Cloud Based, Automated Breach Analytics

Seculert's automated breach analytics platform protects global enterprises from the effects of targeted malware attacks. The Seculert platform drives the network egress monitoring service which does three things to uniquely complement existing malware infection prevention systems:

1. Fully automates the breach detection process;
2. Provides continuous visibility into how "owned" an organization is by cyber criminals;
3. Precisely identifies devices infected by malware beaconing to criminal command & control servers.

The Seculert platform achieves all of this while requiring no new hardware, software, or agents to be installed.

Improved Detection

- Identifies exactly which devices are infected by which malware
- Detects up to 90% more infections than prevention and SIEM solutions
- Identifies active infections that have evaded perimeter-based prevention systems
- Reports only "true positive" infections…no chasing false positive alerts
- Observes "timed" malware behavior designed to defeat real-time detection solutions

Enhanced Operating Visibility

- Reduces detection, containment, and remediation time from weeks to 1-2 days per incident
- Provides continuous visibility on prevention system performance and response to new attacks
- Feeds accurate infection data back to prevention layer components thus improving their efficacy
- Leverages crowd sourced threat data across the global Seculert platform meaning an infection identified in one domain can be prevented in others

Better Coverage

- Utilizes a combination of big data analytics, machine learning and external context to generate unique malware profiles that are used to identify long dormant advanced threats
- Detects and reports on malware at its weakest point when it is communicating with cybercriminal servers or exfiltrating data
- Covers all users and all devices in all geographies with no required hardware, software, or agents

Integrated Protection

- Leverages and Interoperates with existing prevention layer solutions by extracting and analyzing logs from them while sending malware data on new infections to them
- Covers infections introduced through network protection blind spots for both local and remote users
- Provides integrated threat visibility with leading SIEM solutions