CHECK POINT + SERVICENOW

ACCELERATING CYBER THREAT PREVENTION AND RESPONSE IN THE CLOUD

Benefits

- Real-time threat prevention
- Identify mission-critical security incidents
- Accelerate incident response
- Eradication of zero-day attacks
- Automatic or manual blocking

INSIGHTS

Companies often deploy an assortment of point solutions to protect their critical assets from the proliferation of cyber threats. While implementing additional solutions may seem more secure, too many solutions can overload IT personnel, increase complexity and add unnecessary costs. Traditional response techniques rely on manual measures and IT staff to correlate heaps of information, identify mission-critical incidents and act on potential threats. The lack of communication among security solutions also leaves companies susceptible to zero-day exploits and weaponized documents. To combat these issues, Check Point and ServiceNow are closing the security gap by preventing and responding to cyber threats with a seamless integration to protect critical assets as well as users.

SOLUTION

Check Point has partnered with ServiceNow to combat the rise of cyber-attacks and make security response more efficient. By integrating Check Point's Next-Generation Threat Prevention Platform with ServiceNow® Security Operations enterprise security response solution, joint customers can accelerate threat prevention and eradication throughout the network and cloud. ServiceNow receives mission-critical Threat Prevention events from Check Point that require immediate attention and prioritization. In real-time, ServiceNow creates security incident records and triggers workflows to accelerate threat identification and remediation within the organization.

IDENTIFY AND BLOCK THREATS IN REAL-TIME

Cybercriminals are becoming more sophisticated and are enhancing their techniques to deploy zero-day attacks in order to bypass legacy security solutions. Check Point's SandBlast Zero-Day Protection combines CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous zero-day attacks and weaponized documents. Check Point can block these unknown attacks coming from the network, endpoint and cloud, and send these Threat Prevention events to ServiceNow. This real-time communication between Check Point and ServiceNow will improve the performance of prevention systems as well as incident response, ultimately saving time and money.

As hackers try to establish a command-and-control (C&C) channel of communication to export sensitive information to the outside, Check Point's Anti-Bot software blade identifies and blocks this C&C traffic. In parallel, Check Point instantaneously sends this mission-critical C&C event to ServiceNow Security Operations to initiate an incident response workflow. This accelerated response eradicates the attack and prevents lateral infections within the company's network and cloud.

RESPOND TO MISSION-CRITICAL SECURITY INCIDENTS

Check Point's mission-critical security events are sent to ServiceNow Security Operations to accelerate prevention, response and eradication. When the security event is received by Security Operations, a security incident is automatically created containing information received from Check Point. Incident criteria trigger response workflows to gather more data such as threat intelligence from other tools, and automatically assign the incident to the correct teams for response. Security incidents can also be correlated with the ServiceNow configuration management database (CMDB) to prioritize them based on business criticality.

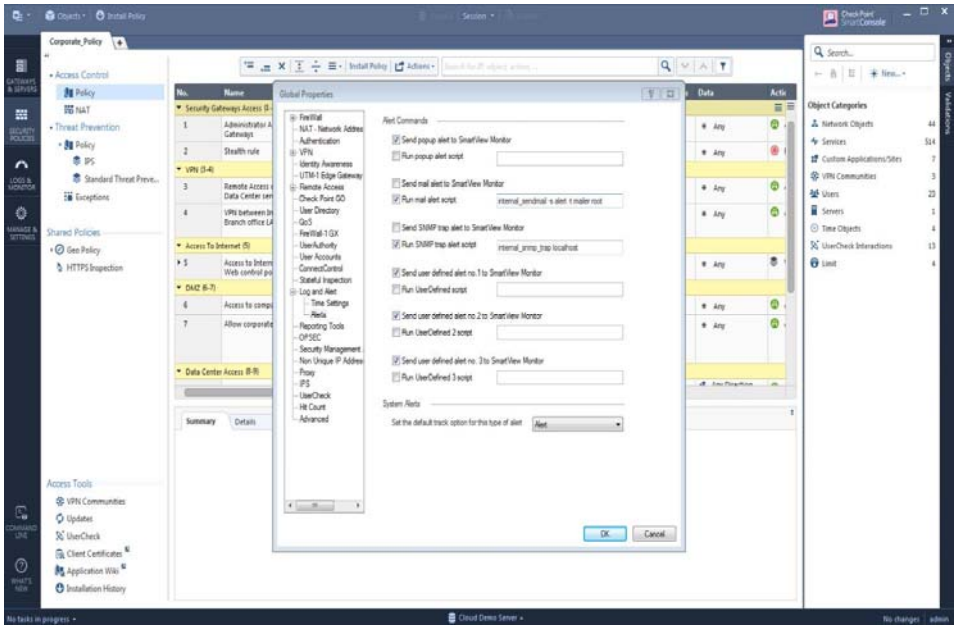

Fig. 1: Check Point SmartConsole

When incident resolution requires collaboration with IT, ServiceNow provides visibility across teams while keeping sensitive data secure. Related IT tasks are associated with the security incident to provide security teams visibility into their assignment, and security incident data is not visible to IT teams unless deemed necessary.

Because events and incidents are tracked within ServiceNow, an organization can get visibility into their overall security posture through metrics, dashboards, and reports. Post-incident reviews are automatically created for each security incident, including a time-stamped record of activities, work notes, and assessments from participants.

SUMMARY

The real-time communication between Checkpoint and ServiceNow empowers organizations with the information they need to stop zero-day exploits and weaponized documents. Real-time detection and comprehensive incident response are critical to avoid a full network breach. By integrating Check Point's Next-Generation Threat Prevention Platform with ServiceNow Security Operations, security and IT teams are able to quickly identify and eradicate cyber threats. By adding ServiceNow Security Operations to an organization's security suite, time to detection is reduced, detailed attack forensics are gathered, and mission-critical alerts are raised, ultimately improving a company's ability to defend against the most advanced cyber-attacks. Paired with Check Point's Next Generation Threat Prevention Platform, customers fortify their prevention capabilities with automatic or manual blocking, detailed information for remediation, and incident response. By utilizing this joint solution, security and IT teams can leverage workflows and automation, thereby accelerating threat identification and remediation.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest network cyber security vendor globally, providing industry-leading solutions and protecting customers from cyber-attacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises – from networks to mobile devices – in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

ABOUT SERVICENOW

ServiceNow (www.servicenow.com) is changing the way people work. Customers use our platform to define, structure and automate the flow of work, removing dependencies on email, spreadsheets and other manual processes to transform the delivery of service to the enterprise. With ServiceNow Security Operations, customers can bring incident data from their security tools into a structured enterprise security response engine that uses intelligent workflows, automation, and a deep connection with IT to prioritize and resolve threats based on the impact they pose to your organization.

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com