OVERWATCH OT/IOT SECURITY SERVICE DESCRIPTION

1. OVERVIEW

With the rise of critical device IoT implementation in the modern office, manufacturing or medical spaces comes the added complexities of securing Internet-connected devices that cannot benefit from additive software protections, such as EDR.

Overwatch OT/IoT Security Service is designed to provide your organization with robust security measures for your Internet of Things (IoT) infrastructure, in an agent-less solution that segments these IoT devices from the local area network (LAN) with general network micro-segmentation for increased security posturing across the network attack surface.

Overwatch OT/IoT Security service is a comprehensive solution that deploys, manages, and maintains segmented IoT networks to minimize security risks and enhance overall cybersecurity by leveraging expertly deployed Airgap, to divide your network into smaller, isolated segments, limiting communication between devices or systems to only those that require it.

Overwatch OT/IoT Security provides two primary benefits: 1) Limiting the attack surface for the individual devices, thus limiting the scope of malicious activity (such as the spread of ransomware in the environment) by preventing the devices from having general access to the network (micro-segmentation) and 2) providing increased logging potential from such devices that otherwise would not be primed to share such telemetry with a security monitoring service.

The Overwatch OT/IoT Security solution provides these benefits, enforcing segmentation without the need to install software agents on individual devices, or interrupt network traffic to implement complex and expensive NAC switches.

2. SERVICE DEPLOYMENT

Overwatch OT/IoT Security deployment includes:

2.1 NETWORK & SECURITY INFRASTRUCTURE ANALYSIS

The deployment process begins with a thorough analysis of the existing network and security infrastructure. Our team of cybersecurity experts assesses the current systems, the type of data being handled, and the threat conditions facing the environment. This step is crucial in understanding the specific security needs of your organization and creating a tailored micro-segmentation strategy.

2.2 IMPLEMENTATION

The Overwatch team will install and configure two (2) hardware appliances in a high availability manner (HA) for each of the customer's sites.

2.3 CONFIGURATION

The Overwatch Team will configure the Airgap technology with the necessary VLAN(s) for network micro-segmentation and develop group and policy definitions to be applied to the Project environment and validated by the Customer.

2.4 LEARNING MODE ANALYSIS AND DOCUMENTATION

Overwatch will provide documentation on network configurations as well as configurations on Airgap with groups and policies based on a learning mode period of at least 14-days to 30-days depending on the complexities and scope of the deployment.

2.5 MONITORING

Overwatch will monitor all alerts generated in the Airgap console via SIEM/SOAR integration. Alerts will be based on predefined thresholds established in the Playbook and generated via the Airgap appliance. Specific Ransomware KillSwitch (RWKS) response policies can be defined based on behavior such as locking down all lateral movement in a network based on IDS telemetry.

3. SERVICE ONBOARDING

Overwatch will design and deploy a micro-segmentation solution into the client's environment to achieve network and IoT policy-based device segmentation and monitoring. A pair of Airgap gateways (Active/Passive High Availability) will be deployed per site (Virtual Machine options available to deploy on client-supplied hardware or new hardware procured and delivered by Airgap to client location), installed (by Overwatch technician) into client-supplied rack-space and client-supplied network.

The gateways will be configured to connect to the Airgap portal and validated for initial functionality. An initial "best practices" policy configuration will be implemented after passing review by the client stakeholders for the project. "Learning mode" will be implemented to help further refine the policy needs for the specific environment.

3. SERVICE MANAGEMENT

Overwatch OT/IoT Security service includes:

3.1 24/7/365 US-BASED MONITORING AND RESPONSE

Overwatch OT/IoT service offers round-the-clock monitoring by our 100% US-Based SOC Analysts to ensure consistent protection of your network. We identify and neutralize threats before they can cause significant damage, mitigating the risk of downtime and data loss.

3.3 REGULAR REPORTING & REVIEW

Our service includes regular reporting, giving you an overview of your security posture, the threats we've neutralized, and any potential areas for improvement. Regular reviews are conducted to ensure the service evolves with your organization and continues to provide the most effective protection.

3.4 CONTINUOUS UPDATES & MAINTENANCE

Overwatch OT/IoT Security is continuously updated to respond to the latest threat trends and vulnerabilities, with new detection rules and SOAR response pathways added in as emerging threats become known. Regular maintenance ensures the efficiency and effectiveness of the service, minimizing your cybersecurity risks.

3.5 POST-DEPLOYMENT SUPPORT

Post-deployment, we provide ongoing support to ensure the service, platform and Airgap integration are functioning optimally. Our support team is available 24/7 to answer any queries or concerns you may have. We operate as your tier 1 and 2 tech support for all deployed services with dedicated SMEs on staff.

4. BENEFITS

Overwatch OT/IoT Security provides your organization with a proactive and comprehensive security solution tailored specifically for the unique challenges posed by IoT devices. By implementing segmented networks, strict access controls, and robust monitoring, we aim to protect your sensitive data, prevent lateral movement of threats, and maintain the integrity and availability of your IoT infrastructure. With our experienced team and ongoing maintenance, you can trust that your IoT environment is in safe hands, enabling you to focus on your core business operations without compromising on security.

This service offers:

- Improved security: It helps prevent lateral movement of threats like ransomware and supply chain attacks, and contain breaches, limiting the impact of a compromised device.
- Reduced attack surface: By isolating devices, the attack surface available to potential attackers is significantly reduced.
- Enhanced compliance: micro-segmentation can help organizations comply with industry-specific regulations that require strong security measures.
- Easier monitoring and management: smaller segments make it easier to monitor and control the traffic and behavior of IoT devices, allowing for more effective management.
- Minimized impact of IoT device vulnerabilities: Since IoT devices often have limited security features, micro-segmentation can help mitigate the impact of their potential vulnerabilities.

Together, Overwatch OT/IoT Security offers a comprehensive security solution that offers robust protection for your network and Internet-connected devices.