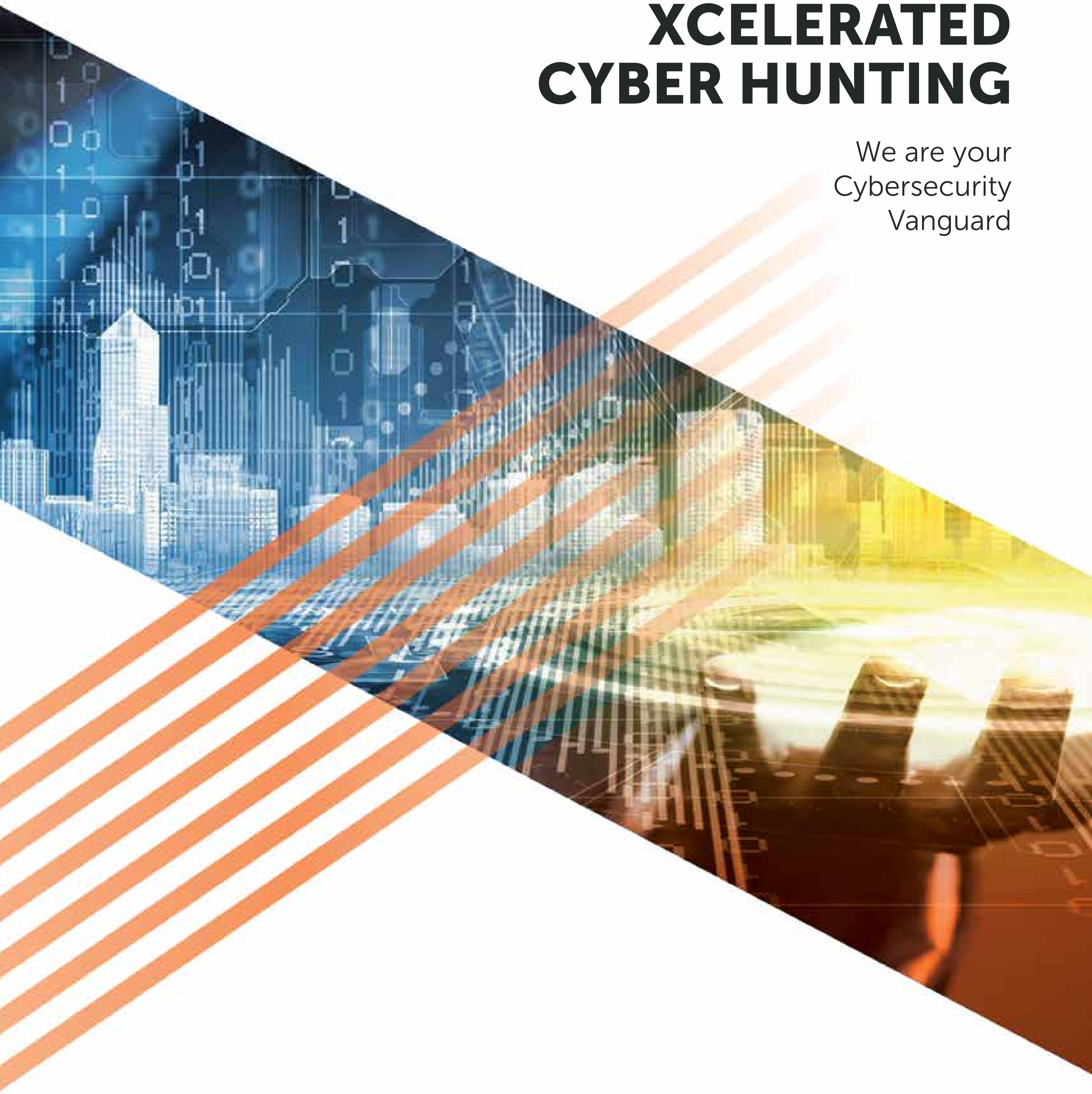
WHITEPAPER 2017

SNIPER: XCELERATED CYBER HUNTING

We are your
Cybersecurity
Vanguard



XCELERATE SOLUTIONS

Secure Results.
Delivered.

xceleratesolutions.com

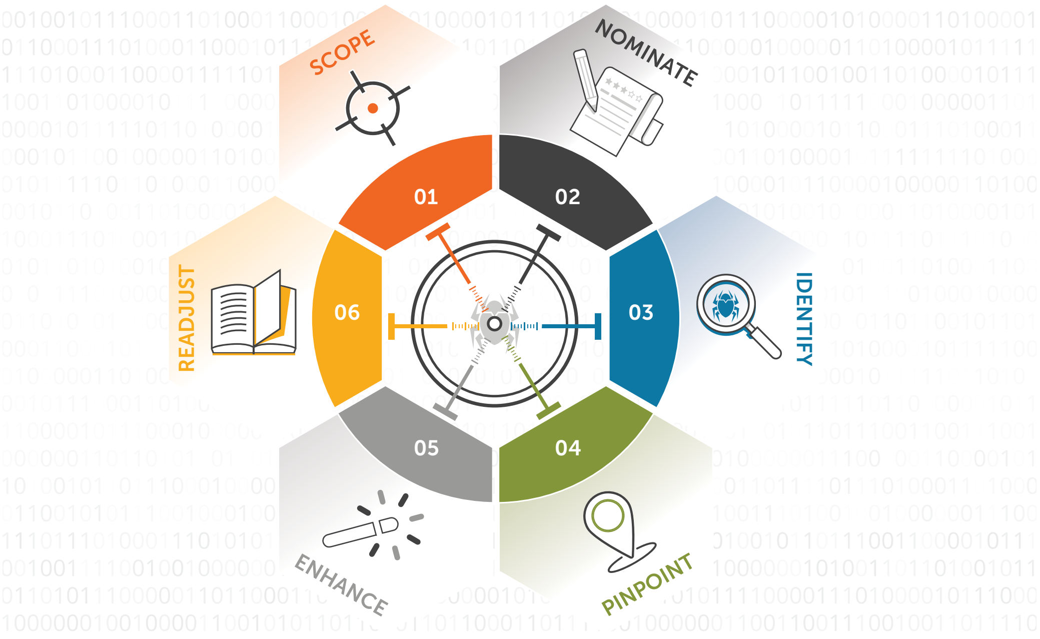
TABLE OF CONTENTS

Xcelerate Solutions (Xcelerate) puts you on the offensive by applying our Cyber Hunting framework—SNIPER—to manage risks from advanced and persistent cybersecurity threats, malicious insiders, and zero-day vulnerabilities. In this paper, we explain the background, benefits, tools, and techniques we use to bring your adversaries in focus and stop them in their tracks with our SNIPER approach to the cyber defense of your organization.

Traditional defense mechanisms—including firewalls, intrusion detection and prevention systems (IDPS), security incident and event management (SIEM) tools, and even personnel training—have, time and again, failed to prevent serious security breaches. With the proliferation of storage and processing of personal and sensitive data, these incidents can cause exceptionally grave damage to our national and personal security.

While the mechanisms above are critical, the systematic gap we see is that they are "bandages" for security: they treat the symptoms (an ever-shifting set of vulnerabilities) but not the underlying disease—the attackers, especially those may already be inside your perimeter.

Our cybersecurity thought leaders—hunters, information systems security professionals, expert risk management professionals—designed and follow our agile and disciplined SNIPER approach to rapidly learn about, identify and eliminate threats to your mission systems and cyber infrastructure.



Xcelerated Cyber Hunting with SNIPER is an innovative, agile, and self-learning process to seek out, quarantine, and destroy bad actors in and around your systems and networks that threaten your unique mission.

For 2016 alone, the Identity Theft Research Center, a non-profit that tracks security breaches and supports victims of identity theft, identified **725 breaches**. Government agencies and systems were the source of **42%** of compromised records.

idtheftcenter.org/

ADAPTABILITY THROUGH AGILE

SNIPER is designed to rapidly adapt to the evolving threat vectors that your adversaries are using to attack your infrastructure. We apply the expertise we've learned through our successful Agile Engineering programs to meet this challenge.

We follow a sprint-based approach, executing the entire process in regular intervals; we typically suggest two or three weeks based on the specific risks and pace of your enterprise.

This iterative approach enables us to

- Ensure *continual alignment* with your program vision and enterprise operations, avoiding service interference and prioritizing defense of your highest value assets.
- Demonstrate *results with predictability and transparency* through reports on activity, proof of success, and repeatable automated scripts.
- *Learn quickly* from our experiences in your unique environment, building on our successes and adapting to the changes in the cyber threat landscape.

In agile software development, sprints are focused around user stories — use cases or requirements expressed in a conversational form by business users.

We act under the assumption that bad actors are going to use both known and unknown (zero-day or simply undetected) vulnerabilities.

- As an insider threat, I want to modify the port settings on the external-facing firewalls, so that I can exfiltrate sensitive data from the network.
- As a hacktivist, I want to access your log files, so that I publicize what I perceive as wrong-doings by your agency.
- As a hacker, I want to tunnel into your network through ports that are open for communication with a critical legacy system, so that I can access data and system interfaces for which I am not authorized.
- As a hacker, I want to elevate my privileges by exploiting a known Windows Server vulnerability that has not been patched in two weeks, so that I can install a backdoor into your network and manipulate systems remotely.

The first two sample evil user stories above guide our identification previously unknown vulnerabilities, describing the actions a threat may take but not the specific method. The latter two are focused on known vulnerabilities (e.g., pending items on a Plan of Action & Milestones [POA&M]) that we want to verify have not yet been exploited and automatically check going forward.

We turn the agile user story model on its head, building our assessments around **evil user stories**,[1] predicting the actions that a hacker or criminal —someone you definitely do not want to be a user— would take.

[1] Our concept of evil user stories is built on the best practices espoused by the Open Web Application Security Project (OWASP): https://www.owasp.org/index.php/Agile_Software_Development:_Don%27t_Forget_EVIL_User_Stories

THE BENEFITS OF OUR STEADY, RAPID-FIRE TECHNIQUE

Xcelerate designed our SNIPER cyber hunting approach to deliver several key benefits to our customers:

IMPROVED CYBER RISK POSTURE by lowering the likelihood of risks being realized. We are tied into your risk management process and personnel: your highest impact areas of risk are those that we most want to ensure remain uncompromised.

ACCELERATED RESPONSE TO CYBER THREATS through our active approach to detecting nefarious or unanticipated activities. Industry estimates suggest that advanced persistent threats can remain undetected within an enterprise network for a year or more. We aim to reduce that by seeking out those abnormalities, determining the path they are following, and eliminating vulnerabilities they may have introduced. Furthermore, because we iterate and adapt in an agile manner, we are able to pivot quickly when new methods of attack are discovered.

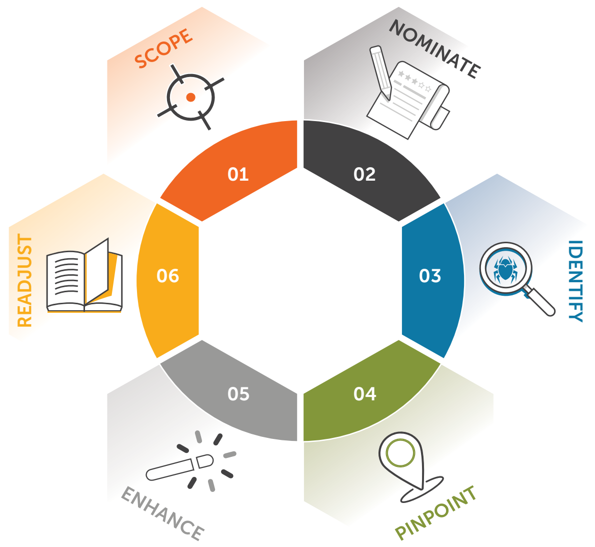
IMPROVED SECURITY by identifying vulnerabilities in your network and hosts that may have been missed through traditional tooling. We work closely with your security, operations, and development teams to add remediation activities to the backlogs for maintenance and security testing.[2] Today's automated tools, even those that are more proactive than firewalls, are built upon known signatures or known learning algorithms. These must be supplemented with human intelligence for a truly proactive model. Your adversaries are just as much focused on the capabilities offered by vendors of cybersecurity products as you are, and they work continuously to subvert them.

INCREASED CUSTOMER SATISFACTION AND CONFIDENCE as we work to keep your agency from being the next victim of a breach. We know that your success is tied to the continued use and enthusiasm for your services by your users, and we seek to maintain your reputation in that regard.as Amazon AWS / GovCloud / C2S, IBM SoftLayer, Microsoft Azure, and Defense Information Systems Agency (DISA) milCloud Defense Enterprise Computing Centers (DECC)—to present a detailed cost-benefit analysis of alternative providers for each component of your unique solution. Leveraging our IT Program Management and Agile expertise, we oversee the team executing the detailed improvement plans.

ALIGNING YOUR SIGHTS AND TAKING ACTION

SNIPER is a cyclical, 6-step learning process that incorporates continuous improvement into the tactics for detecting the presence of bad actors in your systems and infrastructure. We follow all 6 steps in every sprint, which allows us to adjust quickly when your or your adversaries' priorities change and maintain continual alignment with your overall cybersecurity vision.

[2] This approach can be further augmented by the Xcelerate Real-time Assurance Engine (XRAE), which streamlines the resolution, maintenance, and reporting of vulnerabilities. We provide an example of this toward the end of this white paper, and we look forward to discussing SNIPER and XRAE with you soon.



> If you are not hunting, you are losing the battle over your enterprise's cybersecurity.

1. **SCOPE** out the types and depth of data to analyze, the adversaries who may be interested in your systems, and your organizational risk profile. We take this action holistically in our initial engagement with you, and we iteratively improve our understanding every sprint. Through our connections to cyber threat intelligence feeds, we provide a thorough picture of the threats to your enterprise.

2. **NOMINATE** evil user stories as potential or probable attack vectors for our evaluation and mitigation in each sprint. We collaborate with you to ensure that the evil user stories we are focused on are in alignment with where your priorities and areas of high risk reside.

3. **IDENTIFY** the processes, methods, algorithms, and enabling technologies that we will use to collect data, analyze potential threats, and detect nefarious activities. This is the detailed design of our user stories—how we will go about evaluating and resolving them.

4. **PINPOINT**, isolate, and eliminate advanced threats to your enterprise. We leverage our expertise in data inspection and analysis as we perform in-depth research and assessments of your network traffic and audit logs. When we detect anomalous behavior or abnormal patterns, we recommend and take action to turn off the channels by which those actions occur. This could include removing backdoors/Trojans, closing ports, disconnecting servers, changing server names or IP addresses, etc.

5. **ENHANCE** future analysis, detection, and alerting by developing and deploying automated scripts based on the actions we took to detect the patterns of activity in the previous step. Wherever possible, we develop automated detection and alerting scripts as extensions to the functionality of your current enterprise threat detection tools to keep your baseline consistent.

6. **READJUST** tactics based on sprint success, new evil user stories, changes in your vision and priorities, cyber threat intelligence updates, and the availability of enabling technologies, algorithms, and industry best practices. This is also our opportunity to hold a retrospective session, where we seek to continuously improve the way that our cyber hunting team functions in your environment and in support of your unique mission.

APPLICATIONS

The samples below illustrate just some of how Xcelerate can deliver support to your mission's enterprise cyber security with SNIPER, our innovative cyber hunting technique.

The Advanced Persistent Threat (or when the IDPS says "all is normal"...)

A large enterprise organization is finding that their Intrusion Detection and Prevention Systems and firewalls are not sending any notifications about abnormal activity, aside from fairly standard attacks using known signatures. Is cyber defense really as easy as turning on some perimeter analysis tools? The themes from top cybersecurity conferences and companies are that attacks are constant and varied. This inconsistency leads the organization to proactively analyze their network and host activity with Xcelerate's SNIPER methodology. An iterative analysis of the organization's network and server logs and traffic metadata uncovers a strange pattern of activity, including modifying firewall logs. The agile and targeted SNIPER approach to applying new automated detection scripts to these patterns enabled the organization to catch an Advanced Persistent Threat (APT) in the act of perusing the network, discover how they are accessing the system, and seal the holes that had gone undetected by traditional security tools.

Cyber Hunting in Development

The innovative structure and techniques of SNIPER are built to be applied to new or refreshed engineering/development efforts, in addition to protecting those systems in a production environment. An agency is building an enterprise system that processes Personally Identifiable Information (PII) and sensitive government data. The team is architecting and developing with security in mind, referencing Security Technical Implementation Guides. They are finding, though, that this is not enough to prevent the possible abuse of their systems.

Xcelerate cyber hunters apply SNIPER's agile techniques as part of the agency's integrated development teams. By identifying and prioritizing evil user stories as requirements for the system, the agency is able to proactively tie cyber risk management and development together. Furthermore, by applying SNIPER to penetration tests and remediation in the pre-production integration test environment, the security operations team is able to supplement the security defense tools with advanced detection protocols built for the agency's specific and unique cyber concerns.

SNIPER and XRAE: Xcelerating the Operationalization of Security and Compliance

A program recognizes the importance of applying proactive cyber hunting techniques alongside reactive tools (IDPS, log analyzers, notification services, etc.) and security patches, including Information Assurance Vulnerability Alerts (IAVA). These activities, though, are not unified in addressing the government's requirements surrounding the Authority to Operate (ATO) and POA&M list for the systems they maintain. This challenge is overcome by combining SNIPER and the Xcelerate Real-time Assurance Engine (XRAE).

XRAE leverages automation to streamline the generation of compliance artifacts as a minimal-impact part of the daily activities of engineers and operators. SNIPER and XRAE work in harmony, with the activities of cyber hunters directly feeding the generation of compliance artifacts. Reports on remediation activities and risk management are automatically updated based on the activities of hunters. Not only does the program gain transparency throughout the enterprise of cybersecurity activities, but engineering and operations are synchronized and gain efficiencies in addressing cyber priorities and risks.

XCELERATE SOLUTIONS

Secure Results.
Delivered.

FOR MORE INFORMATION ON SNIPER:
XCELERATED CYBER HUNTING CONTACT:

eti@xceleratesolutions.com

ABOUT XCELERATE SOLUTIONS

We exist to create innovative solutions that deliver results, manage risk from individuals to systems, and *xcelerate* time to value. Across our three practices — Enterprise Technology & Innovation; Project, Program & Portfolio Management; and Enterprise Process Management — we optimize efficiency and effectiveness and enhance the security and resilience of America's personnel, physical and cyber infrastructure.

PHONE 703.462.1500 **SOCIAL** @XLR8Solutions xceleratesolutions.com
HEADQUARTERS 8405 Greensboro Drive, Suite 930 McLean, VA 22102