CyGlass by NOMINET

So you think you need a SIEM?

Security Information and Event Management (SIEM) tools have been around for several years now. They were supposed to be the solution to the lack of visibility into the security posture of a company. The reality is SIEMs have been too expensive and too complicated to deploy for many companies. Security Operations Centers (SOCs) built on SIEMs are being flooded with events that are burning out cyber analysts. For companies that have already deployed a SIEM, getting a second pair of eyes on the threats in the network will reduce false positives and keep employees engaged on the riskiest of threats.

Is your SIEM giving you value in this new normal? SIEMs charge by Events per Second so storing network traffic in a SIEM can be expensive. CyGlass can digest and store your NetFlow and only send the alerts to the SIEM which will cut your costs considerably.

CyGlass NDaaS | Network Defense as a Service

CyGlass Network Defense as a Service simply and effectively identifies, detects, and responds to threats to your network without requiring any additional hardware, software, or people. Our SaaS platform is constantly expanding to support and meet the needs of SMEs.

CyGlass is up and running within 15 minutes. It is cheaper, more effective and more efficient than a SIEM, by allowing the security team to concentrate on just the most critical alerts. This minimizes alert fatigue and burnout and helps you to retain your highly skilled personnel.

Key Benefits

Threat Hunting – robust analytics and tools for threat hunters.

All Sources of Information – CyGlass uses third party threat intelligence to identify suspicious traffic to external sites. CyGlass can consume traffic from the network, VPN, User/AD and key SaaS applications, like Office365 and GSuite.

Single Pane of Glass – Reports provide detailed and insightful analytics on an organization's cyber risk. As well as identifying the most common threats faced, it also applies a powerful, but easy-to-understand threat score to allow SOC teams to prioritize their work.

Initiate Actions – Suspend user and block traffic at the firewall. Customizable notifications and integration with downstream systems via API.

Actionable Advise – Smart Alerts have easy to understand guidance and security events are mapped to MITRE ATT&CK.

Detects Threats Behind Your Firewall – CyGlass is like having a team of experts analyzing network traffic, detecting anomalies and policy violations. It then triages the alerts, notifying you of anything serious.

How will CyGlass help my business?

Visibility: SMEs are looking for an easy-to-deploy, comprehensive, and cost-effective solution that provides visibility across the network through a security/risk lens.

Compliance: Focused on Identify, Detect and Respond functions, based on the NIST CSF (Cyber Security Framework). Reports are generated that you can use to prove monitoring of the network is taking place, thus proving compliance with the relevant audit and regulatory rules.

Extra Resource: Businesses can't hire enough cyber analysts to investigate alerts coming from their existing systems. CyGlass alerts are based on risk, allowing cyber teams to prioritize.

Reduced Costs: Ultimately, CyGlass leads to reduced cost of ownership due to the absence of an appliance and the corresponding complexities in appliance deployment and maintenance.

Get your free, no obligation threat assessment

CLICK HERE

CyGlass
by NOMINET