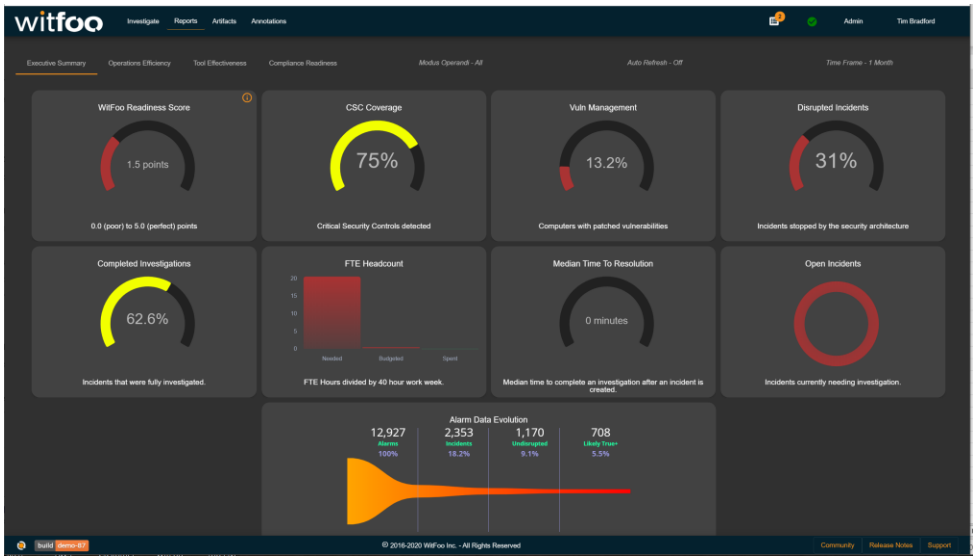
Leveraging Law Enforcement Expertise for Cyber Security

The fundamental challenge in cybersecurity today is the lack of human resources. Every day, organizations have more security events to investigate than is humanly possible — the problem is compounded by the number of tools contributing events and the complexity of each tool. Best practices can be learned from cyber security and law enforcement communities, but how can you harness that expertise and integrate those practices into your everyday work?

WitFoo Precinct

WitFoo Precinct reduces time and labor spent performing cyber security investigations by greater than 90%. It is the world's first and only ***diagnostic SIEM*** combining the best approaches of legacy SIEM and Incident Response Platforms, Behavioral Analytics, Orchestration & Automation tools and Big Data Analytics while learning and crowdsourcing insights from cybersecurity experts. All these capabilities are delivered in a flexible, infinitely scalable architecture that can be instantly deployed and operational in any environment.

WitFoo delivers a fully integrated solution with SIEM, SOAR, UEBA and IRP in a single platform, reducing complexity and providing visibility in a single pane of glass.



JOINT SOLUTION BENEFITS

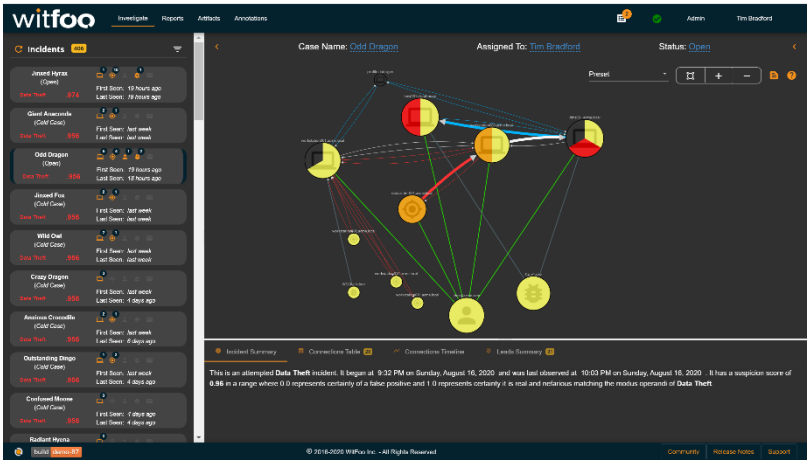
- Zscaler's rich data source enables WitFoo to determine IOC matches and identify attacks disruptions.
- WitFoo Precinct normalizes Zscaler records and extracts relevant fields that are analyzed, indexed and searchable by our mutual customers.
- WitFoo's advanced SOAR capabilities can automatically perform attack mitigation.
- Provide CSC compliance details

WitFoo integrates with Zscaler by ingesting its high resolution NSS logs in the standard CEF format. Unlike other solutions, Precinct is able to intelligently index and extract fields for analysis. Zscaler's high value fields such as URL, file, malware, user and data loss details are uniquely leveraged by Precinct to monitor for a wide array of attack types.

With Precinct, you can start small and scale to an infinite number of data and processing nodes to allow for infinite ingestion, processing and storage.

Incident Creation and Analysis

Using investigative models borrowed from law enforcement, WitFoo Precinct builds relationships of all network computers, users, files, and emails and evaluates them for potential nefarious behavior by analyzing data, objects, and relationships for matches against the modus operandi of attackers.



Normalized incidents are analyzed using high-level Security Orchestration, Automation & Response (SOAR). WitFoo SOAR checks the entire incident for all observations that an expert analysis would run. The results of these observations impact the suspicion of incidents. Suspicion informs investigators if there is enough evidence to act against attacking hosts or compromised credentials.

WITFOO PRECINCT

- WitFoo Precinct reduces time and labor spent performing cyber security investigations by greater than 90%
- Delivers full parity with SIEM, SOAR, UEBA and IRP solutions in a single platform while delivering unparalleled security reporting capabilities
- Provide readiness metrics of all security controls
- Customer centric license model allowing for Infinite scale and data retention
- Unparalleled security business metrics on compliance readiness, tool effectiveness and operations efficiency

Disruption Detection

Precinct analyzes every incident to determine if the security architecture successfully disrupted (blocked/quarantined, etc.) an attack. These incidents are closed as “disrupted” and generally do not require action by the local operator. Through API integrations, Precinct can automatically respond to threats using SOAR actions.

About WitFoo

WitFoo was founded in 2016 by veterans of the US Military, law enforcement and cybersecurity to mature the craft of cybersecurity operations. From 2016 to 2019, WitFoo conducted research with organizations ranging from higher education to the Fortune 500 to develop a comprehensive cybersecurity platform. WitFoo Precinct 6.0 was released for GA as the world’s first ***Diagnostic SIEM***.

About Zscaler

Zscaler enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match.