KONTEX

Microsoft
Adversary Emulation Services

advisory@kontex.com

KONTEX

Where Security Meets Quality

Formed in 2015, Kontex has become a trusted supplier for Information Security Advisory Services and Security Technologies to organisations around the world.

Our approach emphasises providing the highest quality of service delivery from a skilled and personable team of security experts who care about your needs from the top down.

Why Adversary Emulation is Essential

Most well-known offensive security assessments today are heavily focused on pre-compromise. Organisations use "red teams" to evaluate their assets with vulnerability assessments and penetration tests, simulating a sophisticated attack as realistically as possible. It is a defensive exercise, as well as a way to get a view of the exploitable attack surface of the organisation and a method to identify gaps in defence.

These tests, however, provide actionable data only on how to remediate vulnerabilities in a certain subset of assets. Consequently, the tester can spend only a limited amount of time executing post-compromise actions, such as data exfiltration and credential dumping, meaning that the exploration of the defensive capability is limited in scope, breadth and depth.

What's more, few organisations can measure, assess or prove the ability of their cyber security controls (endpoint, proxy, SIEM, etc.) to safeguard against attackers that have already gained access. This activity is often more relevant and related to the actual goal of an attack. After all, the objective of an attacker is generally not to exploit a vulnerability or successfully social engineer a password, but rather to steal data and information or disrupt business-critical services.

Vulnerability management, penetration testing and red teaming are key exercises, but it's critical to consider **adversary emulation** at both technical and behavioural levels to ensure highly effective post-compromise resilience.

Failure to Detect Attacks, Ineffective Security Controls and Security Gaps

Attackers can go undetected for long periods of time, so organisations need to continuously test their security team's ability to detect and respond to today's sophisticated, targeted attacks. Secondly, organisations need to validate that their current security controls and processes are effective against today's evolving adversary Tactics, Techniques and Procedures (TTPs). Finally, you need to identify gaps in your current security posture to understand how an attacker may breach your network.

Microsoft Adversary Emulation Service

Maturing Security Through Emulation

A real cyberattack incorporates multiple chained techniques; therefore, and effective adversary emulation must simulate realistic behaviour that either resembles or is inspired by attacks that have been observed "in the wild".

Kontex's Adversary Emulation solution empowers Red and Blue Team members so that organisations can enhance their threat mitigation processes and extend the value of their current technology purchases. Unlike technology-focused simulation tools and vendor driven engagements that walk security teams through the same, automated steps, Kontex's approach is a fully-customisable emulation solution aligned with the attack campaigns that matter today.

Our solution has been designed to empower your security teams with our easy-to-use, real-world emulations. You will be able leverage contextual business risk so that your Blue Teams can prioritise their vulnerability remediation activities by using real-world TTPs for a proactive approach to threat response and mitigation activities.

Our customisable capabilities will empower Red Team members and Blue Team members of all skill levels to run multiple campaigns at once. By reducing the time it takes to build a campaign, you can test against new and evolving threats found "in the wild," including ransomware and privilege escalation attacks.

Enhance Your Processes By Building Kontex Into Your Cybersecurity Workflow

We map all emulation behaviours to MITRE ATT&CK and fully integrate with Atomic Red Team to enhance reporting. With us, you will be able to create more robust detection and response processes by tracking what happened in your environment.

Our priority is to extend the value of your current tools by taking the information from your emulations to modify security tool configurations and parameters. We will enable you to maximise your return on security tool investment by moving beyond default configurations to reduce alert fatigue and enhance detection.

Microsoft Adversary Emulation Service

Enable Better Metrics and Drive Improvement

A primary goal of using emulations is to enhance your security posture. When setting metrics around your detection and response solutions effectiveness, our service will enable you to answer the following questions:

Logging: Is your Blue Team getting more effective data from your security tools?

Alerting: Is your Blue Teams reviewing fewer false positives?

Detection: Is your Blue Team detecting threats faster?

Business Terms: Are you able to incorporate your metrics into Board of Director reports to help prove governance?

Breakout Time: Can you establish baseline metrics that capture for continuous improvement of people, process, and technology: detect, respond, and remediate?

Contextual Business Risk: Is your security team's ability to mitigate threats better than your industry's average?

Continuous Insight: Are your teams consistently identifying and remediating vulnerabilities for continuous iteration and insights?

Key Benefits

TEST YOUR RESPONSE TO TARGETED ATTACKS

An Adversary Emulation Exercise allows your organisation to test your security team against the latest threats posing the greatest risk to your industry.

TEST THE EFFECTIVENESS OF SECURITY CONTROLS

A focus on objective-based testing demonstrates the effectiveness of your security controls and incident response processes.

EVALUATE YOUR MATURITY LEVEL

Measure your organisation's cybersecurity maturity level by evaluating it across the phases of the MITRE ATT&CK framework.

Proven Track Record

We support businesses across a range of technologies and industries, including some of the largest organisations in the world. A selection of our experience is outlined below.

Life Sciences

Our team of analysts provide implementation support, incident monitoring, and operational support across a range of security technologies spanning:

- Endpoint Security;
- Data Loss Prevention;
- Patch Management;
- Web Proxy; &
- SIEM.

Our client has 15,000 employees globally across 50+ locations.

Construction & Manufacturing

We mobilised a team of SOC engineers to provide on-premise support to implement a new endpoint security technology and to on-board users from over 20 disparate subsidiaries and locations onto the solution. Our team of analysts continued to monitor the solution for cyber security threats and tuned detection policies to provide comprehensive detection and response across the enterprise.

Insurance

We supply an on-premise team to maintain and operate the client's endpoint security solution, spanning over 120,000 endpoints globally. Additionally, we've operated other endpoint and server hardening solutions to protect legacy operating systems from new and evolving threats.

Manufacturing Client

We deployed and onboarded our client onto a 24x7 managed SIEM service to provide protection over their estate.

The client has over 7,000 employees across the globe.

KONTEX
www.kontex.com

Where Security Meets Quality

Ireland: Alexandra House, 3 Ballsbridge Park, Dublin, D04 C7H2
T: +353 1 631 9452
Web: www.kontex.com
Email: advisory@kontex.com

Ireland – United Kingdom – Netherlands – United States
ISO27001: 2013 – Information Security Management System Certified Company
ISO9001: 2015 – Quality Management System Certified Company
Follow us on Social media