Adversary Emulation Service

Proving Security Tool Effectiveness

July 2021

KONTEX

Microsoft Partner
Microsoft

Gold Data Analytics
Gold Security
Gold Cloud Platform
Silver Application Development
Silver Small and Midmarket Cloud Solutions

Industry: Why Adversary Emulation is Essential

Most well-known offensive security assessments today are heavily focused on pre-compromise. 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.

CHALLENGES

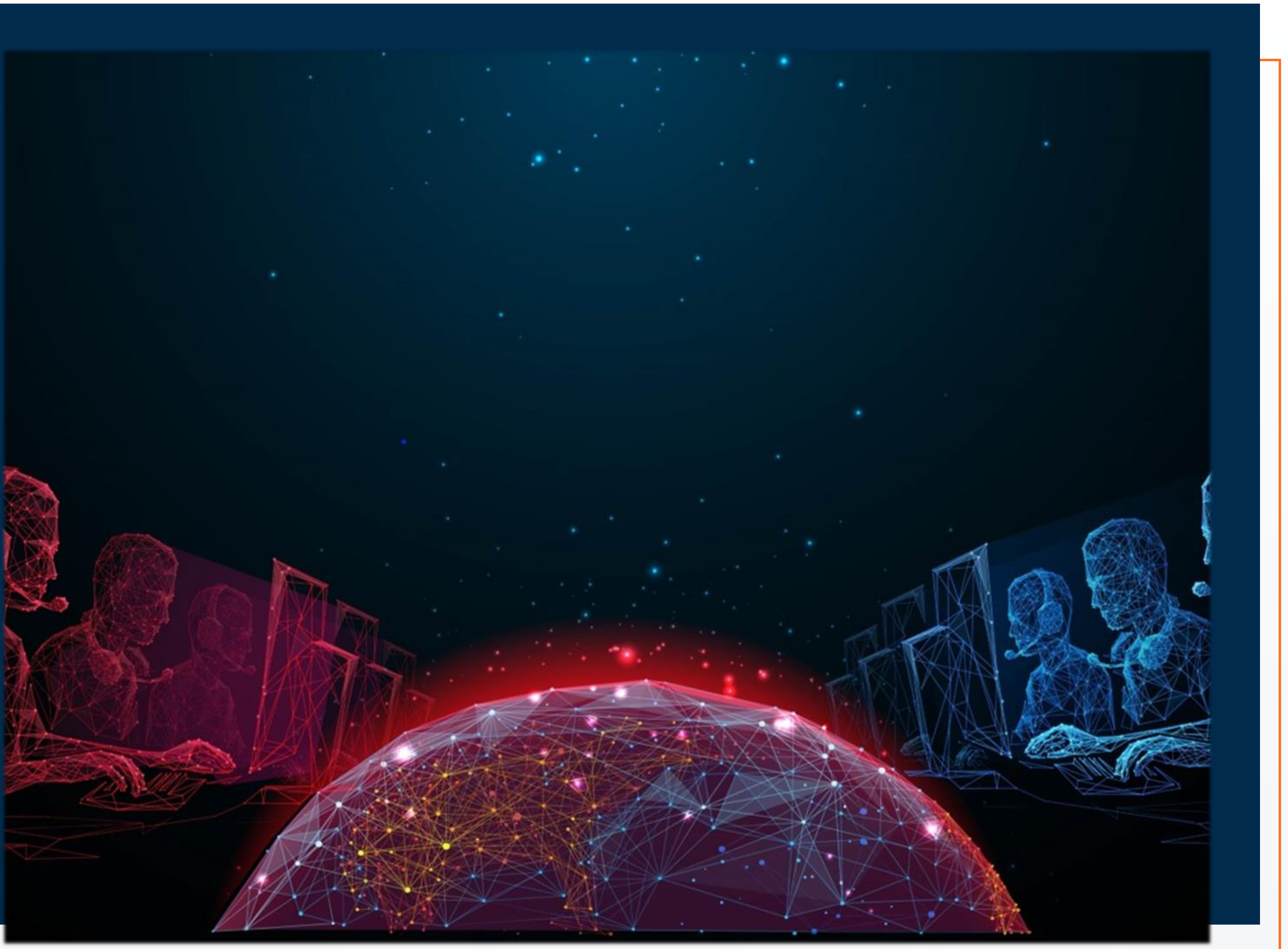
Attackers can go undetected for long periods of time, so organisations need to continuously test their security team’s ability to detect and respond to today’s sophisticated, targeted attacks. Organisations need to validate that their current security controls and processes are effective against today’s 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.

IDEAL SOLUTION

Our solution empowers Red and Blue Team members so that organisations can enhance their threat mitigation processes, extending the value of their current technology purchases. Our approach is a fully-customisable emulation solution aligned with real world attack campaigns. You will be able leverage contextual business risk so that your Blue Teams can prioritise their defensive and IR activities by using real-world TTPs for a proactive approach.

DESIRED OUTCOMES

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.



KONTEX

Adversary Emulation Service

Test your team's ability to detect and respond to sophisticated attack, validate your current security controls against TTPs, identify gaps in your current security posture, understand how an attacker may breach your network, with our real world emulations.

1

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.

2

TEST THE EFFECTIVENESS OF SECURITY CONTROLS

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

3

EVALUATE YOUR MATURITY LEVEL

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

Kontex Adversary Emulation & Microsoft XDR

The ability to prove the efficacy of our cyber defenses has never been more important. The rampant spread of new ransomware variants, unpredictable exploitation techniques and the evolution of attacker behaviors has propelled the need for comprehensive detection and response strategies. Kontex's Adversary Emulation service allows organizations to enable a comprehensive XDR strategy that is tested and proven against real world attack campaigns such as Conti, Maze and Ryuk with new synthetic variants released every month.

Prove Readiness Against Relevant Attack Campaigns

By leveraging our synthetic malware variants, you can prove to leadership that you are ready to respond to the most recent and relevant attack campaigns.

Get More Out of Your Microsoft Investment

Our unique approach maps each technique used in an attack campaign to an aspect of your Microsoft and third party detection and prevent capabilities while driving improvement.

Find and Respond to Threats Faster with Intelligent Automation

By focusing on the specific techniques used in an attack, we can leverage MS XDR and MS Power Apps to automate complex response activities, freeing up security teams.

Customer success: Client Confidential

By leveraging Kontex's Adversary Emulation service, the client was able to measure the efficacy of their Defender & Sentinel XDR deployment against 42 Tactics, Techniques and Procedures (TTP) used by the Conti ransomware variant. Initially, only 28% of the TTPs were detected as malicious. By tuning the client's XDR investment, the ability to respond and prevent to a complex ransomware attack was increased dramatically while detecting > 90% of Conti's behaviors.

Life Sciences - Our client has 38,000 employees globally across 50+ locations.

Our team of analysts provide implementation support, incident monitoring, and operational support across a range of security technologies spanning: • Defender; • Data Loss Prevention; • Sentinel.

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.

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 IR across the enterprise.

Channel partner success: Kontex proves MS XDR value in key account

Kontex was able to displace a very large IBM qRadar deployment with Defender and Sentinel XDR by demonstrating the speed and flexibility of Microsoft's XDR capabilities when responding to a complex ransomware attack. Kontex's Adversary Emulation service proved that Microsoft XDR could be tuned and respond to threats faster than the incumbent IBM and Symantec solution.

Semi-State Postal Service – Sentinel Expansion

By building a custom deployment of Sentinel to detect and respond to application risk, Kontex were able to increase security ACR with the client by over 400% in 6 months.

Semi-State Utility – IBM qRadar Displacement for Cloud Workloads

Kontex were able to prove the flexibility of the Sentinel platform over IBM qRadar in detecting and responding to threats across the client's cloud applications and application pipelines.

Education – UK University – Defender XDR Deployment

Kontex successfully deployed the full XDR stack across 20,000+ devices over a 4-week period. The project involved the displacement of incumbent technologies while customizing MS XDR to meet the unique needs of the education sector.

Test your ability to respond to complex cyber attacks with Kontex’s Adversary Emulation Service

Call for more information: 00353-1-5667050

Ask a question via email: advisory@kontex.com

Learn more: Kontex Adversary Emulation Services

Market Place Offer ID: adversary_emulation_service

KONTEX

Microsoft Partner

Microsoft

Gold Data Analytics
Gold Security
Gold Cloud Platform
Silver Application Development
Silver Small and Midmarket Cloud Solutions