Team8 2023 Cyber Themes

2023 Cyber Themes

Theme	Drivers	Impact	Select Providers
01 **Cloud Security** 	Buoyed by tailwinds from the pandemic and digital transformation, cloud adoption is experiencing a meteoric rise, and enterprise cloud migrations are expanding from small, low-risk applications and experiments to business critical initiatives. As such, security capabilities are evolving to allow enterprises to reap the benefits of moving to the cloud, while retaining control over their security posture, data protection programs, and application integrity.	• Many companies, especially smaller ones, tend to use a single cloud plus SaaS strategy • More sophisticated and/or mid-to-larger companies tend to think about multi-cloud for several reasons: for technical resilience, to prevent vendor lock-in, and for specialization of features. • In order for cloud provider-based security solutions to be successful, the cloud providers themselves are going to have to be able to support their customers' hybrid & multi-cloud environments.	paloalto NETWORKS, Gem, aqua, CHECK POINT, orca security, WIZ, netskope, Lacework
02 **Resilience & Recovery** 	In a world in which digital infrastructure is now business-critical infrastructure, cybersecurity cannot afford to stop at "identify, protect, detect, and respond". Any sound security strategy must also consider resiliency and include the capability for rapid recovery from degradation, disruption, or denial of access to enterprise systems or data, and swift reconstitution of assets and capabilities.	• When thinking about resilience and recovery, cybersecurity must primarily focus on operational risk and resilience, i.e. the risk to business processes, including the underlying data and IT systems. • Standard continuity of business processes are insufficient in the face of malicious cybersecurity action.	COMMVAULT, semperis, Own{backup}, rubrik, NetApp, COHESITY
03 **Smarter Security** 	Cybersecurity is becoming highly complex and is becoming difficult and expensive to manage. At the same time, there is also a shortage of cybersecurity talent while, simultaneously, adversaries are increasingly leveraging sophisticated attack capabilities. All of this stretches response capabilities. Smarter security solutions will mitigate many of these challenges through the incorporation of automation, data, and AI to plug gaps and provide security teams with better options to best-use their human capital.	• Because of both the supply problem (lack of talent) and the demand problem (dramatic increase in volume/speed of attacks and AI-driven attacks), there may be no alternative other than automation and AI-supported defense.	paloalto NETWORKS, DATADOG, tufin, splunk>, exabeam, VULCAN, CYWARE, Cynet

TEAM8

2023 Cyber Themes

Theme	Drivers	Impact	Select Providers
04 **Security of Things** 	The growth of the Internet of Things (IoT) is driving digitization and unlocking business value. But Security of Things requires that every connected device or network - each with its own identifier and ability to transfer or process data - must be protected. Each of these devices acts as a potential breach-point into an organization or to private data, which increases overall risk exponentially.	• In the context of industrial IoT, there are concerns regarding the resiliency of critical infrastructure, and unfortunately, much of this infrastructure is decades old and difficult to secure. • In general, there continues to be a massive acceleration in the number and variety of IoT devices, creating new categories of attack that need to be planned for in order to protect individuals, data, and enterprises.	CLAROTY, ARMIS, TANIUM, cybereason, FORESCOUT, CROWDSTRIKE, SOPHOS, deepinstinct, SentinelOne
05 **Perimeterless World** 	The enterprise perimeter is nearly obsolete, and the dramatic shift to remote work during the pandemic is accelerating its demise. This requires enhanced processes for identity and access management (IAM), with a growing use of zero trust architectures that provide better control.	• In the modern environment, there are many things outside of the network that still need to be trusted and depended upon. • Thus, using network topology as the basis for trust simply isn't a valid assumption any more, and that's where identity comes into play.	paloalto NETWORKS, AKEYLESS, CATO NETWORKS, monogoto, TALON, zscaler, SECRET DOUBLE OCTOPUS, SILVERFORT, okta, perimeter 81
06 **Data Security** 	On one hand, globalization and the growth of the digital economy are accelerating the need for digital collaboration. On the other, emerging privacy regulations and consumer preferences are driving investment in privacy-enhancing technologies and the means for users to have more control over their data. The net result of these colliding forces will be new data protection- and privacy-driven strategies that impact underlying architectural design and business processes. The need to mitigate data breaches is also driving more data security and privacy regulation.	• Data is at the heart of everything in the modern corporation, with concerns focused on confidentiality, data integrity, and data availability. • While the focus has previously been on confidentiality, today there is an increased focus on availability. Integrity of data will be the last frontier for data security considerations.	Duality, VARONIS, BigID, OneTrust, Dig Security, PIANO, VERY GOOD SECURITY, inpher

TEAM8™

2023 Cyber Themes

Theme	Drivers	Impact	Select Providers
07 **Shift-Left** 	Developing and managing software is more agile and faster than ever. However, developers currently have neither the expertise nor the tools to handle the security issues while the security team doesn't have the staff to cover the gap. Cybersecurity needs to be shifted-left in the application development process to ensure that security considerations are embedded from the start.	• If Shift-Left works, the biggest impact will be that it enhances the relationship between security and AppDev, which will enable the faster creation of secure applications. • However, in order for Shift-Left to work, security has to adapt to the way developers think, act, buy, and consume tools. • Additionally, with the emerging focus on the "software bill of materials" (SBOM), the ability for software creators to track application componentry and provide evidence to their customers will be critical.	ox security, Secure Code Warrior, Checkmarx, apiiro, aqua, tenable, snyk, MEND, paloalto NETWORKS
08 **Layer 8** 	No matter how much money a company invests in security controls, humans will always defeat them. A good red team always wins because the one thing that they can rely on is human weakness. Layer 8 is all about how we train humans, how we empower them, how we monitor them, or in certain instances, how we take them out of the loop.	• A common first entry point of an attacker to an organization is usually a human (employee), who can easily be compromised by malicious software, social engineering techniques, or simply by human error. • Compromised employees allow attackers to bypass significant portions of companies' defensive controls, and these humans cannot be "patched". • Thus, the human attack surface can only be mitigated by compensating controls.	IRONSCALES SAFER TOGETHER, mimecast, proofpoint, KnowBe4 Human error. Conquered., IMMERSIVELABS

Team8 Disclosure

This 2023 Cyber Themes infographic represents the opinions of Team8 Labs Inc. (“Team8”) and is for informational purposes only. You should not treat any opinion expressed by Team8 as a specific inducement to make an investment in any security, but only as an expression of Team8’s opinions. Team8’s statements and opinions are subject to change without notice. Team8 is not registered as an investment adviser under the Investment Advisers Act of 1940, as amended (the “Advisers Act”), and relies upon the “publishers’ exclusion” from the definition of investment adviser under Section 202(a)(11) of the Advisers Act. As such, the information contained in this 2023 Cyber Themes infographic does not take into account any particular investment objectives, financial situation or needs and is not intended to be, and should not be construed in any manner whatsoever as, personalized investment advice. The information in this 2023 Cyber Themes infographic is provided for informational and discussion purposes only and is not intended to be, and shall not be regarded or construed as, a recommendation for a transaction or investment or financial, tax, investment or other advice of any kind by Team8. You should determine on your own whether you agree with the information contained in this 2023 Cyber Themes infographic. Certain of the securities referenced in this Team8’s 2023 Cyber Themes infographic may currently, or from time to time, be constituents of an index developed and maintained by WisdomTree Investments, Inc. using data provided by Team8, which has been or will be licensed for a fee to one or more investment funds. In addition, certain officers or employees of Team8 or funds or other persons or entities affiliated or associated with Team8 may hold shares of, be officers or directors of, or otherwise be associated with some or all of the issuers of the securities referenced in this 2023 Cyber Themes infographic or included in such index. Team8 expressly disclaims all liability with respect to any act or omission taken based on, and makes no warranty or representation regarding, any of the information included in this 2023 Cyber Themes infographic.

TEAM8™