CloudShield Eclipse is a robust network detection and response platform that delivers highly customizable, stealthy, and trusted active cyber defense capabilities. Combining threat intelligence data with the functionality of Asset Inventory/Tracking, Threat & Anomaly detection, Intrusion Prevention, and Network Traffic Analysis solutions, CloudShield Eclipse can be tailored to meet your organization and mission needs, provides comprehensive network visibility, and supports advanced threat detection and inline response at machine-speed.

A GHOST ON THE NETWORK

CloudShield Eclipse transparently peers inside communications traffic and provides real-time visibility into potential threats distributed across the network. Sensor and enforcement nodes that report to a controller can be deployed throughout your environment. These nodes:

- Are invisible to the network and your adversaries with no MAC or IP address
- Can be deployed either passively or active inline
- Detect signature-based, indicator-based, and behavioral-based threats via standard formats
- Operationalize threat intelligence
- Adhere to and enforce zero trust principles for your security operations
- Can be customized to process traffic at various line rates deployed across your cyber footprint
- Provide secure mechanisms for processing insecure network traffic with sensitive or classified signatures, scripts, and intelligence

OPERATIONALIZE THREAT INTEL, RESPOND AT MACHINE SPEED

As cyber attacks grow in complexity and persistence, organizations need innovative capabilities that deliver dynamic, operational impact through automation. Blocking attacks at the network perimeter while merely monitoring internal and virtual networks is no longer sufficient.

CloudShield Eclipse contains multi-engine detections to enable automated, customizable inline mitigations driven by wire-speed policy and orchestration. These real-time actions can help your cybersecurity team with:

- Network and asset management
- Defensive cyber operations
- Threat hunting
- Incident response
- Adversary engagement
SHAPE YOUR ADVERSARY'S EXPERIENCE

Go beyond blocking as your core cyber response to network incidents.

With CloudShield Eclipse, you can shape an adversary’s experience by transparently rerouting malicious traffic to deception environments automatically. CloudShield Eclipse effectively increases the return-on-investment for organizations that have already deployed honeypots or deception technologies with our seamless, transparent rerouting.

With multiple built-in deceptive mitigations from CloudShield Eclipse, you can change the economics of an attack to make it more costly, less accurate, and more troublesome for your adversary to attack your organization. CloudShield Eclipse can strategically and tactically manipulate the attack surface of your cyber footprint, misleading attackers based on your mission and objectives.

DEPLOY YOUR WAY, SCALE WHEN YOU NEED TO

CloudShield Eclipse’s unique sensing and mitigation capabilities enable flexible and cost-effective implementations. The platform can be installed on commodity hardware, as a virtual machine, and deployed to cloud infrastructure. Additionally, different deployment models are available, designed for classified environments, enterprises, and smaller or flexible/rapid deployments (e.g. incident response or threat hunting).

The platform can scale based on your needs. You can choose to extend sensors and enforcement nodes into subordinate networks, enclaves, cloud networks, and lateral detection paths as you need it – all while maintaining situational awareness and command and control across the platform from a central management dashboard.

<table>
<thead>
<tr>
<th>FEATURES</th>
<th>BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy-to-use interface with centralized management to customize detection</td>
<td>Achieve coordinated strategic and tactical control of network both at the</td>
</tr>
<tr>
<td>rules and responses</td>
<td>perimeter and throughout your entire ecosystem</td>
</tr>
<tr>
<td>Sensors and nodes that adhere to and enforce zero trust principles</td>
<td>Acquire trusted, distributed network traffic analysis and asset collection</td>
</tr>
<tr>
<td></td>
<td>visibility</td>
</tr>
<tr>
<td>Multi-engine, policy-driven advanced threat detection and orchestration</td>
<td>Drastically reduce the time between detection and response, resulting in</td>
</tr>
<tr>
<td></td>
<td>fewer successful attacks and less downtime</td>
</tr>
<tr>
<td>Advanced mitigation options beyond a simple block or allow</td>
<td>Dynamically shape and manipulate internal and externally facing attack</td>
</tr>
<tr>
<td></td>
<td>surfaces, forcing the adversary to pivot tactics or even targets</td>
</tr>
</tbody>
</table>

ABOUT LOOKINGGLASS CYBER SOLUTIONS

LookingGlass is the leader in intelligence-driven risk management, offering the industry's most comprehensive and integrated cybersecurity solutions to the market. Our deep portfolio of flexible tools and technologies, supported by a global team of analysts, makes security seamless for enterprises and governments worldwide. We deliver relevant and tailored threat intelligence and response, making LookingGlass an insightful, proactive partner to organizations of all sizes. When intelligence informs product development, you get innovative solutions.

Learn more at http://www.LookingGlassCyber.com

© 2020 LookingGlass Cyber Solutions, Inc. All rights reserved.