Panopticon SOAR

Achieve over 80% SOC automation across a multi-year timeline.

Incident Response (IR) Automation & Integration

Real-World SOC Compromises[4]

95%
One Year Automation

83%
Three Year Automation

82%
Five Year Automation

76%
Ten Year Automation (N=145,729)

3-15
Minutes Automated Response Time

The 18:49 Problem

Security analysts are inundated with alerts—dealing with 10x the amount of alerts a human can handle. What's worse is that it's taking our cyber adversaries just 18 minutes, 49 seconds to compromise and begin moving laterally[1] while it takes the average entity 279 days to identify and contain that breach[2].

Initial commercial SOAR solutions offer the promise of reduced alert load through automation. However, most solutions focus on incident investigation rather than actual automated response. In practice, these SOAR solutions seem to be stuck in a rut[3] and only result in a handful of useful IR use cases.

A New Approach to SOAR

Introducing Panopticon SOAR, the only solution on the market with over ten years of real-world use. Developed in the trenches of a large SOC by DevSecOp engineers, Panopticon SOAR takes an "action first" approach. It allows analysts to focus on the most accurate detections and enables them to fully automate the response to those incidents. By automating the "known bad" incidents first, Panopticon SOAR can help SOCs automate up to **95% of their incidents across real-world networks** and **decrease dwell times to under 15 minutes**.

Panopticon SOAR helps liberate security analysts from mundane & monotonous operations for innovation and discovery.

Automation

Create autonomous workflows that can lock compromised user accounts, null route systems, and send notifications to impacted users and IT support teams.

- End-to-end automation workflows
- Context-specific workflow stubs
- Exception management

Integration

Unify your team, processes, and technology on a single interface and provide the real-time collaboration tools necessary to manage and respond to incidents.

- Security inbox from all sources
- Embedded ticketing
- Incident case management

Delivery

Leverage a product built for large, complex environments and automate across broad use cases ranging from breached systems, to critical vulnerabilities, to policy violations.

- Real-time response
- Scalable across multiple clients

[1]2019 Global Threat Report by CrowdStrike
[2]2019 Cost of a Data Breach Report by IBM and Ponemon
[3]2019 Market Guide for SOAR Solutions by Gartner
[4]2019 Panopticon SOAR Data from UT Austin SOC

TEXAS
The University of Texas at Austin

Automation by the numbers.

> **I can clearly demonstrate that Panopticon saves our campus time & resources every day.**
>
> Cam Beasley, UT Austin CISO

Critical Vulnerability Response

25,000+
Exposed Remote Services (VNC, SSH, RDP)

19,000+
Windows 7 Legacy Systems

2,400+
WannaCry Vulnerable Systems

Known Breach Scenario Response

47,000+
CNS Bots/Trojan Compromised Systems

5,600+
Compromised User Account Scenarios

3,000+
Android Malware

Panopticon SOAR currently serves as the security operations backbone to one of the largest universities in the United States, The University of Texas at Austin. Over the past decade, it has helped their IR team come together, automate workflow processes, and ensure a complete system of record. Cam Beasley, UT Austin CISO mentions, "Panopticon SOAR has helped us automate many of our daily tasks and allowed us to be faster to incident containment while enabling us to consistently implement our vulnerability management strategy across a highly decentralized and diverse campus. I can clearly demonstrate that Panopticon saves our campus time & resources every day."

Built for All SOCs

Panopticon is a suite of tools designed to adapt to and solve the specific and acute pain points of SOCs and their IR teams across the continuum of maturities.

Emerging SOCs
Integrate your team & tools and gain the big picture view your SOC needs for an effective IR program.

Maturing SOCs
Automate your most frequent and critical incidents and dial in your alerts to improve your signal-to-noise ratio.

Enterprise SOCs & MSSPs
Automate at scale across the vast majority of incidents and manage multiple clients from a single workspace.

READY TO SEE PANOPTICON SOAR IN ACTION?

Contact us to discuss your use cases and set up a personalized demo.

info@saltycloud.com
+1.512.222.9711

U.S. AIR FORCE

SBIR Select If you're a potential DoD or GOV customer, contact us for an extended proof of concept trial or direct "pre-competed" purchase through SBIR Phase III or SBIR/GSA contract.

saltycloud

@saltycloudpbc

 |