An IDC InfoBrief, sponsored by Mandiant

A GUIDE FOR SECURITY VALIDATION

RESEARCH BY:

Chris Kissel
Research Director, Security & Trust Products, IDC

October 2021 | IDC Doc. #US48050421

Navigating This InfoBrief

Click on titles or page numbers below to navigate to each.

Executive Summary

There is a notable gap in the enterprise security programs today. Companies buy several tools and attempt to integrate these tools. Security validation is a platform that tests the efficacy and interconnectedness of security tools against the threats and tactics of an adversary.

This InfoBrief:

- Identifies and quantifies the challenges that businesses face from adversaries.
  - The need for security validation becomes evident quickly. The question of whether a company is appropriately protected cannot be simply addressed by malware signatures and threat simulations—it requires a greater understanding of how the company's defenses perform against threat actors and tactics relevant to its business.
- Examines what is important in security validation (it is decidedly more than threat simulation).
  - Security validation is a compelling use case; however, a well-conceived security validation solution can be used to understand initial baselines, validate timestamps, determine if telemetry is being properly passed between point products, help security practitioners improve their skills, help in the proof-of-concept stage of purchasing, and make relevant threat intelligence actionable.
- Presents experiences from security practitioners to provide tangible illustration.

Proving Security Effectiveness Despite Today's Threat Revolution

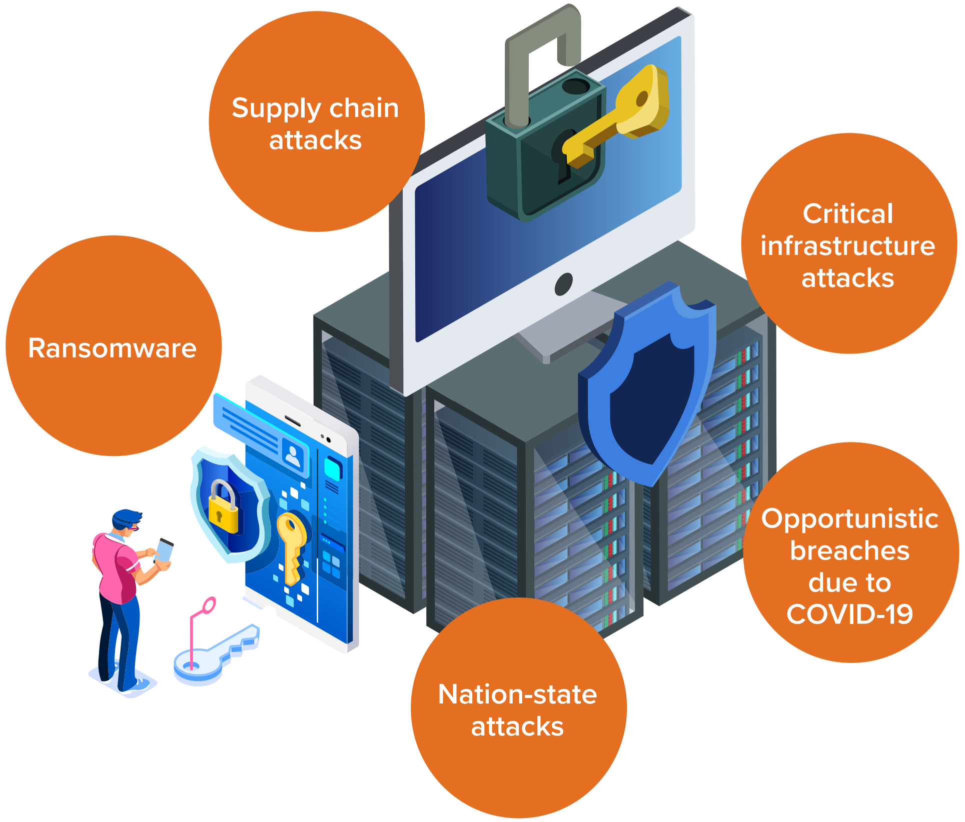
The Organizational Challenge in Cybersecurity

Adversaries pose an existential threat to IT that directly affects an organization's operational risk and bottom line: brand, stock price, customer loyalty/retention, reputation, and operational competency.

The enterprise response has been to spend more on security technologies, services, and people, but there's no mechanism to measure and demonstrate the value of these investments.

Top executives and boards demand hard data from security leaders around both the effectiveness and value of their cybersecurity spend against prioritized attack types and a company's risk profile.

A Growing Set of Threats


Supply chain attacks
Critical infrastructure attacks
Ransomware
Opportunistic breaches due to COVID-19
Nation-state attacks

Cybersecurity Spending Is Out of Control

The average organization uses

30–70

SECURITY TOOLS

and may spend millions of dollars addressing a single type of attack.

According to the IDC Software Tracker, in 2020,

$66.5 BILLION WAS SPENT ON DEDICATED SECURITY HARDWARE AND SOFTWARE APPLIANCES,

a market forecast to grow 12% year over year through 2026.

Security hardware and software appliances can be connected with OpenAPI, but connectivity alone does not deliver the visibility and insights necessary to measure the critical benefit metrics of detection, prevention, and alerting.

Cybersecurity often wastes dollars pitting IT and operational technology in a competition for money and talent, instead of enabling them to collaborate on designing for specific outcomes.

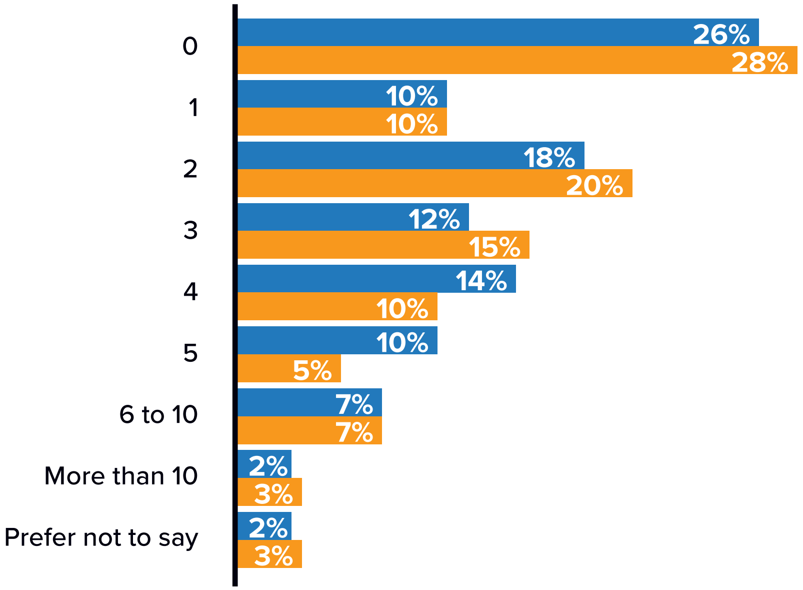
Simple questions in the security operations center (SOC) go unresolved: that is, is the SIEM picking up telemetry from security tools, or is telemetry from endpoints picked up from the SIEM? The SOC needs visibility into the behavior of tools, how tools are connected at each intersection, and how the cybersecurity stack works throughout the full life cycle of an authentic attack.

Confidence in Prevention Despite Increase in Major Breaches

Believing they are better prepared to prevent future security breaches, 61% of organizations view a major breach in the next year as unlikely despite 70% having had one or more major breaches in the last two years.

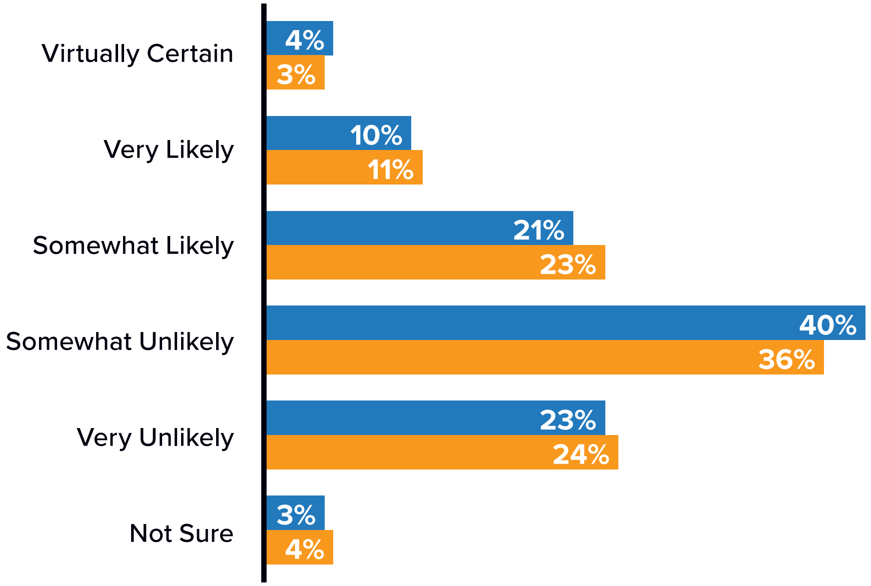
Major security breaches in last two years

(% of respondents)



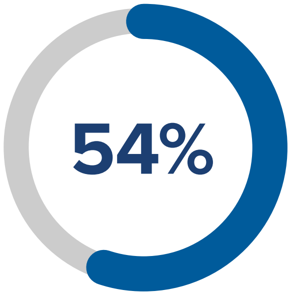
Likelihood of a major security breach in next 12 months

(% of respondents)



■ 2,500 to 4,999 employees (n = 252) ■ 5,000 or more employees (n = 252)

Source: IDC's *EDR and XDR Survey*, December 2020. n = 504



of organizations that sustained four or more breaches view a breach in the next 12 months as unlikely

Why Security Outcomes Aren’t Changing Despite Significant Investments

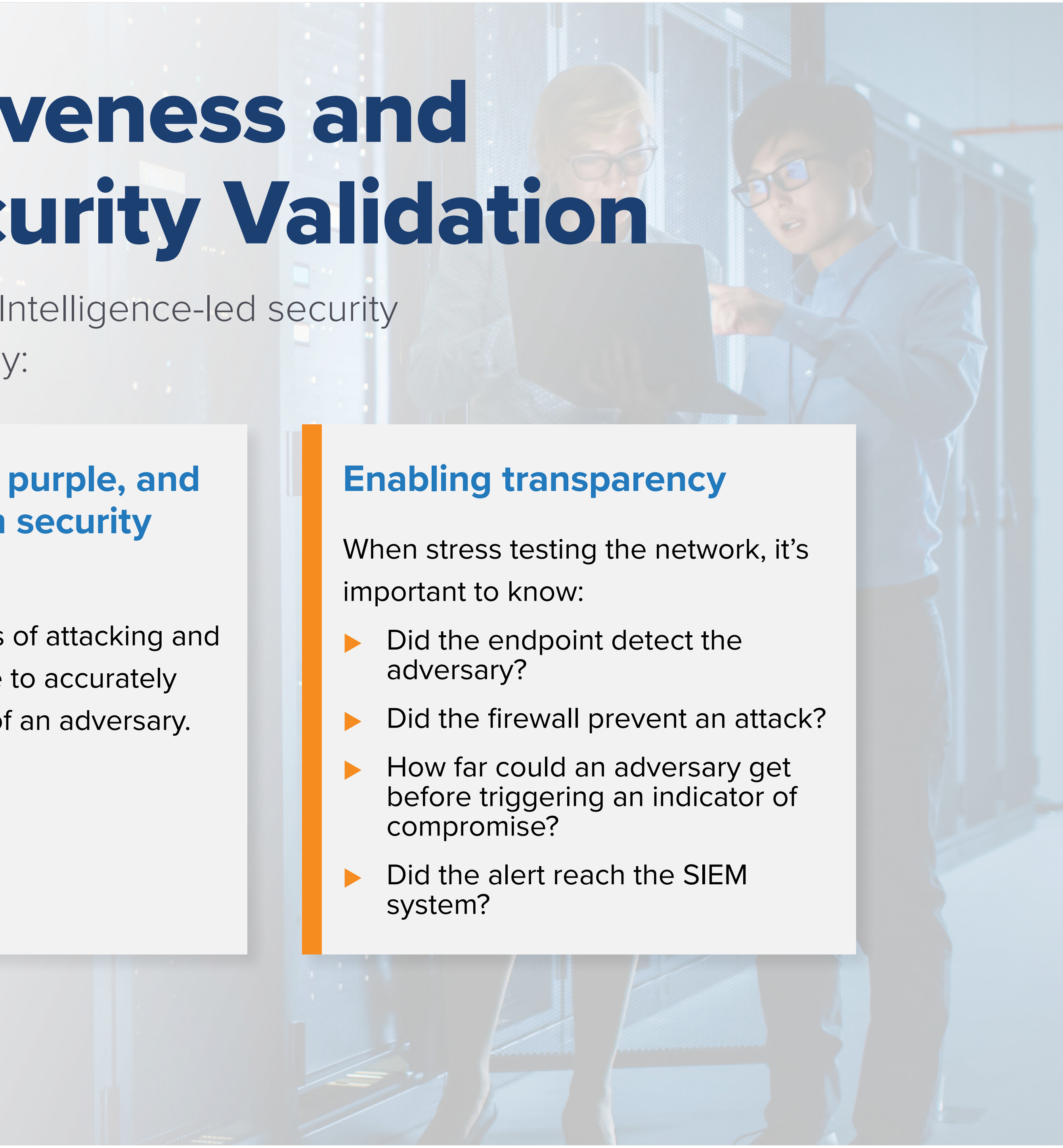
Security leaders and their teams deal with a complex set of challenges including:

- A shortage of data when selecting/managing tools, technologies, and vendors
- Growth in heterogenous environments and expanding attack surfaces
- Little visibility into ongoing threats and why breaches so frequently occur (misconfigurations, default settings, and broken processes)
- An abundance of threat data that lacks the curation to make the data actionable
- Too many tools
- Threat evolution
- IT drift over time

How best to ensure a healthy security stack/infrastructure? Create a good known baseline and continuously maintain it—with the use of security validation technology to assess the efficacy of the security stack and its controls.

Prove Security Effectiveness and Competency with Security Validation

Security threats are constantly changing and growing. Intelligence-led security validation helps companies fortify enterprise security by:



Measuring security infrastructure health

The perfect security stack takes many iterations and requires automated stress testing against real tactics and real artifacts. Validation of network segmentation and remediation of unknown IT changes that may impact security controls are critical to ensure the stack's health.

Optimizing red, purple, and blue teams with security validation

The proper functions of attacking and protecting teams are to accurately emulate the tactics of an adversary.

Enabling transparency

When stress testing the network, it's important to know:

- Did the endpoint detect the adversary?
- Did the firewall prevent an attack?
- How far could an adversary get before triggering an indicator of compromise?
- Did the alert reach the SIEM system?

Operationalize Threat Intelligence with Validation Technology

Organizations need to find the appropriate threat intelligence services and the right way to integrate the data into the security stack. An intelligence-led security validation platform can help determine relevant organizational threats and inform a validation strategy.

With access to active and relevant attacker tactics, techniques, and procedures (TTPs), a validation platform can challenge security controls to:

- Address gaps and redundancies
- Identify areas for improvement/optimization
- Enable decisions based on workflow
- Report with evidence
- Prove and demonstrate business competency

Benefits of an Intelligence-led Security Validation Solution

Cyber innovations enable security teams to emulate attackers during the controls testing process. Teams can safely deploy real attacks informed by authentic, relevant, and active threat data.

Emulated attacks allow an organization to validate its security controls against current threats and quantify the degree to which they are optimized and configured.

Such a process can determine if tools are aligned with Top 20 SANS Controls, NIST 800.53 Rev. 4, or MITRE ATT&CK Framework.

Validation is dramatically changing the security market from a black box to a set of business outcomes.

Considering Mandiant Security Validation Technology

Mandiant Security Validation provides evidence required to prove value of security investments and security effectiveness to continuously optimize a cybersecurity program.

Mandiant's adversary visibility informs an extensive library of threat actor behaviors and malware and is integrated into its security validation platform. The platform can operationalize threat intelligence and serve as a force multiplier for red and blue team tools to find indicators of compromise not yet detected from the security tools.

Its intelligence-led validation technology shows how controls respond to active attacks with full attack life-cycle visibility to capture accurate data on an organization's security effectiveness.

Security validation is an automated, continuing practice that delivers quantitative data on the efficacy of security controls across technology, people, and processes that can proactively enable continuous optimization of cyber defenses.

> ***"The red team uses the same script as the platform, which allows us to replay packet captures."***
>
> —CISO of a major U.S. banking and financial institution

Mandiant Security Validation Technology in the Field

Between November 2020 and February 2021, IDC interviewed five different Mandiant Security Validation technology clients. The following are brief synopses of how the tool was used in the field:

A U.S. healthcare provider uses Mandiant Security Validation to assess the efficacy of everything from firewall rules to endpoint tools. For example, the platform discovered endpoint logs lagged in generating logs in the SIEM. Without timestamp fidelity, the company could not rely on the telemetry to tune endpoints and firewall policies.

An insurance business uses Mandiant's platform to spot gaps and redundancies in the insurer's security posture, helping it consolidate tools. The insurer can now initiate continuous attack scenarios. The platform's "Protected Theater" functionality also provides it with proactive protection against destructive attacks.

> ***"Mandiant Security Validation is used to test attack scenarios against our cybersecurity stack—this also includes email and phishing attack [tests]."***
>
> —CISO of a large U.S. insurer

Mandiant Security Validation Technology in the Field (continued)

A technology company uses the Mandiant platform to stress test its firewall environment. The use of validation content enabled the company to see minute details; for example, that its SIEM was underperforming and required more capacity to handle log ingestion. The tool also found expired certificates and helped analysts improve response capabilities and remediation time. Continuous validation proved which tools were working.

A U.S. loan processor has roughly 40 security point products. Five years ago, it moved all its assets into an AWS-hosted environment. Initially, it deployed Mandiant Security Validation in Windows; the tool is now used to validate Linux, Mac OS, iPads, and iPhones. The company later used the platform to help in the proof-of-concept stage when purchasing new tools, enabling it to have real data to help it choose a vendor.

A major banking and financial institution uses Mandiant Security Validation to test multiple zones such as internal to external communications, DMZ to DMZ, D2 tests, and various tests designed to indicate C2C communications. The intent is to establish a baseline set of rules. The company can put in a test code through an SDK. The test code can create evasive action patterns to catch in Windows or add additional risk rules to watch for after an action passes the threat column and before an incident is picked up by the SIEM.

What Cybersecurity Practitioners Say

"More than a simple attack simulation, Mandiant Security Validation integrates aspects of an attack (active TTPs) to truly validate controls….Threat intelligence from Mandiant is used to test controls against the latest threat actors and behaviors so they can answer the question, "Am I protected against the headline threat of the day?""

—CISO of a large U.S. insurer

"Mandiant Security Validation performs a drift analysis every day."

—CSO of a major U.S. healthcare provider

"The best thing this platform does is it easily allows us to run recurring attacks to determine what behavior can be expected from the security stack."

—CSO of a major U.S. healthcare provider

"We adopted the MITRE ATT&CK Framework. We can perform a specific percentage of techniques that are demonstratable and receive rapid validation."

—CISO of a large U.S. insurer

Challenges to Adoption

Security validation is an important approach to a cybersecurity posture. However, the vast majority of security programs subsist without a validation platform.

The Mandiant Security Instrumentation platform is often discussed in the same realm as other security point products (endpoint, firewall, etc.). The problem is security validation does not "prevent, detect, and respond," as point products and platforms do. What security validation does is provide insight into how well the components of a security stack (tools/resources) perform in a real-time, emulated threat environment, and determine which of these tools are working properly.

It is possible that extended detection and response (XDR) will begin to subsume many of the validation functions that are currently a part of the Mandiant Security Validation platform.

Benefits of Intelligence-led Security Validation

Interviewees told IDC that Mandiant’s intelligence-driven platform provided the data and insight required to prove security effectiveness and led to security health assurance, optimization, and rationalization of spend. Additional points of validation include:

Reinforcement of “fiduciary responsibility”

Organizations must understand the threats specific to their organization, industry, or region and stress test defenses against relevant and active TTPs. Mandiant Threat Intelligence adds to one side of the equation, and Mandiant Security Validation technology covers the other.

Authentic, active, and relevant

Security validation technology is lightweight, and its deployment is conducted safely despite use of attack binaries, malware, or other destructive attacks. Importantly, the attack scenarios do not inhibit the performance of the network and there is no abrasion to devices.

Automated and comprehensive

Aside from the network perimeter and East-West zones, Mandiant Security Validation validates the security postures of email, cloud, and endpoint security controls. The platform augments red, blue, and purple team exercises. Since companies could validate on a regular basis, they felt their defenses were reliable in-between formal team exercises.

Flexibility

Mandiant’s technology can be deployed in any environment. Standardized testing compares the best practices of analysts, departments, and security stack configurations, enabling continuous validation and optimization measurable over time.

Visibility and context

Mandiant Security Validation provides cybersecurity life-cycle visibility from detection to prevention to SIEM correlation and alerts, and it does so across the security stack. Informed by frontline intelligence, controls validation gains further context into the adversary threats and an organization’s preparedness.

Methodology

In Q420, IDC conducted interviews with security professionals who used Mandiant Security Validation technology. Interviews were conducted in each of the following verticals:

- Healthcare
- Insurance
- Technology
- Banking and Finance
- Lending

Data in this InfoBrief is also taken from IDC inquiries with enterprise IT organizations on related security, IT, and infrastructure and operations topics.

Additionally, data is cited from several other IDC surveys completed independently of the scope of the FireEye study. These surveys are part of IDC's subscription research services.

Interview analysis was combined with existing survey data and client subscriber reports to formulate a full narrative.

IDC's *EDR and XDR Survey*, December 2020

IDC's *Future Enterprise Resiliency & Spending Survey,* February 2021

About the Analyst

Chris Kissel
Research Director, Security & Trust Products, IDC

Chris Kissel is a Research Director in IDC's Security & Trust Products group, responsible for cybersecurity technology analysis, emerging trends, and market share reporting. Mr. Kissel's primary research area is Cybersecurity Analytics, Intelligence, Response, and Orchestration (AIRO). The major technology groups within this practice are SIEM, device and application vulnerability management, threat analytics, and automation and orchestration platforms. Mr. Kissel affectively covers the processes that security operation center (SOC) analysts employ to monitor, detect, remediate, and mitigate threat actors attempting to attack a network within a security and vulnerability management and security analytics paradigm.

More about Chris Kissel

Message from the Sponsor

MANDIANT®
YOUR CYBERSECURITY ADVANTAGE

Mandiant is on a mission to make every organization secure from cyber threats and confident in their readiness.

We deliver dynamic cyber defense solutions powered by industry-leading expertise, intelligence, and innovative technology.

Learn more about Mandiant Security Validation: Validate and continuously measure the effectiveness of your cyber security controls against active and relevant cyber threats. With intelligence-led security validation, identify gaps, misconfigurations, and opportunities for improvement within your security program. Security Validation done right yields quantifiable evidence required to optimize your cyber defenses, prove security effectiveness and the value of your security investments.

To learn more, visit Mandiant

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC

@idc @idc idc.com