Continuous Cyber Attacks: Building the Next-Gen Infrastructure for the New Normal

Executive Summary

High performance. Delivered.
An organization’s digital infrastructure can be critical in blunting cyber attacks, but maintaining its effectiveness can be challenging. Leaders have a variety of choices amongst tools and technology solutions and they must evaluate those options against prioritized business needs.

Organizations should take a comprehensive view of digital security, integrating cyber defense considerations deeply into the enterprise environment. Building a next-generation security infrastructure should accomplish the following:

- Provide greater information visibility, context and meaning regarding security events.
- Give technical analysts the ability to understand the impact of security events in relation to business operations.
- Offer flexible and open access to data and features.
- Drive deeper integration levels for security infrastructure with the rest of the business.
- Leverage automation for faster response times and scalability.

Actions that can be taken to develop such an architecture:

**Create the self-defending enterprise,** which can deliver a quantum leap in performance. A self-defending IT infrastructure knows when and where it needs extra capacity, identifies issues and automatically fixes them and takes steps to optimize services.

**Focus attention on technology maturity,** evaluating technology that increases visibility into behaviors within the organization. This can promote security based on business context and not just technical terms.

**Align threat intelligence with the business environment** to monitor infrastructure behavior and help ensure that security remains up-to-date.

**Implement deceptions to trap intruders,** such as setting up false data sets or dummy passwords. When attackers follow these false leads, organizations can learn about the adversaries and limit the effectiveness of an attack.

**Leverage automation,** which can save on costs and increase agility of the security team. Automation can help disrupt an attack, and it also allows security staff to focus on more challenging issues.

**Feed the analytics engines,** using tools to help understand where threats originate and how well an organization’s defenses are working. Advanced analytics can help identify subtle threats, based on shifting behaviors in networks and devices, so security teams can proactively protect potential targets.

Experience shows that many organizations are siloed with respect to infrastructure, which limits the benefits that can be realized from tools or technology investments. More effective organizations view tool purchases as opportunities to replace multiple older technologies with a single newer one.

Building a strong cyber defense goes hand in hand with achieving operational excellence in security. Steps that support this type of improvement include:

**Experiment:** Pilot new security technologies and automation solutions, develop use cases and simulate sophisticated attacks.

**Create cross-functional teams:** Instead of having separate groups managing the network, the servers and security, organize these experts so they can interact, collaborate and increase the effectiveness of security automation.

**Team to develop talent:** Help staff become specialists, while ensuring that the business, infrastructure and security teams know about all projects so they can benefit from each other’s innovations.

**Raise security’s internal profile:** Make sure the chief information security officer’s level of influence over the infrastructure is commensurate with that of the IT leader.

Organizations looking to build a more effective next-generation security infrastructure should adopt a comprehensive view into their infrastructure security requirements. Look beyond tools and invest only in technology with proven performance. Work across business units, IT and security to maintain alignment with organizational goals and readiness to respond to cyber attacks.
About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 373,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

DISCLAIMER: This document is intended for general informational purposes only and does not take into account the reader’s specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.