Solution Brief

Using Skybox Security Solutions with ArcSight

Skybox ‘network aware’ risk assessment complements SIEM event correlation

Solution Overview

The amount and complexity of IT security information generated by today’s collection of IT tools is staggering. IT managers often use Security Information and Event Management solutions, such as those offered by ArcSight, to collect and analyze event-based information, alerting the IT team to unusual events that need more examination or response.

But effective response to contain threats and limit potential damage from cyber attacks requires quick ‘network-aware’ risk assessments. Skybox Security delivers proactive security risk management solutions that complement a SIEM, delivering situational awareness for network managers, eliminating false positives and reducing the window of risk exposure.

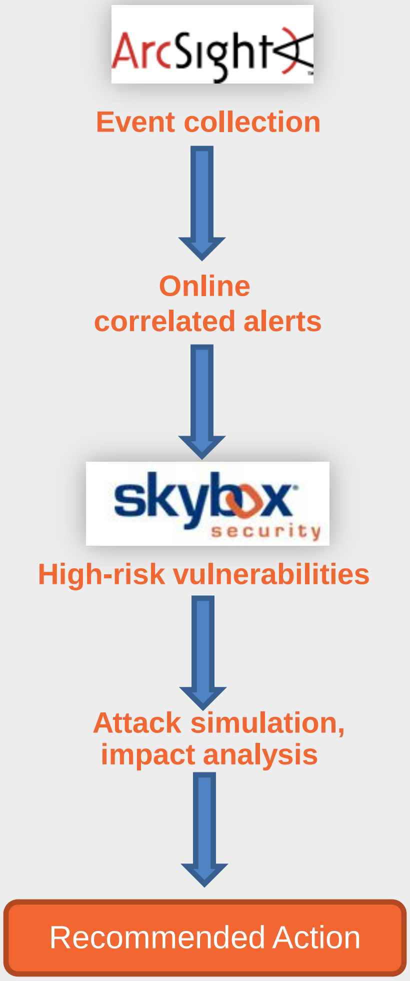
Customers using Skybox solutions in conjunction with ArcSight achieve:

- **Fewer false positives** by correlating ArcSight events with risk-based vulnerability assessment from Skybox Risk Control
- **Faster response times** by using Skybox solutions to analyze attack paths and recommend remediation options
- **Reduced firewall risks** by integrating Skybox Firewall Assurance data with ArcSight logging and alerts
- **Superior risk information** for each business unit, leveraging Skybox for asset classification and organizational mapping

Skybox Solutions for Security Risk Management

- Skybox® Risk Control
- Skybox® Network Assurance
- Skybox® Firewall Assurance

Integration of Skybox and ArcSight



Risk-based Alert Prioritization

Skybox Risk Control correlates network, threat, and vulnerability data, using attack simulation to confirm a list of severe, exploitable vulnerabilities. Regular vulnerability scanners do not differentiate exploitable vulnerabilities from ones that cannot be exploited due to network topology or security controls.

ArcSight can correlate Skybox vulnerability assessments with actual attack information. This focuses attention on critical events fast, avoiding low-impact alerts or false positives.

Attack Simulation and Visualization

Skybox Risk Control and Skybox Network Assurance provides a complete network modeling and simulation 'sandbox' to assess potential attack paths into the network. With Skybox solutions, IT managers can quickly drill down to the exact rules that allow the access.

Combined with ArcSight data on attack source and destination, users can display attack information on the Skybox network map, and analyze the network controls and access rules.

Firewall Compliance and Misconfiguration Alerts

Skybox Firewall Assurance automatically identifies firewall rules and misconfigurations that could lead to a security breach.

When Firewall Assurance detects a risky firewall configuration change, Skybox can generate a new event for ArcSight Logger. Plus, Skybox can deliver comprehensive firewall compliance information to ArcSight compliance reporting modules.

Integration Options

Standalone operation - When responding to ArcSight event information, IT managers can activate the Skybox applications as standalone tools to provide network-aware risk analytics.

Custom integration – Skybox and ArcSight solutions can be integrated closely to provides a seamless risk management experience. The Skybox web API plus data export/import capabilities allow risk assessments to be triggered based on events, and sharing of data. Ask your solution partner about integration services or contact Skybox Professional Services.

About Skybox Security

Skybox Security, Inc. is the leader in proactive security risk management solutions, helping IT managers predict critical risks and take action to prevent data breaches, cyber attacks, and policy compliance violations. Our solutions automatically examine comprehensive network security and cyber threat data – delivering extensive intelligence in minutes. Medium to large organizations in Financial Services, Utilities, Telecommunications, Retail, Government and Defense rely on Skybox Security solutions to continuously reduce risks and maintain compliance. For more information visit **www.skyboxsecurity.com, email info@skyboxsecurity.com, or call +1(408) 441-8060**