Security Operations

Introduction

Security Operations is a race between attackers and defenders, the quicker a threat can be detected and responded to, the lower the risk presented to a firm. Automation through configuration management and increased collaboration holds the key to providing effective security operations and a prerequisite to enabling AI-driven Security Operations Centres.

Upon successful investigation and analysis of an incident, configuration management is the secret to reducing the mean time to resolution. Orchestrating policy changes to the network, endpoints and services through automation of configuration deployment and drift monitoring achieves the closed loop desired by the industry.

Executive Summary

Effective security operations rely upon access to good information from the IT estate and a means to effect change in response to threats. Efforts are hampered by the cost and, in the case of a global operation, the local legal authority to collect, process and store security data, coupled with the traditionally manual means to change the network to be better protected.

Through a configuration management approach to Security Operations, we believe we offer differentiated services that enable faster and more comprehensive means to discover and react to extant threats whilst reducing cost.

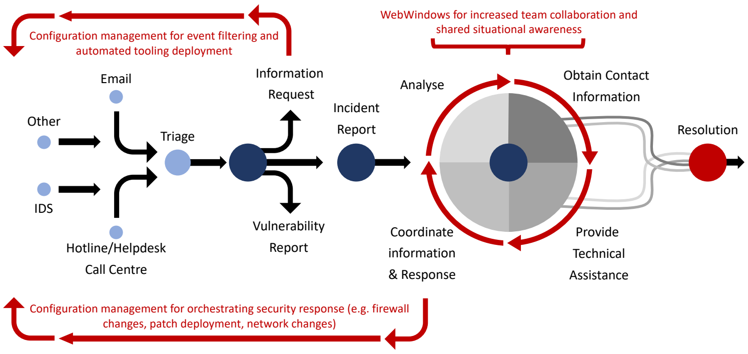
To make a difference, security teams do not necessarily need bigger data, they need smarter collection and action.

Automating investigation and response

Decentralisation of the Security Operations Centre

Collection and processing of security events in a decentralised fashion, allowing for the detection of incidents on platforms at the edge of the network, such as IoT and IT systems with limited connectivity providing capability in challenging operational environments.

In this way, decentralisation allows for reduced network costs, only requiring the movement of large security datasets when the situation requires. Raising the fidelity of events that human analysts have to triage and investigate means they have fewer events that would otherwise consist of noise, freeing them to investigate more complicated threats - using configuration management to open the taps and deploy analytics to filter through events.



Configuration management for event filtering and automated tooling deployment

WebWindows for increased team collaboration and shared situational awareness

Configuration management for orchestrating security response (e.g. firewall changes, patch deployment, network changes)

Email
Other
IDS
Hotline/Helpdesk Call Centre
Triage
Information Request
Vulnerability Report
Incident Report
Analyse
Obtain Contact Information
Coordinate information & Response
Provide Technical Assistance
Resolution

Increased collaboration whilst preserving privacy and data sovereignty

Configured Things' WebWindows compositing engine provides the means to improve collaboration between analysts, incident responders, management and, in the case of Managed Security Service Providers, customers.

WebWindows fuses web content from multiple systems, when coupled with configuration management that allows analytics that can be dynamically deployed into data paths, privacy preserving controls can be implemented on demand. This system enables policy-compliant safe-sharing of data between geographies, automatically redacting, pseudonymising and anonymising as policy allows, ensuring your business' ongoing regulatory compliance.

ConfiguredThings