

www.active-bytes.com



CYBERSECURITY SERVICES

Who We Are

BUILDING CYBER-RESILIENT ORGANIZATIONS

ActiveBytes Innovations has a proven track record of executing successful Information Security Projects for numerous large enterprises across different locations around the globe.

We proudly serve clients from multiple industry sectors, demonstrating our ability to adapt and provide tailored solutions to diverse business environments. Here are a few notable examples showcasing our expertise across various industries:





Safeguarding Diverse Industry Sectors With State of the Art Managed Security Service



Financial



Banking



Government



Oil & Gas



Real Estate & Hospitality



Logistics & Supply Chain



Healthcare



Aviation

TRANSFORMING CYBER DEFENCE WITH OUR UNIQUE APPROACH

We lead in cybersecurity with an unmatched approach to security operations, providing comprehensive support beyond periodic reports and alerts. True peace of mind for organizations, knowing their security matters are in capable hands.



ActiveBytes Innovation: Transforming Security Operations

Our unique approach provides comprehensive services, delivering practical insights into incidents and a well-rounded perspective tailored to your organization's needs.



State of the art Technologies for Optimum Security

Utilizing state-of-the-art products built upon powerful open-source solutions, our Analytical Engine offers robust reporting, alerting, and log enrichment. Compatibility across log formats and machine learning-powered anomaly detection ensures faster search and response times.



Our Unique Formula: Effective Outcome-Based Approach

Drawing from extensive cybersecurity experience, our formula maximizes automation and accuracy. Focusing on real incidents, we minimize false positives, aligning risk priorities with your organization's goals.



Outstanding support and personalized services

Understanding your unique needs, we offer services like real incident reporting, ongoing security assessments, expert audit assistance, dark web breach monitoring, vendor security verification, and prioritized vulnerability lists.



OUR EXTRAORDINARY TEAM OF CYBERSECURITY EXPERTS!

- Cybersecurity experts with deep technical knowledge
- Industry-recognized security-certified team for new confidence and protection



OUR RANGE OF SERVICES



IT Security Service:

ActiveBytes Innovations delivers comprehensive IT Security solutions, including risk assessment, threat detection, and incident response, safeguarding clients' digital assets and ensuring business continuity.



Risk:

Our Risk services proactively identify and manage security threats through comprehensive risk assessments, threat intelligence, and robust incident response strategies for secure infrastructure and data protection.



Compliance:

ActiveBytes Innovations' Compliance services help clients meet regulatory requirements, manage data protection, privacy, and incident response, ensuring a strong security posture and continuous improvement.



Managed Security Services:

Our MSOC is your cybersecurity ally, providing constant threat detection, swift incident response, and cutting-edge CTI. We excel in proactive threat hunting, vigilant security monitoring, robust vulnerability management, and user-friendly endpoint protection. Tailored solutions ensure resilience against evolving threats, fortifying your organization with a personalized touch for proactive cybersecurity.



Governance:

ActiveBytes Innovations' Governance services establish effective security management, compliance with regulations, and swift incident response, safeguarding digital assets and ensuring exceptional results



Active Sense Awareness:

Immerse your team in real-world cybersecurity scenarios with our training platform. Through simulations, exercises, and hands-on training, we elevate your organization's preparedness for cyber threats. Experience the practical side of cybersecurity, ensuring your teams are adept at handling evolving challenges and enhancing their skills to safeguard your organization effectively.



CYBOT - Threat Management Platform

CYBOT, our Threat Management Platform, is an essential cybersecurity service designed to enhance your defense strategies. This user-friendly platform utilizes advanced technology to detect and neutralize threats in real time. Offering simplicity in threat detection and management, it provides actionable insights for swift response.

CYBERSECURITY SERVICES

Based on our extensive experience in the domain of cybersecurity and our deep understanding of the varied security needs across organizations of different maturity levels, we have devised a unique method of categorization.

This method considers the specific cybersecurity services required by organizations at varying stages of maturity. By tailoring our approach to the unique needs and capabilities of each organization, we ensure that our cybersecurity solutions are not only effective but also aligned with their strategic goals and objectives.

This approach allows us to provide targeted and customized services that address the distinct challenges and requirements faced by organizations at different levels of maturity, ultimately enhancing their overall security posture and resilience against cyber threats.



Preparation



Evaluation



Continues
Monitoring and
Improvement



Emergency
Response Services



PREPARATION

Our preparation services assist organizations in establishing their cyber defence strategy and implementing security infrastructure. We provide tailored guidance to ensure a solid foundation for cybersecurity resilience.

Current State Security Assessment

Organization Information Security Current State compared against best practices and industry standards and defined Maturity Ratings and Risk Ratings for each of domain areas

Security Architecture Review

~Identification of the effectiveness of We provide Security Architecture Review services to organizations, conducting thorough assessments of their security setups to identify vulnerabilities and enhance overall protection.

Threat Modeling

Our service begins by thoroughly identifying the threat environment, applications, architecture, and technology utilized within your system. We then define system trust boundaries and analyze data flows to understand potential vulnerabilities. Through comprehensive threat analyses, we provide tailored countermeasures to mitigate risks effectively, ensuring the security and integrity of your systems and data.

EVALUATION

For organizations seeking to assess their cyber resilience and readiness, our evaluation services offer comprehensive analyses. We identify vulnerabilities, measure preparedness, and provide actionable insights for improvement.

Wireless Penetration Testing

We specialize in uncovering and fortifying your network's vulnerabilities. We identify unauthorized wireless access points, capture handshakes, and break encryption methods to bolster your security. Our detailed reporting offers actionable insights and mitigation strategies, ensuring your network stays protected against evolving threats.

Security configuration Assessment

With a foundation in proven methodology and industry-leading practices, we meticulously examine your network, servers, databases, and applications. Our focus is on identifying potential configuration issues to ensure robust security. Our reporting provides concise findings and actionable recommendations, empowering you to optimize your systems for enhanced performance and resilience.

Red & Purple team activities

We specialize in identifying and addressing various cyber attack vectors, including social engineering, network vulnerabilities, physical breaches, and application flaws. Our expertise covers tactics like convincing phishing attempts, exploiting misconfigured networks, breaching physical facilities, and targeting web application vulnerabilities such as cross-site scripting and SQL injection.

OSINT Threat Exposure Assessment

Gain comprehensive insight into your assets and domains' entire internet footprint with our services. We meticulously analyze the volume and nature of open-source information to assess potential risks of profiling and exploitation of key figures within your organization. By understanding the extent of information available to malicious actors, we provide tailored recommendations that outline the expected manpower and implementation costs, ensuring proactive measures to safeguard your business and key employees from potential threats.

Penetration Testing

Our penetration testing service at ActiveBytes follows a structured approach to ensure thorough assessment and analysis of target systems. Beginning with reconnaissance, we actively and passively gather essential information about the target. During the discovery phase, we meticulously identify vulnerabilities using both automated and manual processes. When it comes to exploitation, our team employs a blend of manual techniques and automated tools to launch exploits based on the vulnerabilities uncovered. Finally, in the analysis and reporting phase, we develop comprehensive reports detailing the findings and interpretations of the test results. With our systematic approach, we provide actionable insights to enhance the security posture of your systems.

Attack Surface Mapping and Monitoring

Our service offers continuous discovery and tracking of assets, applications, and devices within your expanding digital footprint. By providing real-time insights into your current risk exposure, you can swiftly prioritize high-risk assets and implement effective risk mitigation strategies. With our solution, you gain proactive control over your cybersecurity posture, ensuring robust protection against evolving threats.

CONTINUES MONITORING AND IMPROVEMENT

Our continuous monitoring services provide real-time vigilance against evolving cyber threats. We collaborate closely with your team to actively safeguard digital assets through ongoing monitoring and engagement. This proactive approach helps detect and address threats promptly, enhancing overall cybersecurity resilience.

Active Application Security Testing

Our rigorous security assessment cycle ensures that any new or modified applications undergo thorough evaluation before being approved for publication. There are no limits to the number of assessment requests, and our process is customized to align with organizational policies and development cycles. We prioritize a DevSecOps approach, focusing not only on reporting vulnerabilities but also on actively addressing and fixing issues. The process begins with the completion of a new application by the development team, followed by a request for assessment. Our team conducts security assessments and provides detailed reporting. Any findings are promptly mitigated and revalidated. Only upon successful mitigation of all findings, or acceptance of associated risks by the business, is approval granted for publication. This ensures that applications meet stringent security standards and minimize potential risks.

Active Vulnerability Management

Our post-publish application security assessment protocol ensures ongoing protection for all published applications. Monthly security scans are conducted to detect any changes or accidental exposures, with a focus on monitoring for potential vulnerabilities. We evaluate perimeter device controls such as SSL and WAF, intervening only in the event of new findings to minimize IT efforts. The process includes monthly application security scans using Dynamic Application Security Testing (DAST) techniques, followed by comprehensive evaluation of results and reporting. Any actionable findings are promptly addressed, ensuring continuous security maintenance and mitigation of potential risks.

Managed Security Operations Center (MSOC)

Active Bytes offers a comprehensive 24/7 Threat Detection and Response Service with over 500 SIEM and XDR use cases, including specialized monitoring for the banking sector with ATM monitoring, honeypot, and DMZ monitoring.

Our service includes automated alert investigation and rapid threat mitigations. Additionally, we provide User and Entity Behavior Analytics (UEBA) monitoring, threat hunting, compliance reporting, and threat intelligence services. Our Managed SOC Service features CYBOT, a threat management platform with native SIEM and XDR capabilities, eliminating the need for additional tools or software solutions.

With unlimited log collection, custom application log collection, and no EPS-based license, our service ensures comprehensive coverage without additional professional service costs for implementation. We provide one year of free professional service, daily, weekly, and monthly SOC reports, and dedicated communication channels with our SOC team. Plus, we offer free credits for additional services, ensuring proactive and efficient security operations.



EMERGENCY RESPONSE SERVICES

In times of crisis, our emergency services provide swift support and remediation. Our expert team stands ready to assist organizations in mitigating the impact of cybersecurity incidents and restoring normal operations promptly.

Malware Analysis

Our malware analysis service offers comprehensive protection by identifying and assessing assets and data vulnerable to the latest malware threats. Using dynamic and static analyses, we reverse-engineer malware to understand its composition and behavior. We specialize in memory malware analysis, identifying indicators of compromise and recommending eradication steps to mitigate risks effectively. Our customized reports provide detailed insights into the nature of the malware, empowering organizations to enhance their security measures and safeguard their assets and data.

Cyber Forensics

We swiftly identify compromised elements in your IT infrastructure, isolate them, and preserve data evidence for forensic analysis.

Cyber Emergency Response

Our Incident Response (IR) plan and methodology are crafted to assist companies in all aspects of handling network security incidents. The primary objectives include minimizing damage, protecting data, and facilitating swift recovery for the organization following an incident.



Threat Hunting Services

Our threat hunting methodology encompasses three approaches: hypothesis-driven investigations, investigation based on known Indicators of Compromise or Indicators of Attack (IOCs/IoAs), and advanced analytics with machine learning.

Hypothesis-driven investigations leverage insights from new threats identified through extensive attack data, aiming to detect corresponding behaviors within the organization's environment. Investigation based on IOCs/IoAs utilizes tactical threat intelligence to uncover hidden attacks triggered by known indicators. Advanced analytics and machine learning analyze vast datasets to identify anomalies indicative of potential malicious activity, leading to the discovery of stealthy threats.

Security Advisory Services

Our highly tailored service involves expert review of each new security issue within the customer's context. Our advisory covers the issue's impact, customer defenses, permanent fixes, impact assessment, and incident response actions.

Threat Intelligence Services

We assist organizations in enhancing their preparedness and preventing potential threats from causing irreparable harm. Our threat intelligence service gathers data from various sources, monitored by our experts and automated tools. Combining human expertise with AI analysis, we transform this raw data into curated threat intelligence feeds. These feeds empower security teams and platforms with actionable insights to proactively defend against targeted threats.

Notice

This document contains information about the proprietary property of ActiveBytes Innovations. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of ActiveBytes Innovations.

Nothing in this document constitutes a guarantee, warranty, or license, express or implied. ActiveBytes Innovations disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to Fitness for a particular purpose; merchantability; not infringement of intellectual property or other rights of any third party or of ActiveBytes Innovations; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technology discussed herein and is advised to seek the advice of competent legal counsel, without obligation of ActiveBytes Innovations.

ActiveBytes Innovations retains the right to make changes to this document at any time, without notice. ActiveBytes Innovations makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein.

Copyright

Copyright © ActiveBytes Innovations Information Technology Network LLC

Trademarks

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owner's benefit, without any intent to infringe.

Contact Us

ActiveBytes Innovations

Sharjah Media City, Sharjah, UAE, Dubai, UAE +971 505676727
www.active-bytes.com