Improve Visibility and Agility– Infoblox DDI Now Integrates with ServiceNow Security Operations

Infoblox has integrated with ServiceNow Security Operations to enable mutual customers to receive alerts on potentially compromised hosts, and to quickly respond to network changes and security events, enabling next-level efficiency for security operations team.

Challenges

Today's enterprise network consists of a large number of network and security devices. All these devices generate their own incidents, but often don't always share information. This lack of interoperability and inability to share event data results in network and security tools working in silos with limited context. According to the Enterprise Strategy Group research report on Security Operations Challenges, Priorities and Strategies in 2017, keeping up with the volume of security alerts and integrating different security tools are the biggest challenges related to security operations. According to the same survey, investing in technologies that automate security operations and threat detection is a top priority for security teams today. Organizations are investing heavily in automation/orchestration of incident response to keep up with volume of security alerts, prioritize alerts and decision making, and shorten response time. ServiceNow Security Operations is used by many organizations to get single pane of glass visibility into security incidents and improve the efficiency and speed of incident response. When customers see potentially compromised hosts and security events in single place, they can proactively identify threats and hence, respond faster and more efficiently.

Joint Solution

Amid all this complexity, customers want the confidence to know their network and security is tightly integrated and built on a rock solid, Tier 1 foundation that cannot fail. Infoblox makes it easier to have tight integration between network and security, with the most extensive threat intelligence and API integrations. The integration with ServiceNow Security Operations enables security response teams to effectively monitor, escalate and investigate DNS security incidents and mitigate risks through a tight integration with BloxOne™ Threat Defense, Advanced DNS Protection and Threat Insight. Thus, integration between Infoblox and ServiceNow increases visibility, provides next level efficiency for security operations and maximizes ROI for security investments already made.

Security Incidents

RPZ/ADP rules management and TI whitelist management
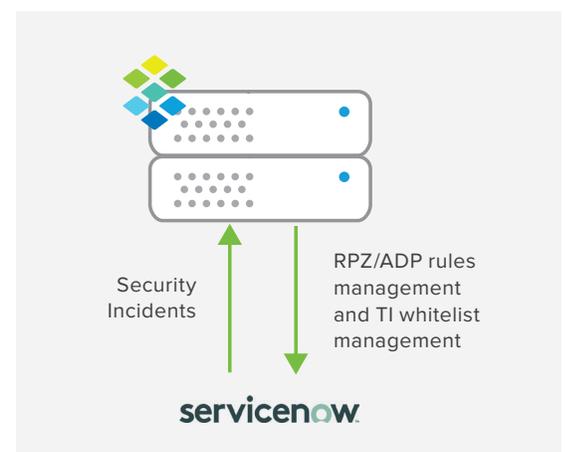
If suspicious DNS activity is detected, Infoblox opens a new record in the Security Incident Response application within ServiceNow Security Operations to notify security ana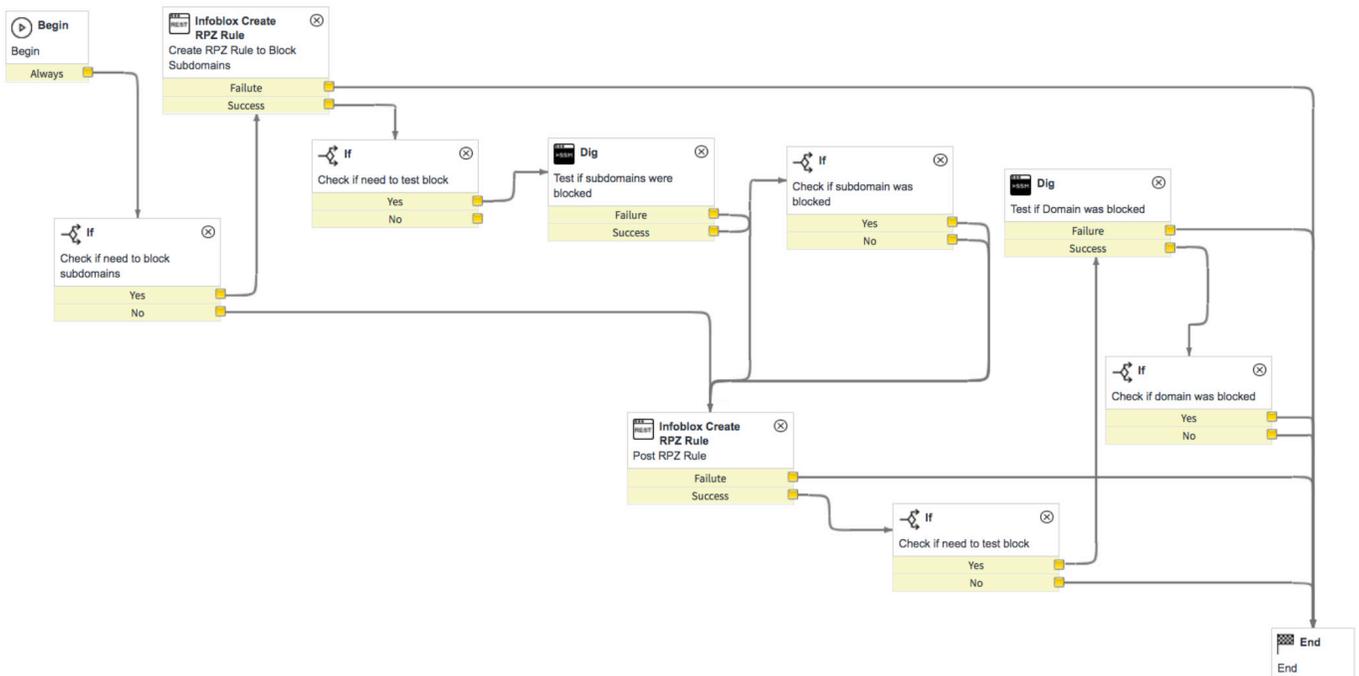lysts about potentially compromised devices and infected hosts. Security admins can manage security incidents and Indicators of Compromise (IoCs), discovered by Infoblox, in the ServiceNow UI as shown below.
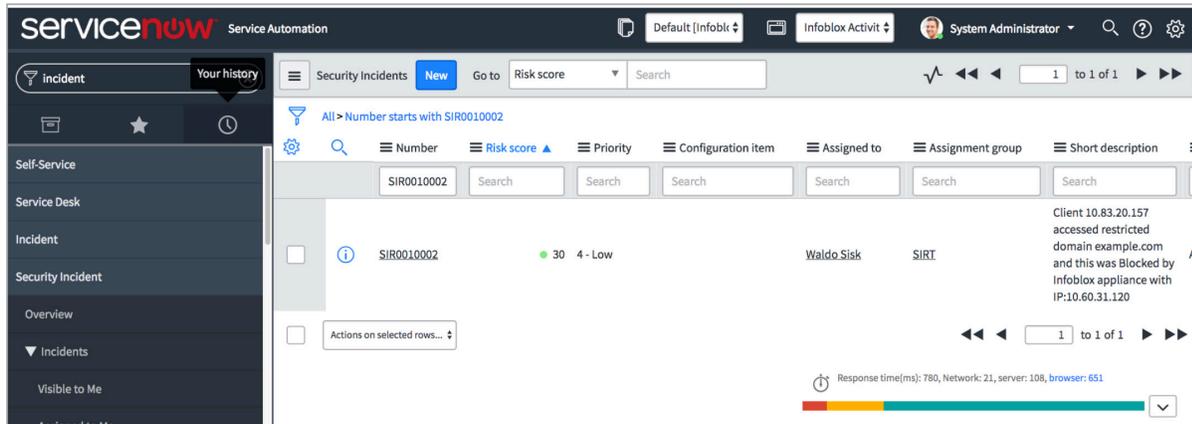
Customers will need an Security Ecosystem license for this integration. To receive network information from Infoblox, they need a DDI license and to receive threat information, they need both RPZ and Threat Intelligence licenses. This integration was built by Infoblox and is supported by the Infoblox community.

Customers may also download Infoblox's application from the ServiceNow Store providing multiple activities including managing RPZ rules. The Infoblox App for ServiceNow Security Operations additionally comes packed with more than twenty valuable activities to manage RPZ and ADP rules as well as assets. For example, with the Infoblox app, users can create Threat Intelligence whitelists to automate security incident response via workflows on ServiceNow across the Infoblox Grid.

Summary

The Infoblox and ServiceNow joint solution provides following benefits to the customers:

Single pane of glass visibility into infected hosts: Integration between Infoblox and ServiceNow Security Operations provides visibility into potentially compromised hosts and infected devices.

Notification of DNS threats: Whenever Infoblox detects a potential DNS threat, it notifies ServiceNow Security Operations, allowing security admins to quickly respond to threats.

Faster incident response: Allows customers to receive the latest information on incidents, thereby enabling them to respond to DNS security events and threats faster, enabling next level efficiency for security operations team.

To learn more about this integration and demo, please visit https://community.infoblox.com/t5/ServiceNow/gp-p/SERVICENOW

About ServiceNow

ServiceNow was started in 2004 with the belief that getting simple stuff done at work can be easy, and getting complex multi step tasks completed can be painless. From the beginning, ServiceNow envisioned a world where anyone could create powerful workflows to get enterprise work done. Today, ServiceNow's cloud-based platform simplifies the way we work through a structured security response engine. ServiceNow Security Operations automates, predicts, digitizes, and optimizes security and vulnerability response to resolve threats quickly based on business impact. Reduce manual processes and increase efficiency across security and IT teams. ServiceNow is how work gets done. To find out how, visit: http://www.servicenow.com/sec-ops.

About Infoblox

Infoblox leads the way to next-level DDI with its Secure Cloud-Managed Network Services with 8,000 customers including 350 of the Fortune 500. Infoblox brings next-level security, reliability and automation to cloud and hybrid systems, setting customers on a path to a single pane of glass for network management. Next-level security helps protect against the rising flood of cyberattacks, leveraging 14 billion threat indicators and 30 plus API security integrations. Next-level reliability provides a Tier 1 foundation with five nines availability, delivered as software-defined services. Next-level automation overcomes complexity, solving problems with intelligence from 17 trillion daily DNS queries. Visit http://www.infoblox.com