crest(data)

CASE STUDY

SERVICENOW · SECURITY INCIDENT RESPONSE

# Reducing Turnaround Time Through Automated Threat Prevention to Accelerate Security Operations

**IP · URL · Domain**
Malicious observables blocked from incidents

**Multi-Gateway**
Block lists managed across security gateways

**Automated**
Entry expiration & block-list hygiene

**Lower TAT**
Reduced SOC threat-response turnaround

## Executive Summary

THE OPPORTUNITY

When security analysts manually manage modern threats across a diverse set of security products — correlating heaps of information and acting on potential threats — it often leads to **critical security gaps**. A leading provider of IT security software and hardware needed to enable its security teams to block malicious IP addresses, URLs, and domains using **block request list capabilities within the ServiceNow Security Incident Response framework**. Responding to potential threats remained a labor-intensive task in the absence of a streamlined automated process, limiting the analyst's ability to act quickly.

To address these challenges, Crest Data developed an integration enabling security analysts to **create block list entries from malicious observables within ServiceNow security incidents**. The solution offered robust capability to manage multiple block lists that apply to multiple gateways, automate entry expiration, and link block list data with detailed threat intelligence. This integration **significantly reduced turnaround time** by enabling SOC analysts to block malicious observables seamlessly.

## About the Customer

A **leading multinational provider of comprehensive IT security solutions**, offering a wide array of software and integrated hardware products.

They hold **extensive expertise across multiple domains** — network security, endpoint security, cloud security, mobile security, data security, and security management.

CUSTOMER PROFILE

INDUSTRY
**IT Security — Software & Hardware Provider**

REACH
**Multinational, comprehensive security portfolio**

DOMAINS
**Network, endpoint, cloud, mobile & data security**

PLATFORM
**ServiceNow Security Incident Response**

## The Customer Challenge

MANUAL, SLOW & DISCONNECTED

As a multinational security vendor, the customer's analysts were held back by **manual, disconnected threat-response workflows** that couldn't keep pace with modern threats.

**Manual correlation across products.** Correlating vast amounts of information gathered from different security products was a manual process — analysts couldn't act on potential threats quickly, creating **critical security gaps**.

**No native block-list capability.** Teams needed to block malicious IP addresses, URLs, and domains using **block request list capabilities within the ServiceNow Security Incident Response** framework.

**High turnaround times.** Responding to malicious observables without a robust automated integration between their threat-prevention platforms and security operations workflows resulted in **higher turnaround times**.

> The customer needed a **robust, automated integration** that connected threat-prevention controls directly to SOC workflows — so analysts could block malicious observables from within an incident, without leaving ServiceNow.

## Proposed Solution

BLOCK FROM THE INCIDENT

Crest Data developed an integration for the **Security Operations (SecOps) framework**, letting analysts create block list entries directly from malicious observables identified in security incidents — and manage them at scale across the environment.

### Block from Observables

Analysts **create block list entries from malicious observables** identified within ServiceNow security incidents.

### Multiple Lists & Gateways

Greatly increased flexibility to **manage multiple block lists across various security gateways** from one place.

### Detailed Reporting

Teams receive detailed reporting on the **nature of blocked sites** — such as those associated with phishing or malware.

### Automated Expiration

Automated expiration periods **maintain block-list size** by automatically removing older entries.

### Tagging & Central Search

Tagging of incidents by observable type — **URLs, domains, and IP addresses** — enables centralized search across block lists.

### Linked Threat Intel

Block list entries link to **incident records with detailed threat intelligence**, so analysts block observables seamlessly.

ⓘ The result: SOC analysts block malicious observables without leaving ServiceNow — cutting threat-response turnaround time.

## Outcomes

BUSINESS IMPACT

By connecting threat-prevention controls directly to the SOC workflow, Crest Data's integration translated into immediate, practical gains for the customer's security analysts.

### Reduced Turnaround Time

SOC analysts **block malicious observables seamlessly** from within incidents, significantly cutting threat-response turnaround time.

### Automated Threat Prevention

Malicious **IPs, URLs, and domains** are blocked directly from ServiceNow incidents — no manual, cross-product correlation.

### Centralized Management

**Multiple block lists across multiple gateways** are managed and searched in one place, with tagging by observable type.

### Self-Maintaining Lists

Automated expiration keeps block lists **lean and current**, removing stale entries without analyst effort.

## About Crest Data

AI-FIRST · SECURITY-LED

Crest Data is a data and AI-first product engineering and technology solutions provider with deep expertise in **cloud and AI, cybersecurity, observability, data analytics, and workflow automation**. With a team of **1,000+ experts**, **5,500+ successful projects** delivered, and **175+ global customers**, Crest Data applied its **SecOps and automation capabilities** to help the customer significantly reduce threat-response turnaround time by enabling the seamless blocking of malicious observables within the ServiceNow Security Incident Response framework.

Backed by strong partnerships with **ServiceNow, AWS, Google, Microsoft, Datadog, Dynatrace, and NetApp**, Crest Data delivers outcome-focused solutions that strengthen security, improve platform reliability, and enable sustainable digital growth.

ACCELERATE SECOPS WITH AUTOMATION

### Block malicious observables without leaving ServiceNow.

Talk to Crest Data's ServiceNow & SecOps experts about automating threat prevention, block-list management across gateways, and threat-intelligence-linked Security Incident Response.

Talk to Our Experts →

www.crestdata.ai/contact

EXPLORE SERVICENOW

crest(data)

USA · CA
3031 Tisch Way #602
San Jose, CA 95128

INDIA · AHMEDABAD
CDS House, SG Road
Makarba, Ahmedabad 382210

INDIA · PUNE
Amar Madhuban Tech Park
Baner, Pune, MH 411045

+1 (408) 551-0051 info@crestdata.ai www.crestdata.ai