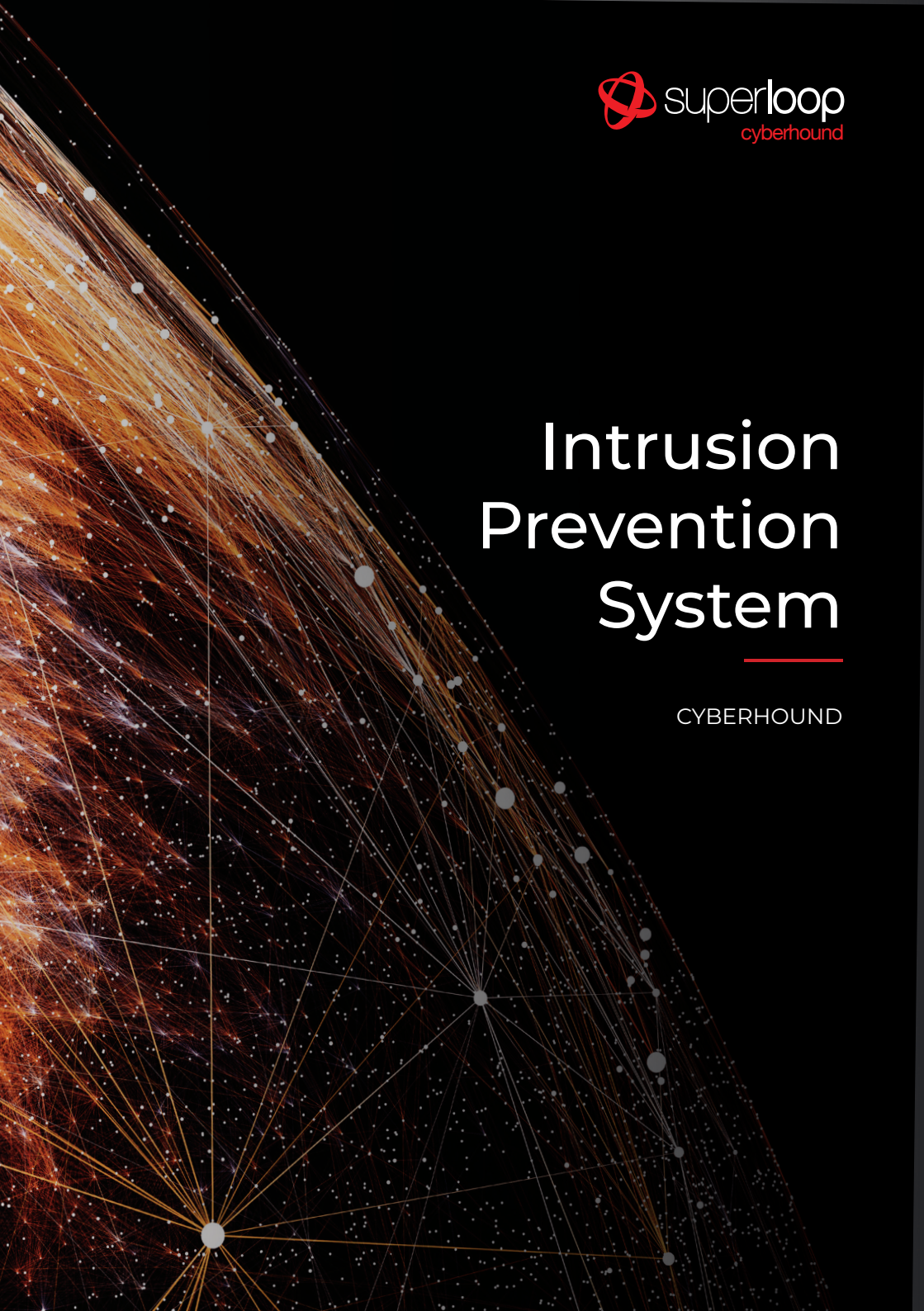

Intrusion Prevention System

CYBERHOUND

superloop cyberhound

AUG2019

Specifications

The Next Generation CyberHound Intrusion Prevention System (IPS) delivers enhanced performance, scalability and protection against malicious network threats. The inline IPS platform can identify threats from a wide range of threat vectors, enabling malicious traffic to be blocked, events alerted and real time reporting.

Severe threats to the network may instigate automated device blacklisting as well as provide threat intelligence feeds to a third party network access control service.

Network Controls

Flexible IPS Policy actions provide controls by category, rule and severity- to block, alert, permit or blacklist network traffic and offending devices, thus minimising threats to the network.

Threat Detection

The Intrusion Prevention System utilises over 12,000 rules to scan for malicious content such as Trojans, Viruses, DoS attacks, Botnets and other threats.

Reporting and Logging

IPS events are visible within CyberHound's XGen reporting platform for analysis. Security events can be seamlessly logged to a third party SIEM for further review and event analysis.

Rulesets

IPS rules are distributed using Superloop's cloud infrastructure via daily updates. IPS rules use 9 granular categories to ensure maximum flexibility and protection to the network.

Third Party Integration

The IPS engine has been integrated with Aruba ClearPass for security policy enforcement. Infected devices can be automatically quarantined or removed.

Performance

Hyperscale architecture allows the IPS engine to scale, delivering enhanced performance for high throughput networks.