dimensional research

Pivoting to Risk-Driven and Proactive Security

A Global 2021 Survey of IT and Security Professionals

Introduction

This paper reviews key findings from a global survey focused on understanding the most threatening security attack vectors, key assets to protect, current activities to improve security posture, and how companies manage their attack surface. The research also investigates the value and adoption of threat modeling, as well as the strategic utilization of managed service providers (MSPs).

A total of 333 security, IT professionals, and executives at medium to enterprise companies representing all seniority levels were invited to participate in a survey on their company's security practices. The survey was administered electronically, and participants were offered a token compensation for their participation.

Executive Summary

This report finds that 83% of companies suffer crippling business damage if they are down for 24 hours or more. Recent surges of ransomware and other attacks are creating tremendous business risk yet security resources remain modest at around 30% of IT budgets. The disconnect between business risk and resources continues as most security teams have received increases of less than 10% since the work-from-home employees began regardless of the growing attack surface and threat vectors.

When security professionals are asked how they are trying to improve their company's security posture, the top answer is upgrading tools (67%), an effort which they also report is being thwarted by integration difficulties, lack of expertise, and just having too many tools. However, only 35% plan to hire more experienced staff to bring expertise in and grow the team. This low resource rate is compounding the reliance on tools and disproportionately consuming key personnel's time with its' maintenance.

Given the new threats, it is surprising that a majority of security teams are trapped doing the same thing they have been doing for years: adding even more tools and needing more resources to manage them. However, when asked what security professionals actually want to be doing, the top answer is risk management, followed by incident analysis and threat modeling. This indicates a philosophical shift from reactive tools to a proactive risk-based approach. This report finds 68% of companies prioritize threats according to potential cost to the business and the impact they fear most is loss of data and negatively affecting customer relationships.

Security professionals state that threat modeling specifically enables a proactive approach by evaluating business risk from understanding the likelihood of attack success and mapping that potential breach to actual business cost. This risk-based approach prioritizes security defenses around the most likely, highest business-impacting attack vectors. Unfortunately, this research finds that less than 40% of companies perform threat modeling today and only 30% practice external attack surface management.

With security team resources growing slowly and consumed by patching, updates, and tool upgrades, combined with a lack of expertise, it is not surprising that 47% of companies utilize MSPs today. But with extra resources available, it is disappointing to find only 17% of the MSPs are being employed to perform threat modeling.

It's clear from these findings that security professionals know that they are being reactive and acknowledge doing the same historical things will not secure their company from growing and evolving attack risks. But they cannot escape numerous mundane and low-value tasks siphoning their time. Looking to MSPs is a solid strategy that can free teams up to be proactive, focusing more on risk management and threat modeling, and initiating the change to a proactive risk-based security approach.

Key Findings

New Attacks Threaten Businesses but Companies Stuck Doing More of the Same

- 83% suffer major business damage if outages last just 24 hours
- Ransomware leads all attack concerns
- 8 out of 10 companies have 30% or less of their IT budget dedicated to security
- 99% trying to improve security posture, but 67% remain focused on tool upgrades
- Companies challenged by tool integration, lack of experience, and too many tools

Threat Modeling Moves to Proactive, Risk-Driven Approach but Few Employ It

- Teams want to do more risk management, incident analysis, and threat modeling
- Companies want threat modeling to provide a proactive security approach based on actual business impact
- Less than 40% perform threat modeling

Security MSPs Provide Resources, Expertise and Threat Modeling Resources

- Patching and updating consumes valuable security resources
- 47% of companies rely on a MSPs
- Only 17% of MSPs are performing threat modeling

About Dimensional Research

Dimensional Research provides practical marketing research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how IT organizations operate.
For more information, visit www.dimensionalresearch.com.

About Netenrich

Netenrich transforms modern digital operations with Resolution Intelligence®, an intuitive software-as-a-service (SaaS) platform, across network, data center, multi-cloud and security operations. The platform seamlessly integrates AI, data analytics and analyst expertise to drive digital operations' transformation, gain operational efficiencies and deliver business outcomes. The complete portfolio integrates with 140+ market-leading digital and security applications to improve tools and incident response effectiveness. More than 3,000 customers and partner organizations worldwide rely on Netenrich. The company is based in San Jose, CA.
For more information, please visit www.netenrich.com