SECBI
Autonomous XDR

MULTI-VECTOR AUTOMATED DETECTION AND RESPONSE

THE SECBI XDR PLATFORM
VENDOR-AGNOSTIC, EXTENDED SECURITY INCIDENT DETECTION AND RESPONSE

Today's multi-vector threat landscape demands a synchronized, unifying solution that correlates the entire security environment under a single pane of glass, enabling automated full scope detection and response. Until now, a typical enterprise network has installed multiple point, siloed solutions, each serving a single purpose, yet without the insight and context an analyst needs to understand the full picture of suspicious incidents. Siloed, disconnected systems deliver poor security productivity with too many alerts, false-positives, and partial breach information. As a result, analysts conduct lengthy investigations, rarely finding the full extent of breaches.

Fortunately, there's a solid cyber defense approach now: By combining data from multiple security tools into stronger signals of the malicious intent, followed by machine-learning based analysis, analysts can receive fast, accurate and extensive detection and automated response.

COMBINING THE XDR APPROACH WITH AUTONOMOUS TECHNOLOGY™

SecBI's XDR platform is a SaaS-based, vendor-agnostic, extended security incident detection and response platform that natively integrates multiple security products into a cohesive security operations system. This tightly synchronized cohesion drastically improves response accuracy and security operations center (SOC) productivity. The goal of the platform is to unify the integration of an enterprise's security controls under a single pane of glass for significantly more accurate detection and faster response.

Once all security data is centralized and normalized in one repository, it automatically applies SecBI's "Autonomous Investigation™" technology to detect advanced threats. This correlated incident response capability optimizes each of the individual security products, thereby raising the organization's rate of return in their security investments. Analysts are presented with complete detection narratives with visibility of all infection points involved in the same incident. This full scope narrative provides analysts with actionable options, such as blocking malicious hosts for the particular incident, and automating the response on preventive tools for the future.

Detect fileless and BIOS malware, crypto-jacking, IoT attacks and the next unknown threat

Automate response.

Augment prevention.

Amplify hunting.

WHAT XDR DETECTS & REMEDIATES IN THE FULL SCOPE OF AN ATTACK?

A complete narrative of the incident, from the initial entry point to the full kill chain, including:

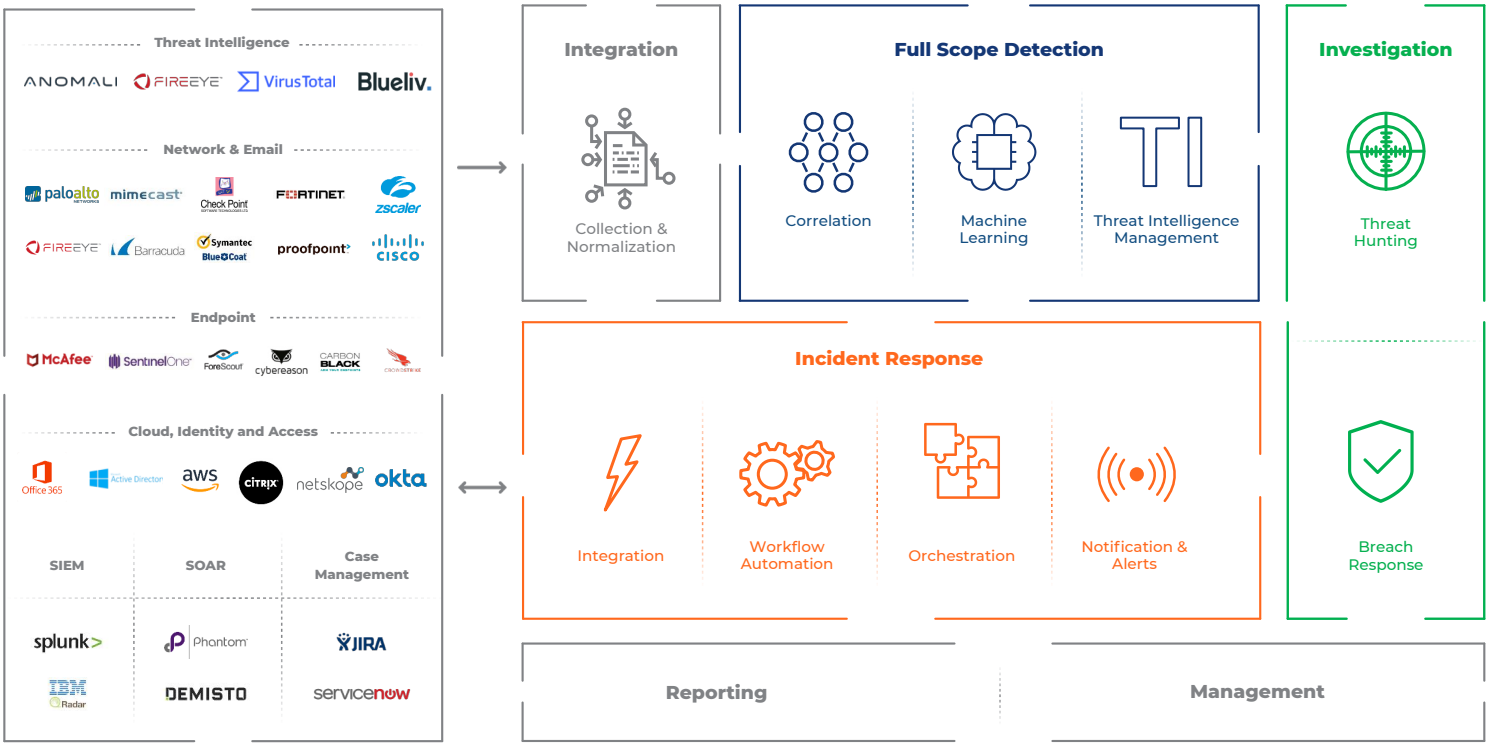
ALL INFECTED USERS & ENDPOINTS

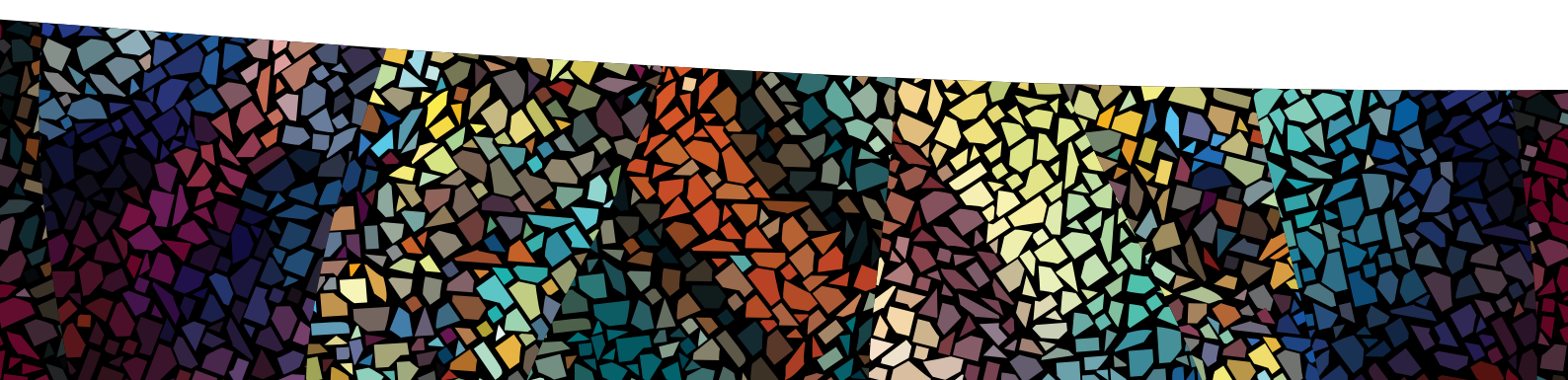
ALL MALICIOUS DOMAINS & HOSTS

THE POWER TO DETECT THE UNKNOWN

SecBI's XDR Platform detects and clusters all internal (e.g. users, devices) and external (e.g. domains, IPs, C&C servers, drop points) entities involved in communications in a compromised network. Identifying a malicious cluster, as opposed to a single discrete anomaly or sporadic alert, ensures faster and accurate detection. SecBI's XDR Platform turns floods of incidents into a prioritized, easy-to-use UI for simple triage, investigation, and mitigation.

THE SecBI XDR PLATFORM: AUTOMATED DETECTION, RESPONSE AND INVESTIGATION





THE MISSING LINK IN CYBERDEFENCE: AUTOMATED RESPONSE AND AUGMENTED PREVENTION

Despite the intuitive coupling of automated response to follow accurate detection, few combined solutions are available on the market. In contrast to playbook automated solutions that are based on sporadic anomalies and false positives, SecBI offers extra value by offering complete automation with high-grade detection technology based on unsupervised machine learning. Deployment is quick without weeks of customization and time investment.

A wide range of predefined automated workflows and playbooks in the system allow for automated building of the complete scope of an incident, with flexibility to inject responses into the workflow for pinpointed response and mitigation. Adding playbooks and connectors to different security appliances allow for flexible configuration and extensions to perform the full playbook-based mitigation via policy updates and enforcement with all relevant security appliances.

DEPLOYMENT WITHIN HOURS AND READY TO ROLL

The SecBI XDR Platform solution is easily and instantly deployed in the cloud with no additional appliances or agents. Your SOC is amplified immediately with zero change to the network infrastructure. Your existing SOC personnel are quickly trained to use the solution. No additional professional services are needed.

BENEFITS OF THE SecBI XDR PLATFORM

- ☑ Lowers TOC and avoids vendor lock-in as the only vendor-agnostic XDR Platform.
- ☑ Agent-less, rapid deployment with a single, software download.
- ☑ Improves SOC efficiency with automated processes.
- ☑ Improves efficiency of point solutions by sharpening the investigation and response processes.
- ☑ Rapid, more accurate detection including alert correlation and full incident response data correlation.
- ☑ Faster time to remediation, providing integrated incident response options.
- ☑ Enables quick pivoting from interactive threat hunting to automated detection and response.
- ☑ Eliminates blind spots by correlating data into behaviors.
- ☑ Ensures analyst collaboration via a common management and workflow.

SECBI
Autonomous XDR

www.secbi.com

info@secbi.com