Duality

SOAA
SPECIAL OPERATIONS
ASSOCIATION OF AMERICA

“Zero Footprint” Dataset Checks to Increase SOCOM Readiness

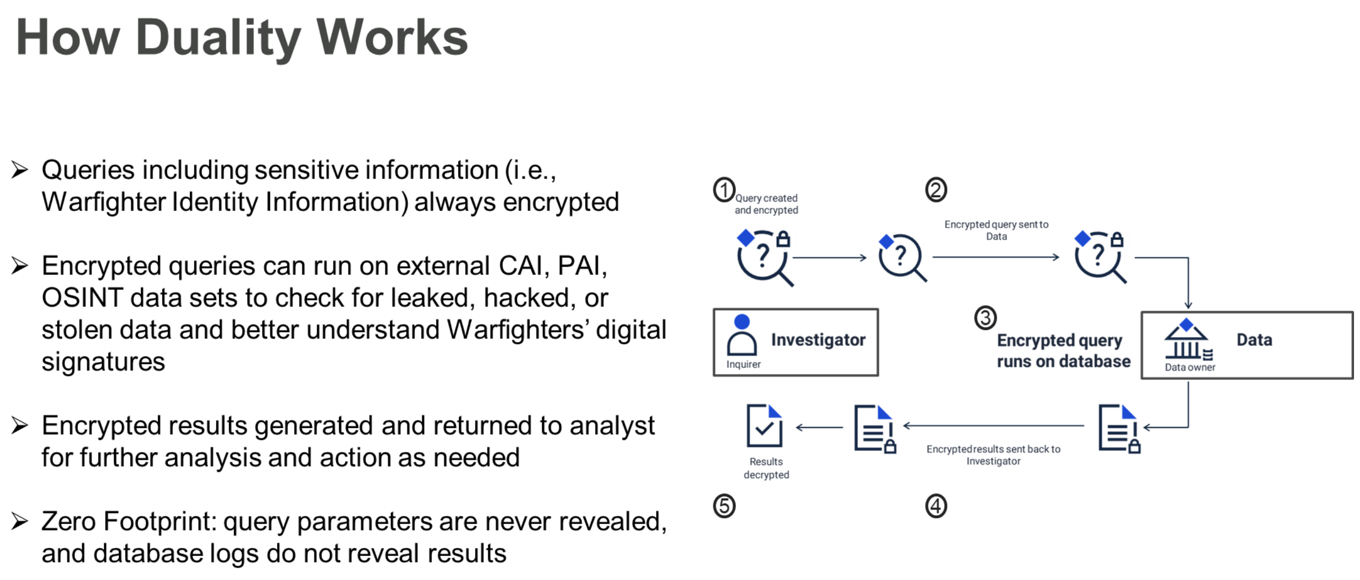
On April 27th, 2022, the Commanding General of U.S. Army Special Operations Command (USASOC), Lieutenant General Jonathan Braga, testified in front of the Senate Armed Services Committee on Emerging Threats and Capabilities, stating bluntly that “There is no sanctuary at home or abroad.” LTG Braga went on to explain that “we must change how we think about protecting and projecting our forces. Advancements in unmanned platforms challenge our legacy systems and programs. Our digital signature exposes individual and collective patterns of life.” US Special Operations Forces (SOF) are uniquely vulnerable to the missions they undertake. With more than 5,000 special operators deployed to over 80 countries worldwide at any given time, a simple call home can expose the service member, and their family, to threats we have not faced in the past. The Department of Defense must adopt digital signature protection programs at an enterprise level to ensure service members, and their families, are protected against online vulnerabilities that disrupt military readiness.

Digital signatures reveal volumes about our warfighters that could be exploited by our adversaries. Five years ago, the Cambridge Analytica scandal revealed that approximately 100 Facebook ‘likes’ were enough to estimate a person’s psychological traits, personality types, and voting habits. Furthermore, data brokers advertise niche datasets of US military members, state actors persistently hack into our most personal information, and military members are bombarded by solicitations from foreign adversaries. As our adversaries increasingly collect information about our warfighters and leverage increasingly potent artificial intelligence and machine learning tools to better aggregate and identify information that they could exploit to attack our warfighters even at home.

LTG Braga’s forward thinking requires solutions the Department of Defense has not yet implemented at scale to protect our warfighters and their families. Service members pay a nominal fee for life or dental insurance, are required to have family care plans, updated health and financial records, are monitored for any security clearance violations prior to, and throughout, deployments – all in the name of readiness, meaning able to deploy, fight and win wars. What about a service member’s digital identity? Military commanders cannot deploy a service member if they are unfit for service due to personal reasons. For example, a warfighter may be unfit for service if they are wrestling with identity theft, if their spouse receives synthetic or manufactured information falsely suggesting infidelity, or believable disinformation that threatens a service member’s security clearance integrity. These are all possible scenarios today. Voice deepfakes can empty a bank account, generative adversarial networks (GANs) can manufacture compromising videos, and well-placed leaked documents funneled to those with security clearances can compromise our most valuable asset – our people.

The Department of Defense (DOD) can monitor our warfighters’ digital signatures, but care must be taken to maintain force protection. The DOD should not openly query commercial data providers, publicly available information, or open-source information about our special forces – we do not want to reveal these warfighters inadvertently to our adversaries. Fortunately, recent innovations from the Defense Advanced Research Projects Agency (DARPA) have enabled solutions that allow DOD to monitor datasets without elevating a digital signature or alerting adversaries about which individuals’ datasets had been viewed. Duality Technologies, a US-based technology startup backed by Intel Corporation and co-founded by DARPA performers, are now offering commercial solutions that would allow the DOD to perform these queries privately, with quantum-safe methods that provide data and identity protections for our warfighters against even our strongest near-peer adversaries.

Duality Technologies' product, which enables "Zero Footprint" Investigations, is currently in use by federal agencies like the Dept. of Homeland Security and has already been sole-sourced into the Dept. of Treasury due to the unique and advanced nature of their software products. Duality even has a 314(b) designation under the USA PATRIOT Act to allow it to be used by financial institutions to protect against broad classes of financial crimes with national security implications. This product comes with a strong legacy of national security involvement, and it is ready to protect our warfighters and their families where they are most vulnerable – at home.



How Duality Works

- Queries including sensitive information (i.e., Warfighter Identity Information) always encrypted
- Encrypted queries can run on external CAI, PAI, OSINT data sets to check for leaked, hacked, or stolen data and better understand Warfighters' digital signatures
- Encrypted results generated and returned to analyst for further analysis and action as needed
- Zero Footprint: query parameters are never revealed, and database logs do not reveal results

For additional information about Duality, reach out to:

Stephan Farrand
sfarrand@dualitytech.com
Director
Duality Technologies
www.DualityTech.com

For additional information about SOAA, reach out to:

David Cook
David@soaa.org
Executive Director
Special Operations Association of America
www.SOAA.org