them meet regulatory and compliance measures (which are not always actively beneficial for the security team).

65% of organizations agree that pen testing/red teaming give them only a snapshot in time, which is of limited value.

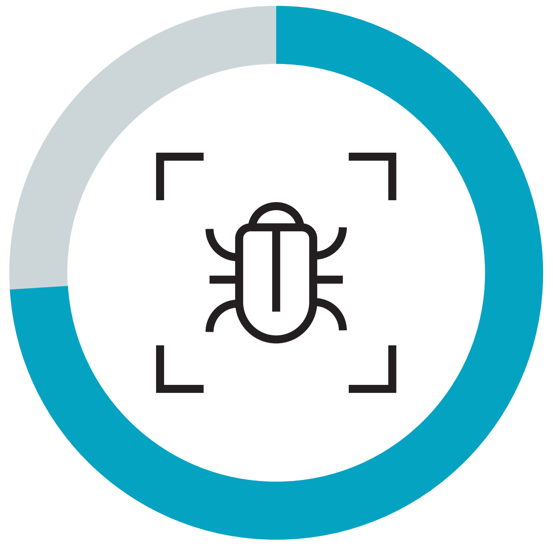
Just **32%** of respondents strongly agree that their team can correlate incidents that arise to find a single version of truth.

Possible solutions: SOC teams must learn to trust artificial intelligence/machine learning (AI/ML) to look for subtle changes in the behaviors of entities within a network. Pen testing and red teams become augmented by AI to provide context — and do so continuously. The strength of security analytics is that it can both prioritize and pinpoint the threats that matter most.

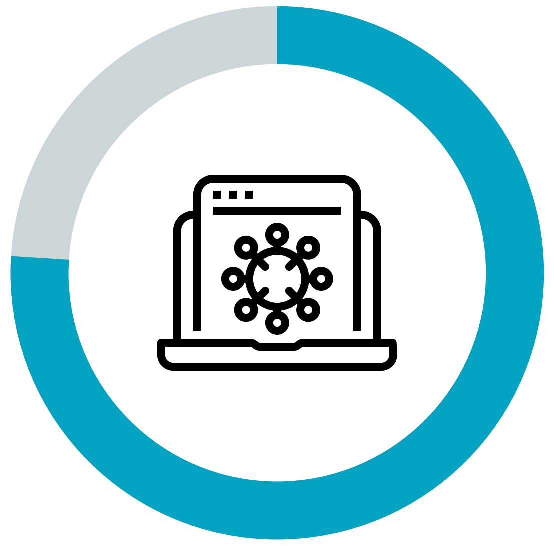
© 2023 IDC

Security tools and practices are integrated, but no one knows how strong the architectures are until the network is under fire.

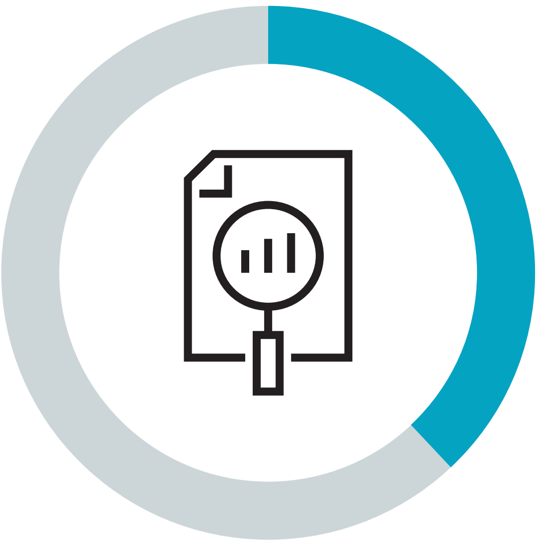
Challenge 3: POSTURE ASSESSMENT



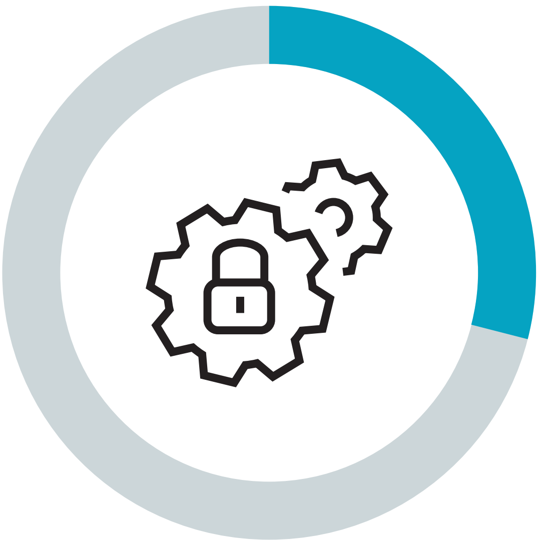
74% of respondents think that prioritizing vulnerabilities is of moderate or high importance.



76% of respondents think that visualizing attack paths and choke points is of moderate or high importance.



Only **38%** said they have high confidence in having good oversight over all assets and where they sit within an environment.



Just **29%** said they have high confidence that they have a robust mechanism to test their environments against the most current threat vectors.

Possible solutions: The security team must move away from vulnerability scores and toward vulnerability prioritization. Attack path visualization is used to prevent egress to the network by the adversary. The ability to identify (manage) all the assets in the digital estate enables proper simulation and threat attack exercises.

© 2023 IDC

Accounting for risk cannot be appreciated enough.

Challenge 4: RISK

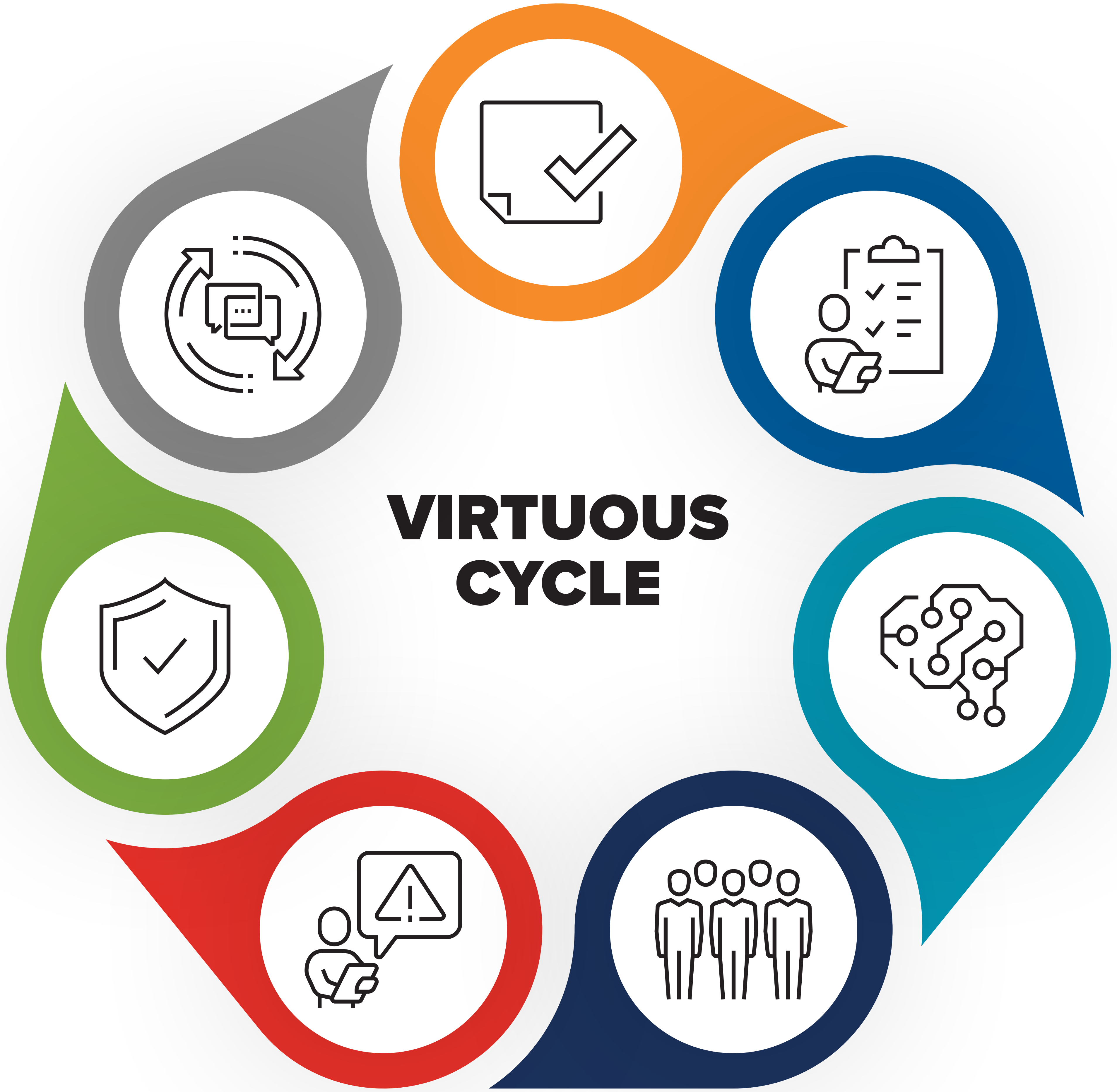
- Risk is a term used to assess outcomes and damages if there is a cyberattack.
- A way to think of risk arithmetically is risk = probable outcomes multiplied by potential damages multiplied by indemnities (compliance, loss of reputation, etc.) divided by (prevention + security controls + mitigation + recovery).
- Reducing risk occurs when any number of small things are improved. Attack surface management, constant inventory management, vulnerability prioritization, security posture assessment, and breach attack simulation all reduce risk.
- Risk reduction includes buy-in from IT, cybersecurity, and compliance departments.

Proof points:

78% of respondents think identifying high-risk assets (people and technology) is of moderate or high importance.

© 2023 IDC

Principles of a virtuous cybersecurity cycle



Details

Zero trust, compliance, secure data handling; working within frameworks is responsible.

Continuous asset inventory

Charting continuous changes in the network.

Artificial intelligence

Making use of telemetry in real time and at scale.

People, processes, technology

The SOC addresses human processes, tool integration, and visibility gaps.

Risk prioritization

Asset criticality, vulnerabilities, and potential blast surface determine what should be acted on first.

Trusted systems

Testing security protocols against threat vectors ensures confidence.

Harmonious feedback loop

Prevention leads to detection; detection enhances protection.

© 2023 IDC

Holistic cybersecurity requirements

Cybersecurity posture and hygiene requirements

- Secure configurations (S3 buckets not internet-facing, defined end-user access, etc.)
- Testing assumptions (breach attack simulation, pentesting, red team)
- Automated scanning (device and applications)
- Continuous asset management and discovery
- Perimeter defense still necessary
- Data and identity access management needed
- Risk-based prioritization

Continuous monitoring

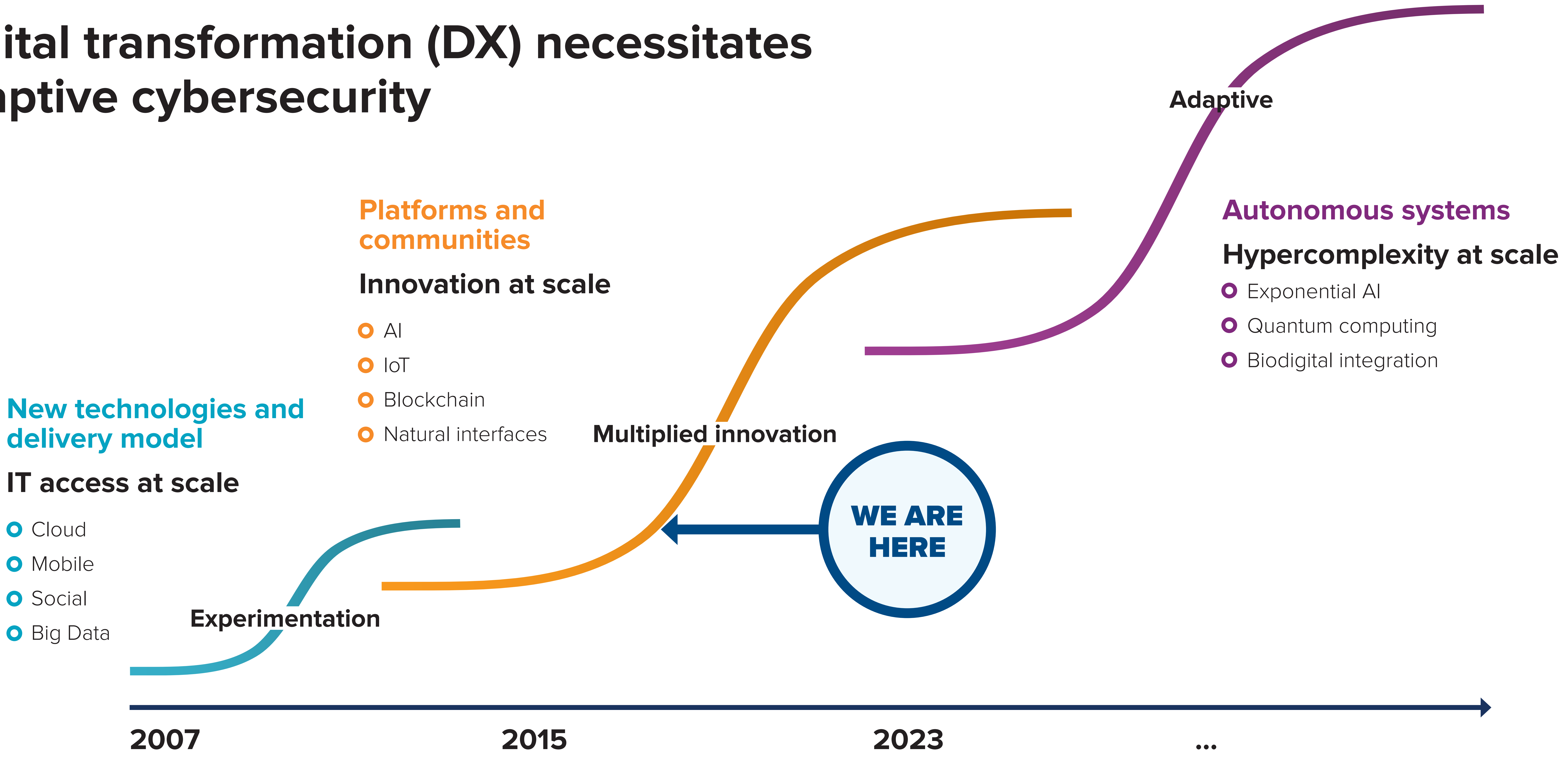
- Establish “individual normal” behaviors based on the weight of activities
- Determine if anomalies are benign, network, or security related
- Bubble up incidents by priority and risk
- Have immediate triage capabilities (the who/what/where snapshot)
- Track adversarial behavior through MITRE ATT&CK

Remediate

- Have an instantaneous response, then seek permanent resolutions (patches, reconfigurations)
- Command the response with assignments and playbooks
- Retest
- Have backup and disaster recovery procedures in place

Shift-through. Each cycle provides enrichment for the next time a team faces a threat. Cybersecurity posture and hygiene practices demonstrably improve over time.

Digital transformation (DX) necessitates adaptive cybersecurity



New technologies and delivery model

IT access at scale

- Cloud
- Mobile
- Social
- Big Data

Platforms and communities

Innovation at scale

- AI
- IoT
- Blockchain
- Natural interfaces

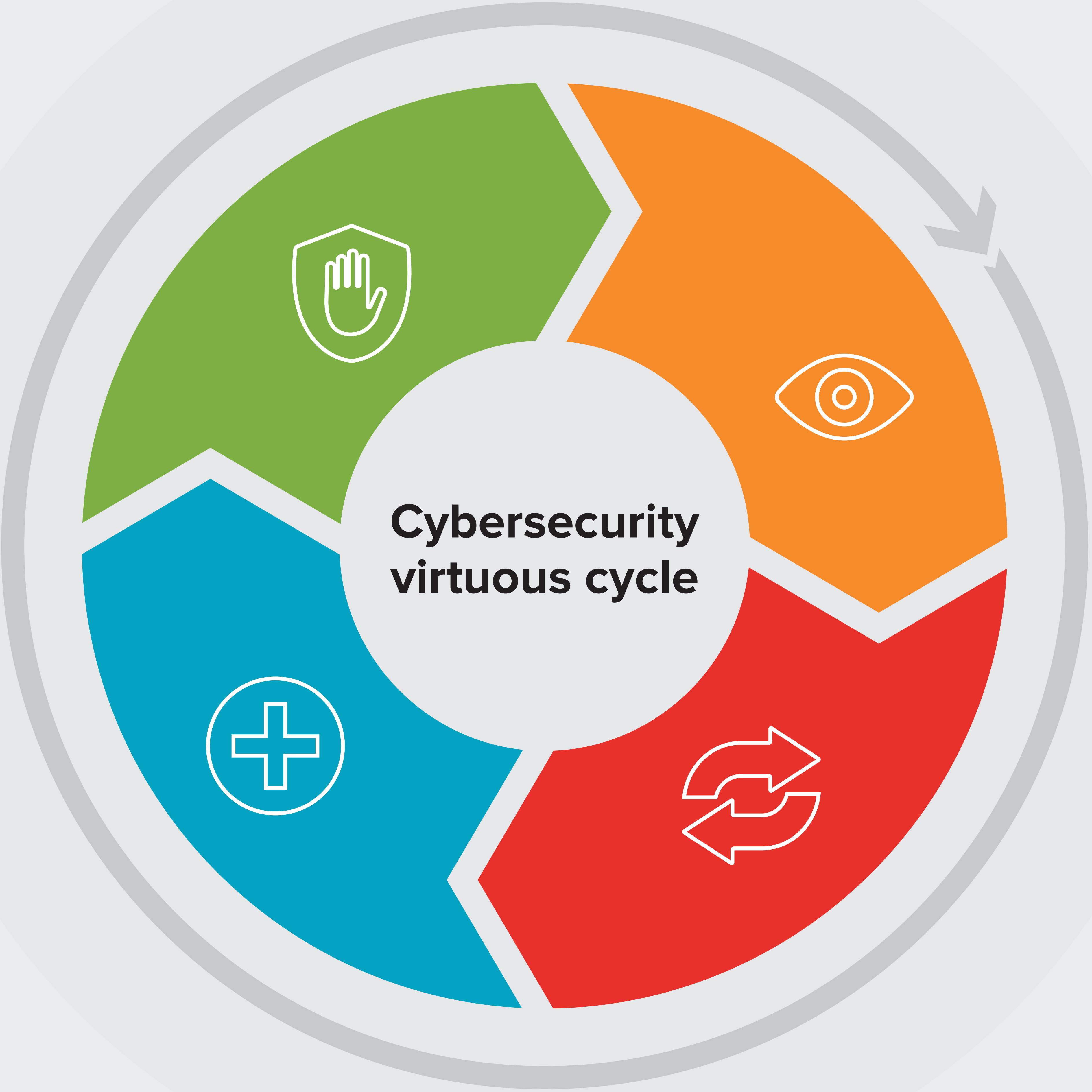
Autonomous systems

Hypercomplexity at scale

- Exponential AI
- Quantum computing
- Biodigital integration

Currently cybersecurity systems are platform and community security-based approaches. The approaches are essentially rigid. In 2023, AI correlates data from multiple data lakes. Companies need to think of security in terms of the surfaces it protects (on premises, private and public cloud, Kubernetes, OT, and shadow IT). There is no way to build manual processes that keep up with the expanding digital estate. Conversely, AI is the gateway to predictive defense, continuous security posture assessment, and autonomous security processes (response, patching, etc.).

Coordinated progression



Prevent

- Close visibility gaps
- Nullify risk
- Harden surfaces
- Test against active threats

Detect

- Continuous monitoring
- Indicators of compromise
- Anomalous behavior

Heal

- Verify that remediations took hold
- Reassess for cybersecurity gaps

Respond

- First action to stop the spread
- Initiate playbooks

© 2023 IDC

Conclusion: The case for building a virtuous cycle in cybersecurity

Creating the virtuous cycle in cybersecurity: current state of security

Current approaches are not enough

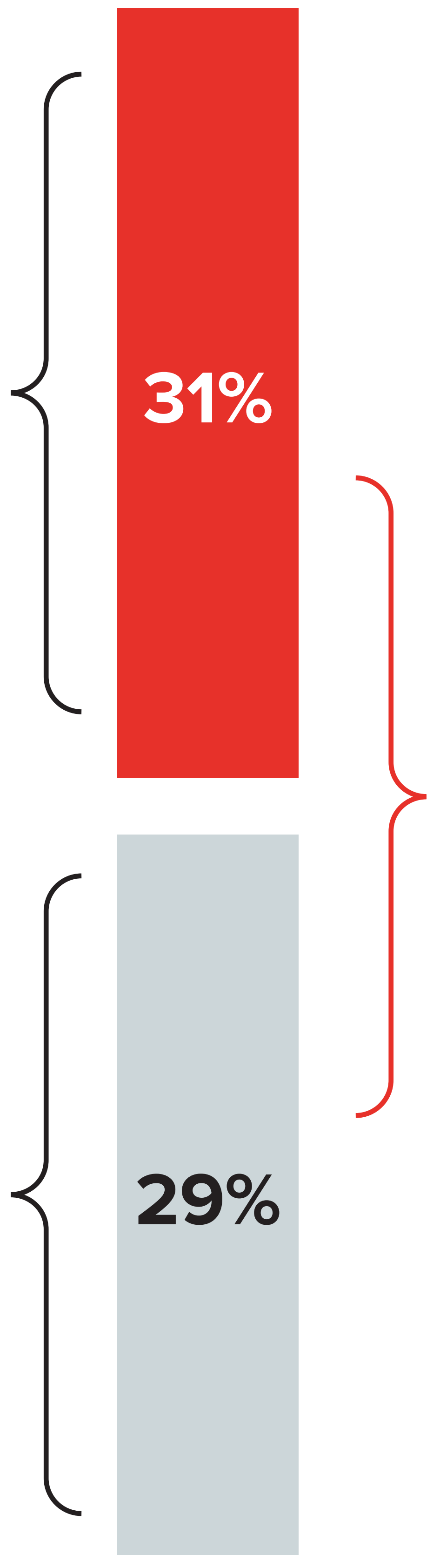
Having gone through their DX journeys, organizations are increasingly adopting digital-first operating models. Digital-first organizations depend significantly on digitalization, data, cloud transformation, and agile software development. The pathway to a digital business must be pursued hand in hand with robust security and navigating potential new risks that might be an unwelcome addition during adoption. As the attack surface expands, point protections lose effectiveness, so organizations need to adopt broader solutions to improve their readiness.

Too much information and too many holes

Companies struggle to keep track of and respond to all threats and frequently cite an inability to accurately prevent threats or mitigate vulnerabilities before they cause damage. Typically, no one knows if security architectures work until they are under duress, which is often too late. Even when performed properly, the offensive/proactive tests (pen testing/red teams) are often not reliable, repeatable, or specific enough on where there are gaps in the security posture.

A holistic approach to cybersecurity

The solution is to take a multipronged approach that includes establishing a security posture and proactively managing the access and assets, monitoring what is happening in the environment, and ensuring a fit-for-purpose remediation approach including backup and disaster recovery. This is how a virtuous cycle is created. Continuous monitoring and AI make for better detect and response capabilities. As importantly, continuous monitoring and AI can determine if remediation is working and if the new cybersecurity posture is better than the one the company had before an incident investigation.



We have high confidence that our tools can continuously adjust to new configurations to identify new threats and vulnerabilities.

We have a robust mechanism to test our environments against the most current threat vectors.

Less than a third of organizations can claim confidence in their ability to adjust to their configurations, much less their ability to test their environments against current threat vectors.

© 2023 IDC

Source: IDC-Darktrace Survey, July 2022 (n = 300)

Conclusions

Virtuous cycles matter

For years, cybersecurity vendors had to be “team prevent” or “team detect.” The thinking is fallacious — both ideas bleed into each other.

The only real cybersecurity answer is AI/ML

Network architectures include on-premises, heterogeneous, cloud environments, wireless, OT, and (soon) the metaverse. Manual processes cannot keep pace.

Practice makes perfect

Cybersecurity platforms seem to be integrated through API. This sounds great until a security team is under siege. Security teams need dry runs against current adversarial techniques.

The defender must understand all of its assets

Continuous monitoring is not an optional requirement. Every asset has a profile, and a proper security strategy understands its baseline activities and its golden state and vigilantly monitors against its norms.

Get to “security shift-through”

Whatever flavor of detection and response is offered, a vendor must prove it can spot the anomaly and prove that after remediation its network is healthier than before the forensics cycle.

© 2023 IDC

Message from the sponsor

Researchers at Darktrace's Cyber AI Research Centre — based in Cambridge, in the U.K. — have been conducting research in the field of preventative security. Darktrace mathematicians and AI experts have been actively looking into how to address the core challenges of hardening environments against attackers.

The IDC-Darktrace survey was conducted to supplement Darktrace's ongoing research to understand the core challenges that organizations face when it comes to implementing preventative security practices. It also aimed to identify barriers to achieving a preventative security strategy that actively increases resilience and reduces risk.

Darktrace PREVENT, Darktrace's latest product family, proactively identifies areas of greatest risk across both internal and external attack surfaces, and empowers defenders to reduce cyber risk by autonomously hardening systems.

DARKTRACE

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Corporate Headquarters
140 Kendrick Street,
Building B, Needham,
MA 02494 USA
508.872.8200
www.idc.com

Copyright Notice

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or permissions@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Corporate Headquarters: 140 Kendrick Street, Building B, Needham, MA 02494 USA P. 508.872.8200 www.idc.com

© 2023 IDC. Reproduction is forbidden unless authorized. All rights reserved.