New Tech: Cyber Ranges, Q3 2019

Forrester's Landscape Overview Of 14 Providers

by Jeff Pollard and Claire O'Malley
July 30, 2019

Why Read This Report

Cyber ranges use a simulated breach environment to prepare your workforce for the stress, panic, and communication barriers they will face during a real cyberattack. In an inevitable cyberattack, how your firm responds will be the difference between permanent brand damage and costly, but short-term, disruption. This report presents a review of the emerging vendors in the cyber range market. Security and risk professionals should use it to understand the capabilities within major market segments and to inform their technology strategies.

Key Takeaways

Cyber Ranges Are A Key Feature In The Incident Response Market

Cyber range capabilities are a crucial feature and capability that the strongest incident response (IR) service providers offer to enhance the value of retainers and improve teams' pre- and post-response activities.

Cyber Range Vendors Are Currently Ahead Of Customer Awareness And Demand

Cyber range vendors are selling more aggressively than their customer bases are buying. The sophisticated capabilities are useful but haven't risen to a must-buy priority for security buyers.

Many Platforms Have Yet To Live Up To The Promise Of An Immersive Experience

Some cyber range offerings are limited to quizzing security practitioners and security leaders on their technical knowledge instead of incorporating the other business stakeholders through a fully immersive breach simulation.

New Tech: Cyber Ranges, Q3 2019

Forrester's Landscape Overview Of 14 Providers

by Jeff Pollard and Claire O'Malley
with Stephanie Balaouras, Christian Austin, Elsa Pikulik, and Peggy Dostie

July 30, 2019

Table Of Contents

Related Research Documents

The Forrester Wave™: Cybersecurity Incident Response Services, Q1 2019

The Forrester Wave™: Global Managed Security Services Providers (MSSPs), Q3 2018

Harden Your Human Firewall

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

All Signs Point To Growth For Cyber Ranges, But It's Early

Many of today's security policies only focus on the proactive measures and technical skills necessary for preventing cyberattacks, instead of preparing the workforce for the stress, panic, and communication barriers they will face during the event. Cyber ranges fill these gaps by creating safe, realistic environments where organizations can test the skills, reactions, and behavior of their incident response team, executives, and security leaders in the event of a cyberattack. Many cyber ranges started as a differentiating feature and capability for IR providers and are now shifting toward a standalone offering. Security teams use these services to:

- **Train in a low-risk crisis scenario.** No one knows how they will react in a high-stress, high-stakes situation until they experience it. Cyber ranges allow security teams, security leaders, and executives to experience the real thing in a protected environment. Running through the exercises reveals strengths and weaknesses that teams can use to further prepare for future cyberattacks, such as role allocation or targeted areas for improvement.
- **Bring all business units together.** Cyberattacks require collaboration from all business units. The security team needs to be able to communicate to business leaders — in non-technical terms — what happened and how much it will cost. They also need to notify the rest of the workforce, as well as any affected customers. If the breach is large enough, journalists could discover it and reach out to employees from any team. Cyber range exercises often include executives from all areas of the business so they can run through the scenarios together and learn what they'll need from each other during a cyberattack.
- **Continuously develop technical security skills.** Cyber ranges also have online training modules that your security practitioners can continually use to improve their skills and assess their knowledge. They also offer red team, blue team, and purple team exercises so your security practitioners can test their abilities in a competitive and fun environment. Many vendors also offer replication capabilities that allow customers to recreate their security environment for enhanced attack simulations.

Established Vendors Are Moving Into The Cyber Range Market

Established vendors see the cyber range market as an opportunity to gain access to client executives and stakeholders with immersive breach response exercises, add value to incident response retainers beyond simple tabletop exercises, and cultivate and shape cybersecurity talent (see Figure 1).

FIGURE 1 New Tech Sample Established Cyber Range Vendors, Q3 2019

SAMPLE ESTABLISHED VENDORS

Booz Allen Hamilton	Booz Allen Hamilton assessments require participants to conduct online research and use open source tools in real time to solve problems, as they would on the job. Kaizen is an additional tool that focuses on developing advanced hunting and "hacker" cyber skills.
Cisco	Cisco Cyber Range offers a cloud-hosted environment that includes more than 50 different attack scenarios and more than 100 applications. It's designed with operations-focused models to assess the methodology, processes, and skills teams need to respond to threats.
IBM	IBM X-Force Command Cyber Range on-premises experiences immerse clients in a simulated fusion center model based on a security operations center (SOC) that can focus on a single participant group or exercise, such as technical operators during a simulated load exercise, or weave an event across multiple areas of the business to emulate way events happen in real life, which can include nonsecurity stakeholders, senior executives, and a firm's board of directors.
Mantech	Mantech Advanced Cyber Range Environment offers both physical and virtual facilities for participants. End-to-end cybertraining includes product evaluations, security architecture testing, individual and collective training, and exercises in a simulated generic or near replica of an existing network.
Palo Alto	Palo Alto Cyber Defense Range and Training Center reproduces realistic environments and features numerous attack types and training simulations. This includes a cyber range structure that uses green, red, blue, yellow, and white teams to fully immerse participants. Currently, Palo Alto offers 6-hour sessions in the US, Europe, and AP.

Four Factors Determine Vendor Maturity

Forrester spoke with our expert analysts and interviewed external subject matter experts in our search for the most important cyber range technologies. We identified nine cyber range technology vendors and differentiated them based on the following four weighted criteria (see Figure 2 and see Figure 3):

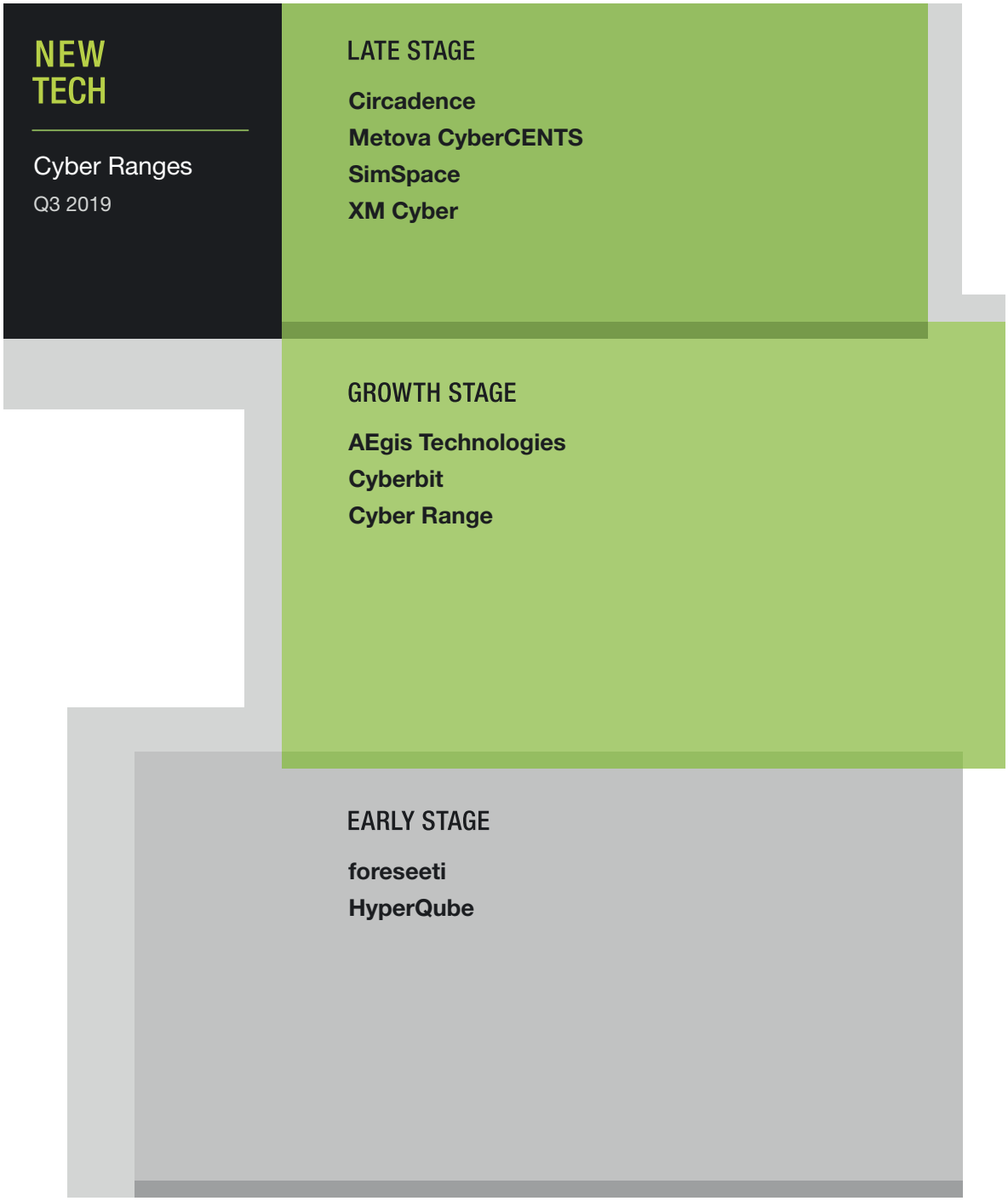
- **Funding level.** This is a measure of how much funding the vendor has raised. Several of the vendors in the space are also privately funded. Funding level demonstrates the financial viability of the startup.
- **Company tenure.** We considered the number of years vendors have been in the market to determine their maturity.
- **Number of employees.** As another part of our measure of maturity, we examined employee headcount for each vendor. We used headcount as a signal of the vendor's presence in the market and its ability to sustain growth.

› **Cyberattack simulation capabilities.** We analyzed the types of cyberattacks available, their deployment options, and all participants who partake in the simulation — individuals or teams — as another criteria to assign maturity.

FIGURE 2 Not-For-Profit Cyber Range Providers

Government	Public sector/academia
Cybersecurity Challenge	Arizona Cyberwarfare
DARPA National Cyber Range	Baltimore Cyberrange
National Cybersecurity Center (UK)	Florida Cyber Hub
	Georgia Cyber Innovation Center
	Michigan Cyber Range
	Virginia Cyber Range
	Wayne State University

FIGURE 3 New Tech Maturity Segments: Cyber Ranges, Q3 2019



Cyber Ranges Offer Exercises For Three Different Stakeholder Groups

We identified the following functionality segments, each with varying capabilities (see Figure 4):

- **Security practitioner.** The cyber ranges in this category focus on use cases most relevant for existing and new security practitioners. Exercises emphasize security operations, forensics, and incident response skills, and mainly seek to improve how security practitioners use commercial and open source technologies.
- **Security leader.** Cyber ranges in this category focus on use cases most relevant for security leaders. Exercises emphasize the overall execution of security processes, governance, and oversight of how the security team would behave when confronted by a large-scale, highly damaging security incident involving various areas of the security and IT team.
- **Executive team.** Cyber ranges in this category focus on use cases most relevant for senior security leaders and non-security senior stakeholders. Exercises include crisis management activities that simulate the fallout and implications of a major cybersecurity-related catastrophe that involves reputational, legal, and regulatory damage and provides insights into how the organization would fare based on its planned response procedures.

FIGURE 4 New Tech Functionality Segments: Cyber Ranges, Q3 2019

Vendor Snapshots In The Cyber Range Marketplace

The following tables provide an overview of vendors that includes primary functionality, geography, vertical focus, and sample customers. You can use them to help inform your understanding of the market and to shortlist vendors (see Figure 5, see Figure 6, and see Figure 7). The cyber range marketplace also includes non-commercial organizations that provide cyber range services to governments, students in training, and other community members that are interested in developing these skills at an affordable cost or even for free.

FIGURE 5 New Tech Late-Stage Cyber Range Vendors, Q3 2019

LATE STAGE

	Primary functionality	Geographic presence	Vertical market focus (top three)	Sample customers
Circadence	Security leader	NA 90%; EMEA 8%; AP 1%	Government; education; financial services	Dairyland Power Cooperative; Loudon County Public Schools; University of Colorado, Boulder
Metova CyberCENTS	Security leader	NA 80%; EMEA 15%; AP 5%	Defense; academia; public sector	Vendor did not disclose
SimSpace	Executive team	NA 100%	Financial services; defense	Vendor did not disclose
XM Cyber	Security leader	NA 75%; EMEA 25%	Manufacturing; critical infrastructure; financial services	Vendor did not disclose

FIGURE 6 New Tech Growth-Stage Cyber Range Vendors, Q3 2019

GROWTH STAGE

	Primary functionality	Geographic presence	Vertical market focus (top three)	Sample customers
AEgis Technologies	Security practitioner	NA 100%*	Defense	Vendor did not disclose
Cyberbit	Security practitioner	NA 50%; EMEA 50%*	Higher education; critical infrastructure; defense	Vendor did not disclose
Cyber Range	Security practitioner	NA 75%; EMEA 25%*	Financial services; manufacturing; defense	Vendor did not disclose

*The vendor did not provide information for this cell; this is Forrester's estimate.

FIGURE 7 New Tech Early-Stage Cyber Range Vendors, Q3 2019

EARLY STAGE

	Primary functionality	Geographic presence	Vertical market focus (top three)	Sample customers
foreseeti	Security leader	NA 25%; EMEA 75%	Critical infrastructure; finance; military	Klarna; Scania; Swedavia Airports
HyperQube	Security leader	NA 100%	Enterprise; education; defense	DHS; Marymount; St. Bonaventure University

What It Means

Cyber Ranges Are Transforming Security's Reputation

The security team has long been kept in isolation and hidden from the rest of the organization — only brought out when disaster strikes or the C-suite wants assurance that they're shielded from the most recent breach to hit the news. However, the elusiveness of the security team creates the false impression that cyberattacks are their responsibility and must be handled by them alone. Responding to and recovering from cyberattacks require collaboration from all parts of the business, and cyber ranges are de-isolating the security team by allowing them to run through drills with their necessary counterparts, such as representatives from risk, legal, HR, communications, and other executives. As more and more business leaders and senior executives take part in these simulations side by side with their security leaders, they will finally come to recognize the security team as trusted risk advisors critical to the organization's digital transformation.

Supplemental Material

Methodology

To determine the segmentation of vendors by maturity (Late Stage, Growth Stage, Early Stage), we took the range of four criteria across the spread of all vendors that were evaluated — funding levels, company tenure, number of customers, number of employees — and divided each criterion into three tiers of maturity. We then used custom weightings that we distributed across all four criteria using the analyst's best judgment based on suitability to the market to reach a total of 100%. From there, we scored vendors against all criteria using progressive point values across maturity stages and divided them into three final groups of Late-Stage, Growth-Stage, and Early-Stage vendors.

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Cisco

HyperQube

IBM

Metova CyberCENTS

SimSpace

Virginia Cyber Range

XM Cyber

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

149338