The Importance of Practical Testing in Today's Cybersecurity Landscape

GIAC Certifications

December 2021

Executive Summary

Real-world scenarios are the future of cybersecurity certification programs, proving a cybersecurity practitioner's ability to defend enterprises against increasingly sophisticated cyberattacks and exploits that target specific vulnerabilities.

Practical testing needs to be a critical component of cybersecurity certifications given that major data breaches continue to impact companies of all sizes and sectors. Malicious nation-state adversaries continue to probe and attack the networks of government organizations and private sector enterprises responsible for critical infrastructures, such as financial services, oil and gas production, and utilities.

The COVID-19 pandemic also continues to present businesses across the globe with cybersecurity challenges, including opportunistic phishing campaigns, discontinuity of information security operations, and long-term financial constraints, according to the Accenture Security 2021 Cyber Threatscape Report.

GIAC, known for providing the highest standard in cybersecurity certifications, recognized that companies, government agencies, and educational institutions need cybersecurity professionals with the technical, hands-on skills to defend our nation's networks and critical infrastructure from all forms of threats. **To meet this need, GIAC raised the bar for cybersecurity certifications even higher with CyberLive – hands-on, real-world practical testing.**

The demand for practical testing is growing among both cybersecurity professionals and hiring managers. Practitioners need discipline-specific certifications with practical testing to enhance their ability to build and maintain a strong career path, with increased opportunities for new responsibilities and better pay. Companies need a way to confirm that the cybersecurity professionals they hire have the necessary knowledge and abilities to protect their organizations from existing and emerging attacks. The need for practical testing has never been greater.

Attacks Are More Damaging Than Ever

Cyberattacks are becoming increasingly more targeted, more damaging, and more elusive.

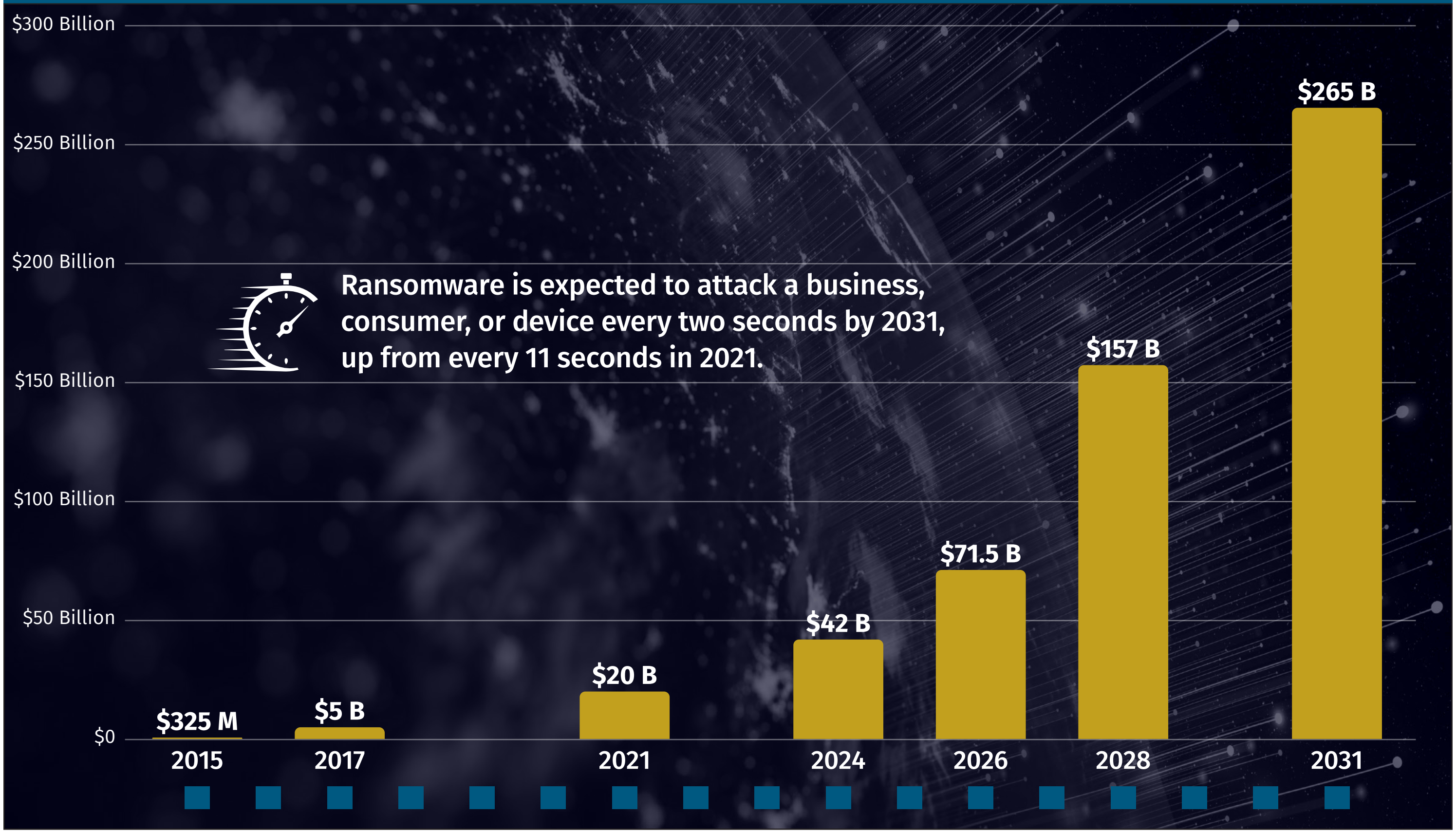
Although a digitally connected world is ushering in an era of efficiency and innovation, this virtually connected world is opening new avenues for adversaries to exploit vulnerabilities in networked systems to access enterprises' critical information.

Attackers have time to do significant damage once they access a network, often moving laterally within the network to identify systems with weak or misconfigured security controls.

Given the current threat environment, security practitioners who can assess target networks, systems, and applications to find vulnerabilities—and who can think like an advanced attacker and find significant flaws in systems—are in high demand.

- **61% of businesses reported being hit by ransomware in 2020 and suffered an average of six days of downtime**
- **86 days is the median time between when attackers gain unauthorized access to victim networks and when incidents are first detected**
- **Ransomware will cost its victims more around $265 billion (USD) annually by 2031**

Global Ransomware Damage Costs



Ransomware is expected to attack a business, consumer, or device every two seconds by 2031, up from every 11 seconds in 2021.

SOURCE: CYBERSECURITY VENTURES

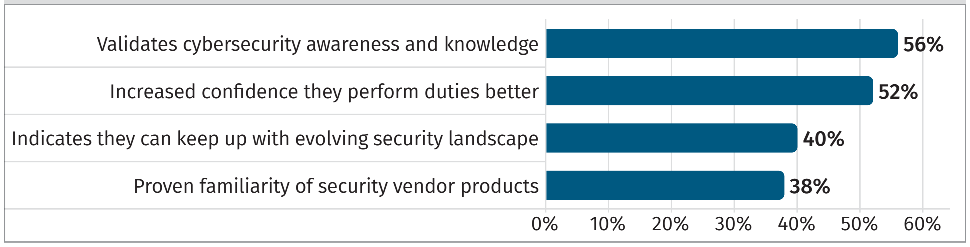
Employers Need Practitioners Who Have Proven Abilities

Keeping organizations secure is critically important, especially in today's threat environment. To address the latest developments in cybercrime, companies need a way to prove that the cybersecurity professionals they hire have the critical knowledge and skills to protect their organizations from all types of attacks.

Certifications—especially those that include a practical testing component—provide confirmation of the skills needed to combat breaches and mitigate threats to the enterprise. Candidates who have successfully earned these credentials are able to add value by helping overcome these challenges faced by organizations today:

- **Securing the enterprise**
  - 73% of organizations had at least one intrusion/breach over the past year that can be partially attributed to a gap in cybersecurity skills. 47% had three or more

Why Employers Prefer a Certified Hire



SOURCE: FORTINET

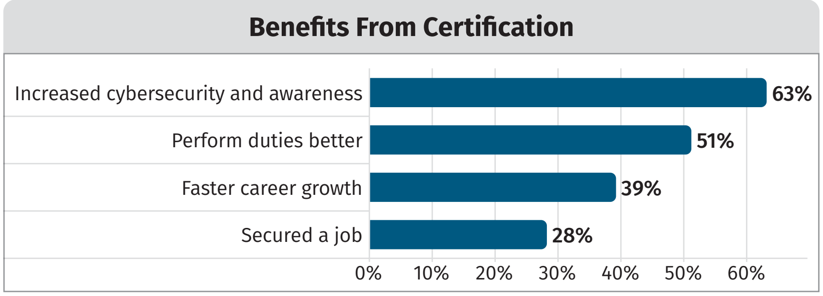
- **Keeping customer data safe**
  - Research shows that 94% of cybersecurity practitioners believe that their certifications have better prepared them for their current role, allowing them to successfully protect their organization's data.
- **Decrease turnover and close the skills gap by hiring the right employees**
  - 68% of organizations reported in a recent survey that their companies struggle to recruit, hire, and retain cybersecurity talent

Practitioners Need Proof They Can Do What They Say They Can Do:

Anyone can claim they have a certain ability or skill. But the only way to back up those assertions is to demonstrate proof. Certifications are that verification of skill. Especially in infosec, **if practitioners have a certification proving they've mastered a specific skillset, both employers and industry peers know that this professional has what it takes.**

Hands-on practical testing, like GIAC's CyberLive, takes this skill verification a step further. Practical testing confirms that certified practitioners could start a new job role and get right to work on day one. The benefits of getting certified are clear:

- **Job security**
  - 82% of organizations prefer hiring candidates with certifications. The right certification could be what gets your foot in the door at almost any enterprise. Certs signal to HR teams and hiring managers that you have the specific job-role skills they need.



SOURCE: FORTINET

- **Career mobility & salary increases**
  - After acquiring certifications in new skill areas, respondents to a recent survey reported a 9 to 16% pay raise
  - Compared to beginner level information technology salaries, those with specialized security skills earn:
    - 10% higher with an intermediate certification
    - 26% higher with an advanced certification
    - 45%+ higher with an expert certification

CyberLive: Adding Value to Traditional Knowledge-Based Testing

In the cybersecurity industry, it's not enough to say you can do something. You have to show you can do it.

Cybersecurity professionals need discipline-specific certifications and practical testing that validates their knowledge and hands-on skills. GIAC recognized this industry-wide need and developed CyberLive—hands-on, real-world practical testing—to fill the gaps in the market.

With nine certification exams featuring CyberLive, and more on the way, GIAC is setting the standard for assessment of real skills in the industry – all with the specialized focus that matters for career development and organizations.

- CyberLive exams include real-world, practical questions in a virtual machine environment
- CyberLive tests the practical application of critically needed infosec abilities
- CyberLive provides a new tool for employers to identify skilled practitioners with key skillsets
- CyberLive skill exams confirm practitioners could start a new job and get right to work on day one – valuable for both the integrity of the employee and their organization

> **"The value of asking multiple-choice questions, while using various cognitive levels, remains valuable and a key tool within exam-performance measurement. The benefit of adding hands-on questions is that it allows a test to better validate that a certification holder has the skills related to that specific certification."**
>
> **—Tommy Adams, a GIAC engineer who helped develop CyberLive**

CyberLive does not replace traditional knowledge-based testing. Instead, it provides a value-add. The practical component of a cybersecurity certification means that a candidate must directly interact with a computer to perform real-world-like tasks in a virtual machine environment. This has practical ramifications, providing both cyber professionals and employers with a measure of the practitioner's real-world abilities.

GIAC's new exam interface enhances the CyberLive experience even further. Rather than switching between the question and virtual machine environment, candidates can now view the exam question while in the VM. This question box overlay can be expanded, hidden, or moved, allowing candidates to prove their skills in an environment customized for how they test best.

The demand for hands-on testing is growing among practitioners, and hiring managers have pushed for the use of practical questions in exams to identify advanced candidates. With CyberLive, GIAC is taking the lead in ensuring that cybersecurity practitioners have the necessary tools to succeed in this challenging landscape.

GIAC Certifications Currently Featuring CyberLive Testing

GXPN: Exploit Researcher and Advanced Penetration Tester (SEC660)

- Network attacks, crypto, network booting, and restricted environments
- Python, Scapy, and fuzzing
- Exploiting Windows and Linux for penetration testers

GCIA: Intrusion Analyst (SEC503)

- Fundamentals of traffic analysis and application protocols
- Open-source IDS: Snort and Zeek
- Network traffic forensics and monitoring

GCIH: Incident Handler (SEC504)

- Incident handling and computer crime investigation
- Computer and network hacker exploits
- Hacker tools (Nmap, Nessus, Metasploit, and Netcat)

GPEN: Penetration Tester (SEC560)

- Comprehensive pen test planning, scoping, and recon
- In-depth scanning and exploitation, post-exploitation, and pivoting
- In-depth password attacks and web app pentesting

GWAPT: Web Application Penetration Tester (SEC542)

- Web application overview, authentication attacks, and configuration testing
- Web application session management, SQL injection attacks, and testing tools
- Cross-site request forgery and scripting, client-injection attack, reconnaissance, and mapping

GCFA: Forensic Analyst (FOR508)

- Advanced incident response and digital forensics
- Memory forensics, timeline analysis, and anti-forensics detection
- Threat hunting and APT intrusion incident response

GSEC: Security Essentials (SEC401)

- Active defense, networking and protocols, and network security
- Incident handling and response, vulnerability scanning and penetration testing
- Windows and Linux security, cryptography, virtualization, and cloud security

GREM: Reverse Engineering Malware (FOR610)

- Analysis of malicious files, analyzing protected executables and web-based malware
- In-depth analysis of malicious browser scripts and malicious executables
- Malware analysis using memory forensics and malware code and behavioral analysis fundamentals
- Windows assembly code concepts for reverse engineering and common Windows malware characteristics in assembly

GNFA: Network Forensic Analyst (FOR572)

- Network architecture, network protocols, and network protocol reverse engineering
- Encryption and encoding; NetFlow analysis and attack visualization; and security event and incident logging
- Network analysis tools and usage, wireless network analysis, and open-source network security proxies

Prove Your Skills by Getting CyberLive Certified Today:
giac.org/cyberlive

Sources

www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-fortinet-survey-skills-shortage.pdf

www.nist.gov/system/files/documents/2018/07/24/nice_value_of_certifications_7.19.18.pdf

https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031

www.accenture.com/us-en/insights/security/cyber-threat-intelligence-report-2021

www.mimecast.com/state-of-email-security

www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report