VERSIVE

INDUSTRY

Network Security Analytics

WEBSITE

www.versive.com

COMPANY OVERVIEW

Versive helps organizations focus on the cybersecurity threats that really matter. Versive automates the discovery of adversary campaigns already unfolding inside corporate networks. Instead of filling dashboards with hundreds of alerts, our less-is-more approach generates about 5 high-fidelity ThreatCases per week.

PRODUCT OVERVIEW

VSE focuses on the core campaign activities adversaries must perform (internal reconnaissance, collection and exfiltration). It first analyzes multi-source raw data (flow, proxy, DNS) and provides visibility into what is normal for your network. VSE then links activities across multiple campaign stages and ties together key findings into a few actionable ThreatCases.

SOLUTION HIGHLIGHTS

- Software-only, no hardware or sensors required
- Built on the open-source frameworks of Hadoop and Spark
- For any environment: on-premises, cloud or hybrid
- Easily integrates into your workflow

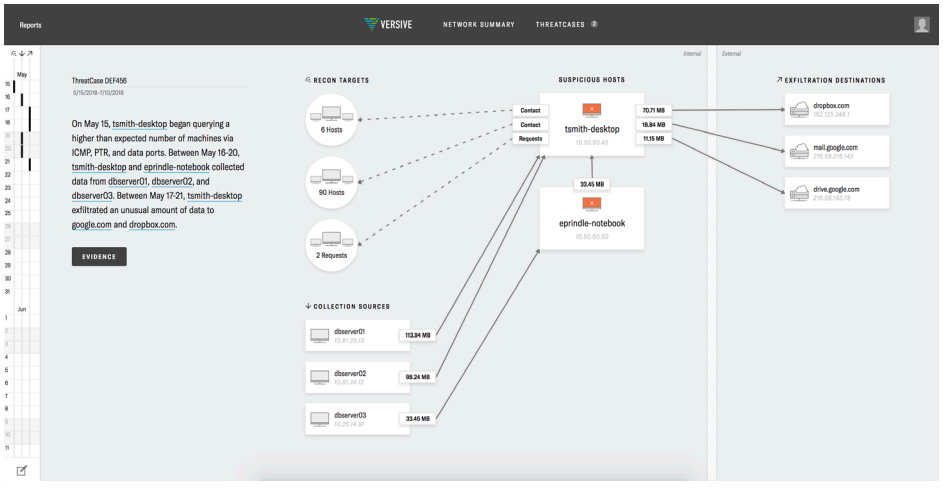
Using integrated machine learning for cybersecurity

Enterprises are faced with a challenging new reality, based on rapid growth in both the sophistication of cybersecurity threats and the complexity of the data they hide in. The combination of increasing data volumes, new computing environments (cloud, hybrid), and more porous networks (Internet of Things, Bring Your Own Device) mean the corporate attack surface is more fluid and larger than ever before. Even with unlimited staffing, organizations would not be able to detect advanced adversaries systematically at scale under current conditions. The challenge exceeds human scale. This leaves organizations vulnerable to loss of capital, intellectual property and brand reputation.

Solution

The Versive Security Engine (VSE) is the critical missing piece in a company's security portfolio, providing continuous situational awareness inside your network. It acts as your last line of defense, detecting internal and external adversaries regardless of what new tools, tactics, or exploits they use. VSE's ThreatCases automate the time-consuming process of compiling the data needed to understand a threat. With an average delivery of 5 per week, security teams can focus on what matters most — shutting down the threats and minimizing risk.

VSE automatically exposes the activities that all adversaries must engage in to accomplish their mission: internal reconnaissance, collection, and exfiltration. Anomalies and adversary behaviors are important, but what really matters is the way they are related. VSE uses AI to automatically uncover the required chain of threat activity that separates the signal — the real risks to your business — from normal network noise. This approach has been how the best experts in the world uncover novel threats, and we've automated and enhanced it with AI.



VERSIVE

BENEFITS OF CLOUDERA

- Powerful – Store, process, and analyze all your data
- Open – 100% open source powered by Apache Hadoop
- Simple & Compatible – Easy to deploy and operate
- Economical – Up to 90% more cost effective
- Enterprise Ready – Support mission-critical operations

BENEFITS OF VERSIVE

Serves as your last line of defense

- Understands core activities that adversaries can't avoid instead of relying on detection of specific tools, signatures, and IoCs

Eliminates alert fatigue

- Discovers and makes sense of ongoing adversary campaigns, instead of filling dashboards with hundreds of alerts
- Generates about 5 high-fidelity ThreatCases per week

Saves time and money

- Force-multiply analysts – automatically compiles the data needed to understand a threat

Scales to any network size

- VSE is a software-only solution that scales to fit the size of your environment
- Does not require any proprietary "black box" hardware

Enterprise-scale, network security analytics

This joint solution enables organizations to fill the most urgent enterprise cybersecurity gap: continuously uncovering threats operating inside the network that you previously did not have visibility to. The partnership combines Versive's AI technology with Cloudera's capabilities to create the only enterprise-scale, automated, network security analytics solution. Using the joint Cloudera-Versive cybersecurity solution, organizations can expedite threat detection, investigation, and remediation via machine learning and consolidation of all enterprise security.

Surfaces threats faster

Today's sophisticated threats require that companies surface advanced threats faster, regardless of what tools, tactics, or exploits they use. This is made possible by applying machine learning and artificial intelligence to larger enriched data.

Adversary behavior within a network inevitably leaves a digital "paper trail" in internal network data (netflow, proxy and DNS). VSE looks for unexpected internal reconnaissance, collection and exfil behaviors and understands how they relate across time and across the network.

It then automatically generates ThreatCases, which tie together suspicious findings from across time and the network into a contextual map. This makes investigation easy and force-multiplying the impact of your existing security team.

Unrivaled performance, scale, and analytics

Cloudera's cybersecurity solution is powered by a next generation data management and analytics platform that breaks down the traditional barriers of data ingestion, storage, processing and analysis. Enterprises can now leverage any type or volume of security data.

VSE is built on the open source frameworks of Spark and Hadoop. It is a software-only solution that scales to fit the size of your environment and does not require any proprietary "black box" hardware, and utilizes data streams that the customer authorizes, controls, and retains.

Versive
www.versive.com

Cloudera
www.cloudera.com