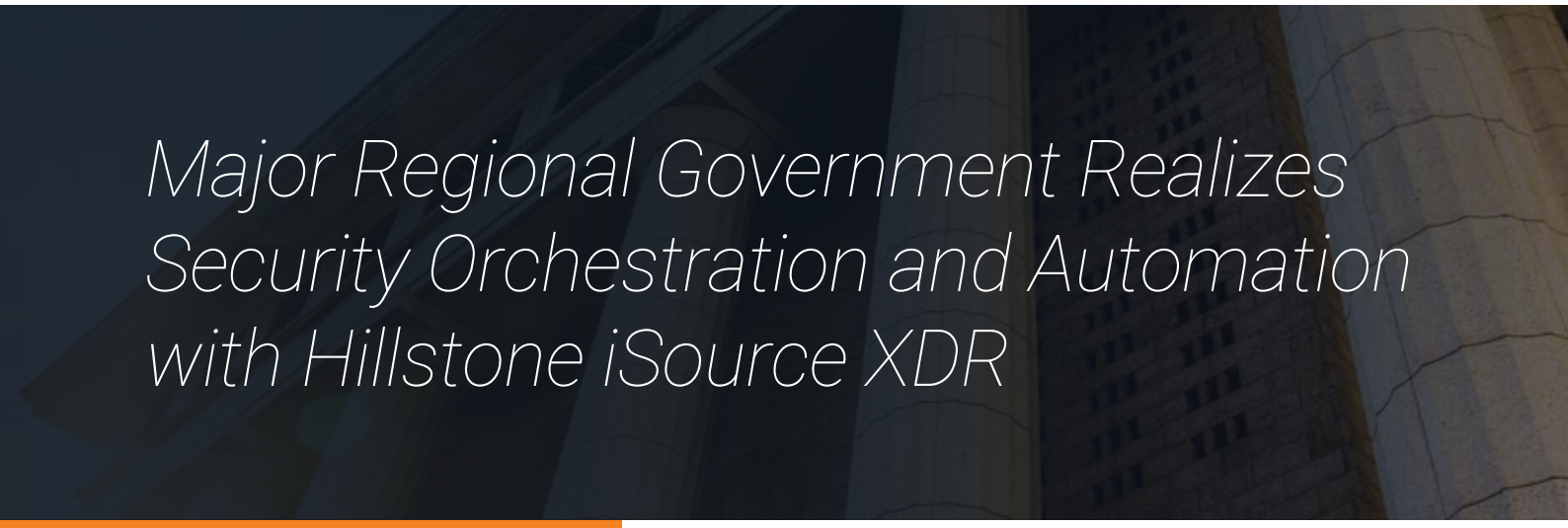
Hillstone NETWORKS



Major Regional Government Realizes Security Orchestration and Automation with Hillstone iSource XDR

The Customer

A major regional government with more than 60 subsidiary agencies, each containing 400+ employees. Despite this, each agency possesses only one or two information service specialists to oversee daily operations. Total inbound traffic reaches over 100 GB, with dozens of nodes for traffic information collection. The government has a network architecture consisting of multiple security zones, including the core business, intranet, publishing, border, virtualization, cloud, security management, and others. Interactions between business systems and security zones are also quite frequent. Currently, the customer realizes essential security capabilities via firewalls, IPS, IDS, EDR, and other virtualized security products.

The Challenge

The customer faced several challenges brought on by an increase in cyber risks and an elevated complexity of the threat landscape. For example, the business operations system relies heavily on passive threat prevention, and large numbers of security logs require manual analysis – which together increases the workload while reducing efficiency of security managers. Meanwhile, as changing national security policies increase requirements on network security, threat monitoring, and O&M, the customer needs to elevate its proactive protections, construct an automated defense system, and achieve a closed-loop operation system.

In the short term, the customer's targets involved shortening the time to remediate threats, improve security operation efficiency through automated incident response, prioritize security operations workloads, and unify security management procedures to enhance team collaboration.

As for long-term goals, the customer requires a standardized solution to enhance security operation maturity. The solution should help analysts combine the accumulated security experience into playbooks and provide a more flexible and customized means to optimize security operations.

Major Regional Government Realizes Security Orchestration and Automation with Hillstone iSource XDR

The Solution

In alignment with the customer's security goals, network architecture, business processes, operational capabilities, and existing network security architecture, Hillstone's iSource Extended Detection and Response (XDR) solution was implemented in the security management zone.

The Hillstone iSource XDR solution collects data such as threat incidents, event logs, and traffic analysis results from each security device in the network. It then integrates and synergizes the data, investigates correlations of incidents, identifies potential threats, and orchestrates security responses across existing security solutions.

Hillstone iSource provides comprehensive risk management for assets like servers, endpoints, applications and services across multiple dimensions, including traffic, behaviors, risks, vulnerabilities, and threats. It can sync up with various security devices to provide comprehensive and cohesive protection. When synchronized with network security devices like NGFW, IPS, and cloud-based security products, the capabilities can be extended to policy configuration and traffic blocking. When linked with top threat intelligence sources, iSource can discover even evasive and stealthy threats.

Hillstone iSource XDR platform can respond quickly and make intelligent decisions based upon playbooks. Since certain third-party devices can also be supported in playbooks via RESTful APIs or SSH connection, iSource XDR additionally offers automated security orchestration and cohesive response through integrated interactions with these security products.

Based on machine learning (ML) and artificial intelligence (AI), Hillstone iSource uses Kafka, a distributed publish-subscribe messaging system, to connect various modules to the message bus. This enables automated operation and processing of the data flow.

For the customer, Hillstone iSource helps realize machine-human collaboration. By training the XDR platform with samples from real-time traffic, it can run statistical simulations and perform baseline behavior modeling for advanced detection capabilities. After generating playbooks based on security incidents and threat intelligence, iSource XDR can achieve one-click deployment assisted by manual verification.

Another reason the customer chose Hillstone iSource is its ease of use. With a graphical visualization dashboard and the combination of built-in playbooks, event correlation, and highly accurate and automated alerts, Hillstone iSource XDR helps reduce the complexity of security operations significantly.

The Conclusion

With security orchestration and automation, Hillstone iSource Extended Detection and Response (XDR) has helped the client streamline complex security operations, transform disparate security tools and functions into a cohesive security response, and optimize security operation capabilities.

By combining the security posture and threat environment, the customer has strengthened threat alerting, detection, and response capabilities and improved security operation efficiency.

Hillstone NETWORKS

Visit **www.hillstonenet.com** to learn more
or contact Hillstone at **inquiry@hillstonenet.com**