Harbor Point Hospitality Group

A Threat Intelligence-Driven Solutions Architecture Case Study

Justin Goncalves

March 16, 2026

Agenda

1
Introduction and Objectives

2
Client Context and Environment

3
Current State Security Posture

4
Gaps, Friction, and Opportunities

5
Proposed Future State Security

6
Recommended Integrations

7
Use Cases

8
Closing Remarks, and Open Discussion

Overview

- Assessment of Harbor Point Hospitality Group's current security environment
- Identifying gaps in visibility, context, and incident response
- Evaluating how Recorded Future intelligence could close those gaps
- Proposing practical integrations using existing tools and workflows
- Demonstrating real-world use cases to show a measurable security impact
- Focusing on solutions that scale without adding operational complexity

Environment Overview

Harbor Point Hospitality Group

Composite, anonymized mid-size hospitality organization modeled on a real-world environment

The company includes six hotel locations and one corporate headquarters across the United States

A centralized corporate IT and security team is responsible for supporting technology operations and maintaining security oversight across all properties.

7 Properties, including a corporate office

400 - 600 Employees

IT and Security Model:

- Centralized IT team with overlapping IT and security responsibilities
- Managed Service Provider (MSP) for network and infrastructure operations.

Technology Posture:

- Hybrid, cloud-first architecture
- Some On-Prem Servers, for AD, Print Services, Shared Data Management, and Property Management System (PMS) Interfaces
- Microsoft 365 used for business productivity and communication
- All endpoints onboarded to Sentinel One EDR
- Security telemetry centralized within Microsoft Sentinel

Security Maturity:

- Foundational controls in place with limited automation and inconsistent operational use of threat intelligence

Industry Relevant Threats

Phishing and Credential Theft

Phishing campaigns target employees to steal credentials, enabling unauthorized access to email, cloud services, and remote access systems across the organization.

Identity and Access Abuse

Attackers exploit weak identity controls to escalate privileges, move laterally, and access sensitive systems such as property management platforms and cloud services.

Ransomware Attacks

Ransomware campaigns commonly target hospitality organizations to disrupt operations, encrypt critical systems, and pressure rapid payment due to business downtime.

Malware and Endpoint Compromise

Malicious files and scripts delivered via email or web activity can compromise endpoints, providing attackers with persistence and initial access into the environment.

In hospitality environments like this, these threats don't occur in isolation; they often overlap and compound each other, which is why intelligence and prioritization matter.

Security Organization Layout

Security Operations

- Internal IT/Security team monitors alerts from Sentinel and EDR
- Internal team validates alerts and determines security relevance
- Internal team escalates confirmed incidents to Incident Response

Incident Response

- Internal IT/Security team leads investigations and response actions
- MSP supports containment efforts and infrastructure changes
- Internal team documents incidents and tracks remediation

Threat Intelligence

- Internal security team consumes Recorded Future intelligence
- Internal team uses risk scores and context to support prioritization
- Internal team aligns intelligence with active alerts and threats

Networking

- Managed Service Provider (MSP) manages servers, firewalls and networking
- MSP implements blocking actions (IPs, domains) during incidents
- Internal team coordinates network changes with security needs

EDR and Vulnerability

- Internal IT/Security team monitors endpoint alerts via SentinelOne
- Internal team investigates endpoint detections and suspicious behavior
- Internal team tracks and remediates high-risk vulnerabilities

IT HelpDesk/Support

- Harbor Point IT serves as first point of contact for user issues
- HelpDesk identifies suspicious activity or security-related tickets
- HelpDesk escalates potential security incidents to Security Operations

Current State Security Architecture

Harbor Point Hospitality Group's security environment relies on a small set of core platforms for identity, endpoint protection, and monitoring across a distributed footprint. While these tools provide baseline visibility, correlation and prioritization are largely handled manually by the corporate IT team.

Identity and Access Management

- Microsoft Entra ID manages authentication, access control, and sign-in logging
- Identity logs are available, but typically reviewed reactively during investigations
- No automated, intelligence-driven risk scoring or proactive response tied to identity events

Endpoint Detection and Response

- SentinelOne provides endpoint protection and detection across corporate and hotel systems
- Alerts generated from behavioral and signature-based detections
- Alerts reviewed and investigated manually alongside other signals

Security Information and Event Management

- Microsoft Sentinel is the centralized SIEM for log collection and review
- Ingests data from identity systems, endpoints, and cloud services
- Alert review and triage performed manually (no dedicated SOC staffing)

Current State Security Architecture (cont.)

Harbor Point Hospitality Group's extended security architecture supports incident response and infrastructure operations through a mix of internal oversight and managed services. While foundational capabilities are in place, most response actions and coordination rely on manual processes and external support, limiting speed and consistency during security events.

Incident Response and Ticketing

- ServiceNow is the primary system for IT tickets and security incidents
- Incidents created from alerts, user reports, or observed issues
- Enrichment, prioritization, and context gathering done manually during investigation

Networking and Infrastructure

- MSP supports firewall and network infrastructure management
- Rule changes and network actions are typically reactive to identified incidents
- Blocking decisions require manual review and coordination between corporate IT and MSP

Security Orchestration, Automation, and Response

- Tines is assumed to be available as the SOAR platform
- Automation is currently limited; workflows depend on manual decisions
- Enrichment, security actions, and escalation are driven mostly by human effort

Operational Workflow

1

Alert Intake

- Alerts generated from EDR, email security, and cloud services
- Alerts ingested into Microsoft Sentinel
- High alert volume with limited initial context

2

Initial Review

- Internal IT/Security team reviews incoming alerts
- Analyst determines basic relevance and legitimacy
- Minimal threat intelligence available at this stage

3

Triage & Prioritization

- Alerts manually assigned severity and priority
- Decisions based on experience rather than standardized scoring
- Risk context varies depending on alert source

4

Investigation & Response

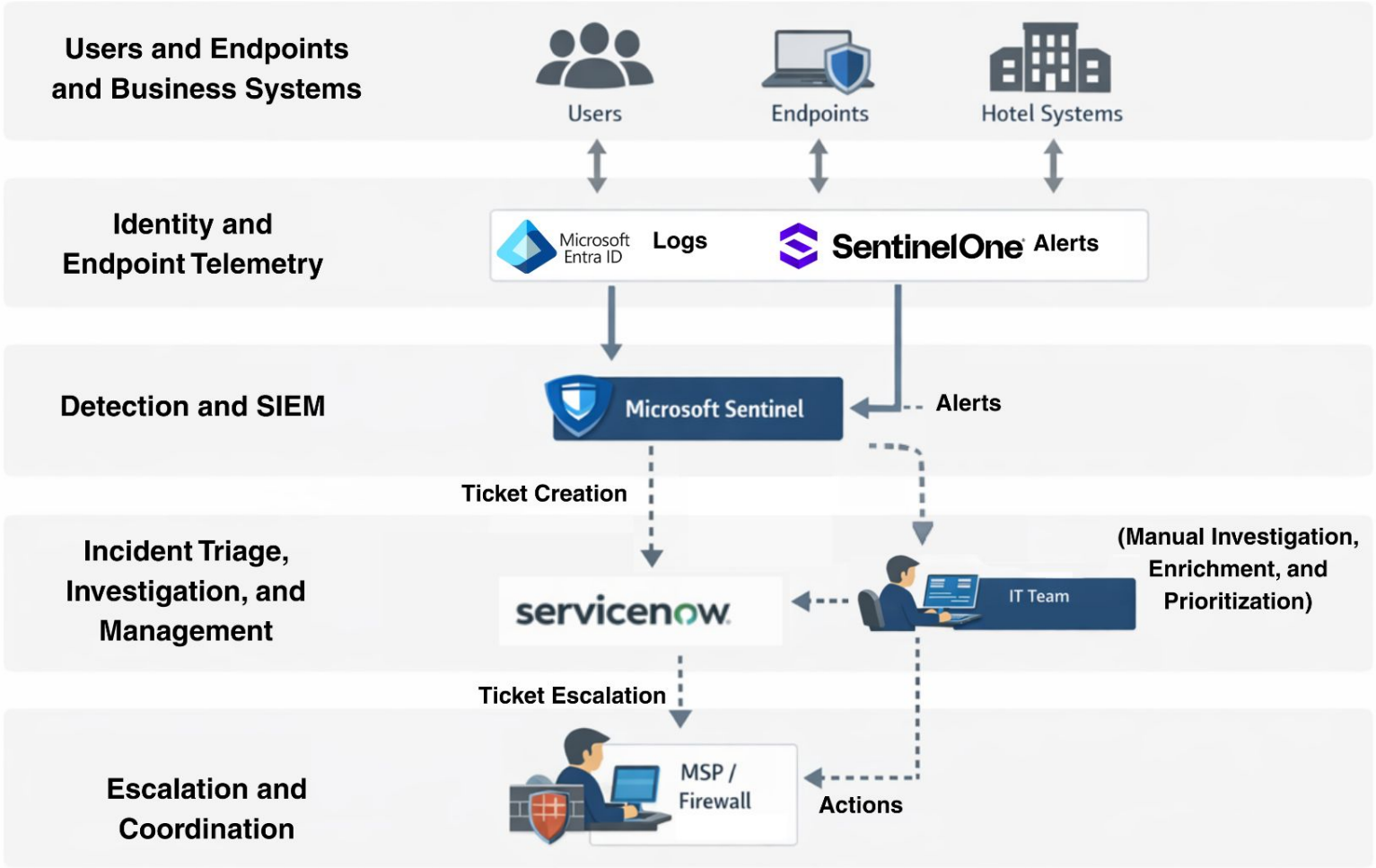
- Analysts perform manual enrichment across tools
- Incident response actions coordinated with MSP when needed
- Containment and remediation executed case-by-case

5

Documentation & Closure

- Incident details documented after resolution
- Remediation tracked to completion
- Limited feedback loop into detection and prioritization logic

Current State Data Flow



Security Gaps and Operational Challenges

Highlighting the key operational and security challenges that limit effective threat detection, prioritization, and response across Harbor Point Hospitality Group's environment.

01

Limited Context for Alerts and Threats

Security alerts often lack external intelligence and risk context, requiring analysts to manually research indicators before understanding severity or relevance.

02

Reaction, Instead of Proaction

Threat response is primarily reactive, with limited ability to identify and prioritize high-risk activity before it escalates into incidents.

03

Inconsistent Threat Intel

Threat intelligence is applied inconsistently across tools and workflows, resulting in uneven detection quality and fragmented analyst decision-making.

04

Manual Triage and Prioritization

IOC validation and alert prioritization rely heavily on manual review, increasing response time and creating variability in how threats are escalated.

Filling in the Gaps

	Current Challenge		Solution
01	Limited Context for Alerts and Threats	→	Use Recorded Future to automatically enrich alerts with risk scores and threat context, giving analysts immediate insight into why an indicator is important.
02	Reaction, Instead of Proaction	→	Apply Recorded Future risk scoring and intelligence feeds to proactively identify and block high-risk indicators before they escalate into incidents.
03	Inconsistent Threat Intelligence	→	Standardize Recorded Future as a centralized intelligence source to ensure consistent scoring, context, and prioritization across teams.
04	Manual Triage and Prioritization	→	Automate IOC enrichment and prioritization, by using predefined risk thresholds to reduce manual triage effort.

Proposed Future State Security Architecture

01

Intelligence Driven Investigations

Alerts are automatically enriched via the Recorded Future API with risk scores, criticality, and intelligence summaries, enabling analysts to immediately assess relevance without manual lookups.

02

Earlier Disruption of High-Confidence Threats

Recorded Future risk scoring and indicator context are applied at ingestion time through API-based enrichment, allowing high-risk domains, IPs, and hashes to be identified and blocked earlier in the detection lifecycle.

03

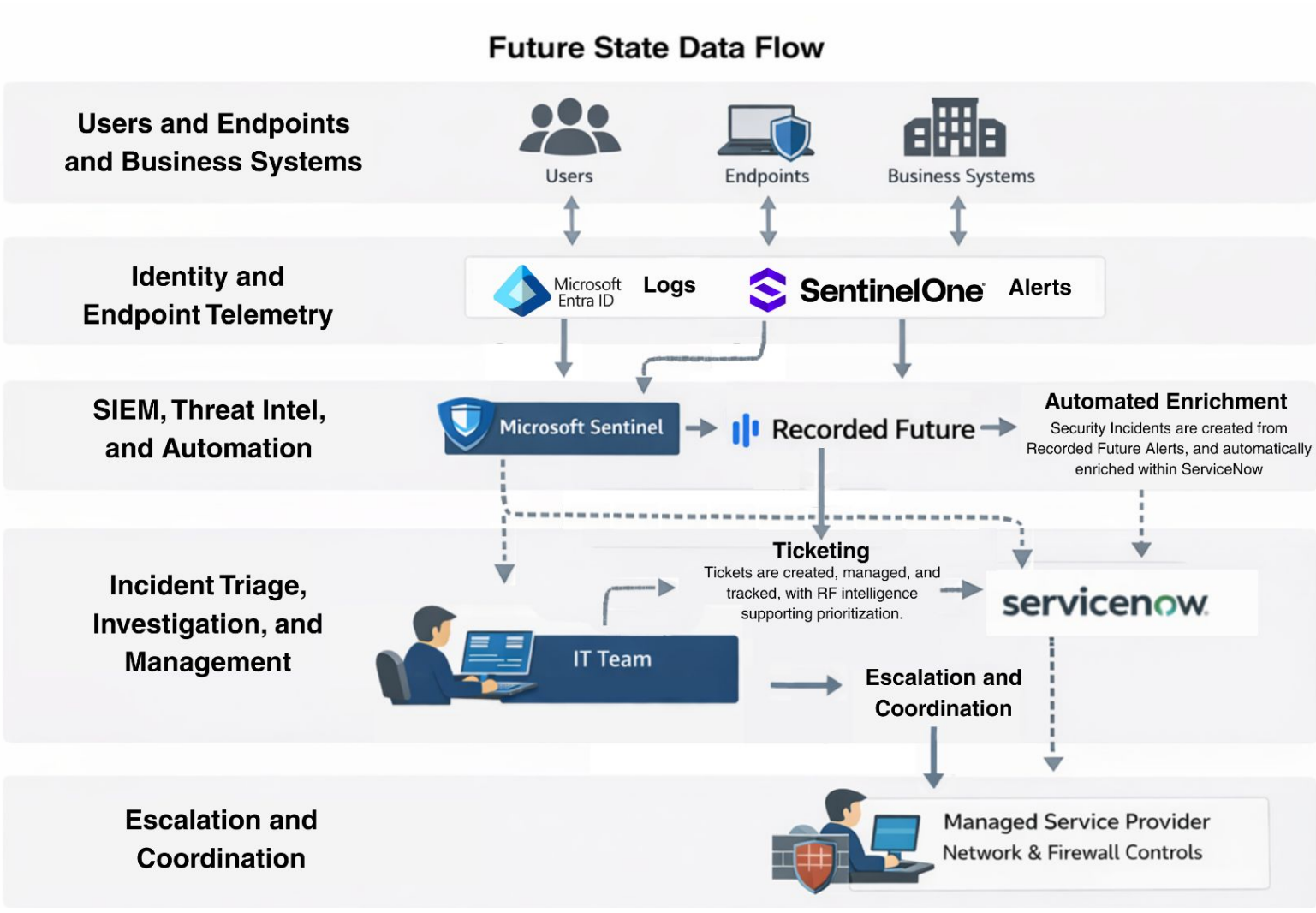
Targeted Automation to Improve Consistency

Tines leverages Recorded Future API responses to standardize enrichment, scoring, and escalation logic, ensuring consistent prioritization decisions across indicators regardless of alert source.

04

Continued Alignment of Current Tools and Roles

Existing security tools remain unchanged, with Recorded Future intelligence consumed via API integrations that enhance decision-making without altering team ownership or operational responsibilities.


Future State Data Flow
Users and Endpoints and Business Systems
Users
Endpoints
Business Systems
Identity and Endpoint Telemetry
Microsoft Entra ID
Logs
SentinelOne
Alerts
SIEM, Threat Intel, and Automation
Microsoft Sentinel
Recorded Future
Automated Enrichment
Security Incidents are created from Recorded Future Alerts, and automatically enriched within ServiceNow
Incident Triage, Investigation, and Management
Ticketing
Tickets are created, managed, and tracked, with RF intelligence supporting prioritization.
servicenow
IT Team
Escalation and Coordination
Escalation and Coordination
Managed Service Provider
Network & Firewall Controls

Integration Recommendations

	Recommendation		Impact
01	SentinelOne and Recorded Future	→	**Advanced Threat Prevention, through XDR** - Proactively prevent known malicious activity before it impacts endpoints or hotel operations
02	ServiceNow and Recorded Future	→	**Threat Intelligence, for Enrichment and Automation** - Ensuring that external intelligence is available within the system where incidents are already tracked, investigated, and resolved.
03	Microsoft Entra ID and Recorded Future	→	**Identity Intelligence by Recorded Future** - Detecting and responding to compromised credentials before they are abused.

Advanced Threat Prevention

SentinelOne

Advanced EDR, that when integrated with Recorded Future, can proactively prevent malicious activity.

Blocking Malicious IOC's such as:

- IP Addresses
- File Hashes
- Domains

Purpose:

Leverage Recorded Future's risk-scored threat intelligence to proactively enforce blocking decisions within SentinelOne, preventing known malicious indicators from reaching endpoints.

Operational Impact:

- High-risk IPs, domains, and file hashes are blocked earlier in the attack lifecycle
- Reduces downstream alerts and investigation volume
- Shifts endpoint security from reactive detection to proactive prevention

Key Benefits:

- Faster disruption of known threats before execution
- Consistent, intelligence-driven blocking decisions
- Improved endpoint protection without increasing analyst workloads

Threat Intelligence Integrations

ServiceNow

Primary ticketing system, enhanced with Recorded Future intelligence to automate enrichment, prioritization, and response workflows.

Integration Capabilities:

- Incident/Alert Enrichment
- Vulnerability Risk Scoring
- External Attack Surface Visibility

Purpose:

Infuse real-time Recorded Future threat intelligence directly into ServiceNow workflows to prioritize risk, accelerate response, and reduce manual investigation effort across security operations.

Operational Impact:

- Incidents and alerts enriched automatically with risk scores and contextual evidence
- Vulnerabilities prioritized based on real-world exploitability
- High-risk assets and issues automatically tracked through ServiceNow workflows

Key Benefits:

- Faster, more confident incident response decisions
- Consistent risk-based prioritization across teams
- Improved visibility into external threats and third-party risk without workflow disruption

Identity Intelligence Integration

Microsoft Entra ID

Platform for identity and access management, and sign-in monitoring, enhanced with Recorded Future intelligence to detect and respond to identity-based threats earlier.

Integration Capabilities:

- Identity risk enrichment
- Suspicious sign-in context
- Compromised credential detection

Purpose:

Enhance identity security by incorporating Recorded Future's intelligence into Entra ID workflows to detect compromised credentials and suspicious identity activity before access is abused.

Operational Impact:

- Identity events enriched with external risk context and exposure data
- High-risk users and credentials identified earlier in the attack chain
- Identity alerts prioritized based on real-world threat intelligence

Key Benefits:

- Earlier detection of credential-based attacks
- Reduced reliance on reactive identity investigations
- Improved access control decisions without increasing analyst workload

Use Cases

	Deliverable	Goal
01	Tines IOC Enrichment and ServiceNow Ticketing Automation	Reducing manual analyst effort during investigations by automatically enriching submitted IOCs with Recorded Future intelligence and creating ServiceNow security incidents only when risk thresholds are met, ensuring consistency and risk-based escalation.
02	Microsoft Sentinel and Recorded Future	Enhancing alert confidence and prioritization by correlating internal Sentinel detections with Recorded Future risk scoring and threat context, helping analysts focus investigations on high-impact security events without changing existing SIEM workflows.

IOC Enrichment + ServiceNow Ticket Creation

This use case addresses how analysts currently validate indicators of compromise through manual lookups and inconsistent escalation decisions. By using Tines to orchestrate Recorded Future enrichment and apply risk-based decision logic, the workflow ensures indicators are consistently enriched, scored, and either escalated to ServiceNow or surfaced to analysts based on defined thresholds without additional manual effort.

Operational Challenge Addressed

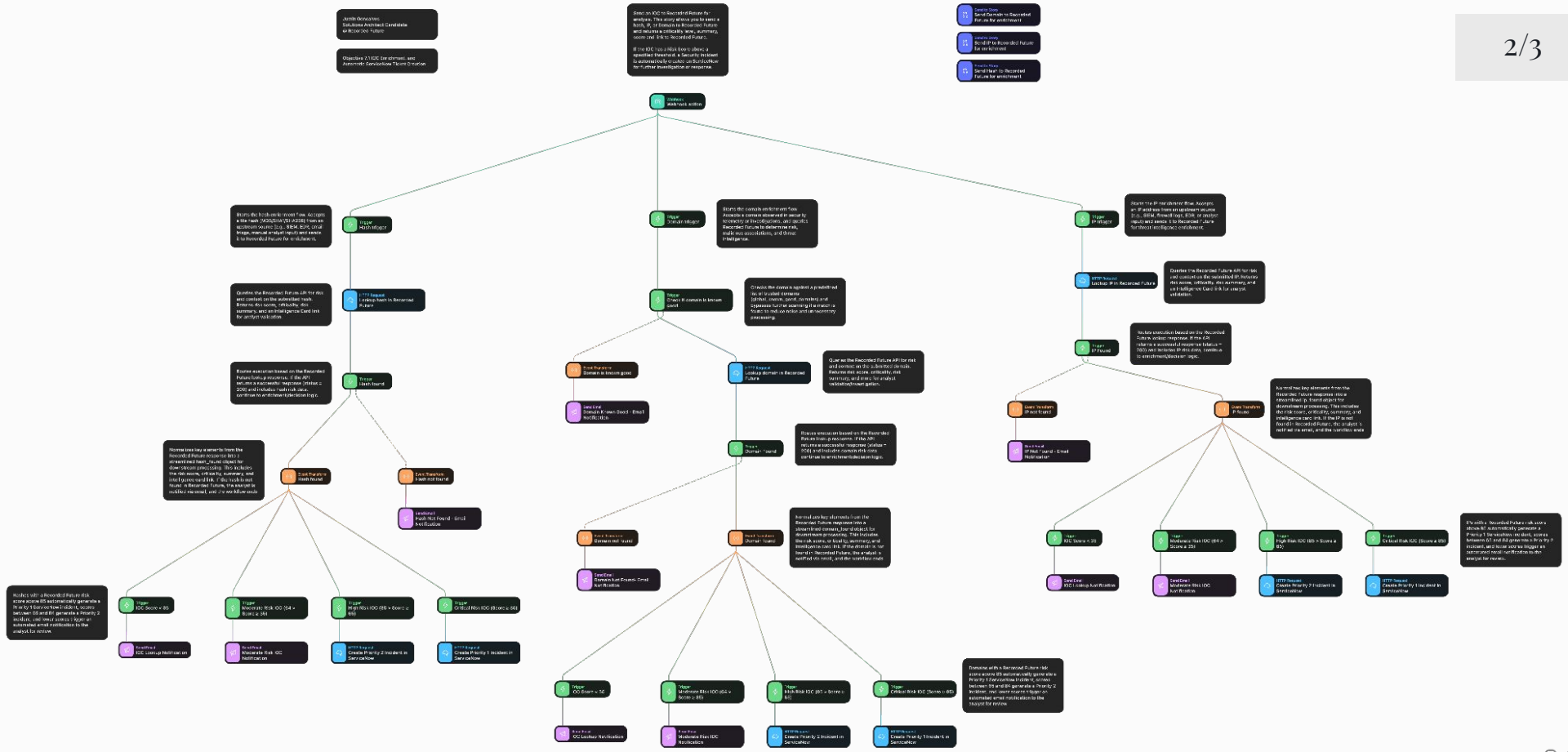
- Manual IOC enrichment and validation across multiple tools
- Inconsistent escalation and prioritization decisions during the investigation process
- High alert volume, and excessive low-risk incidents created without external context

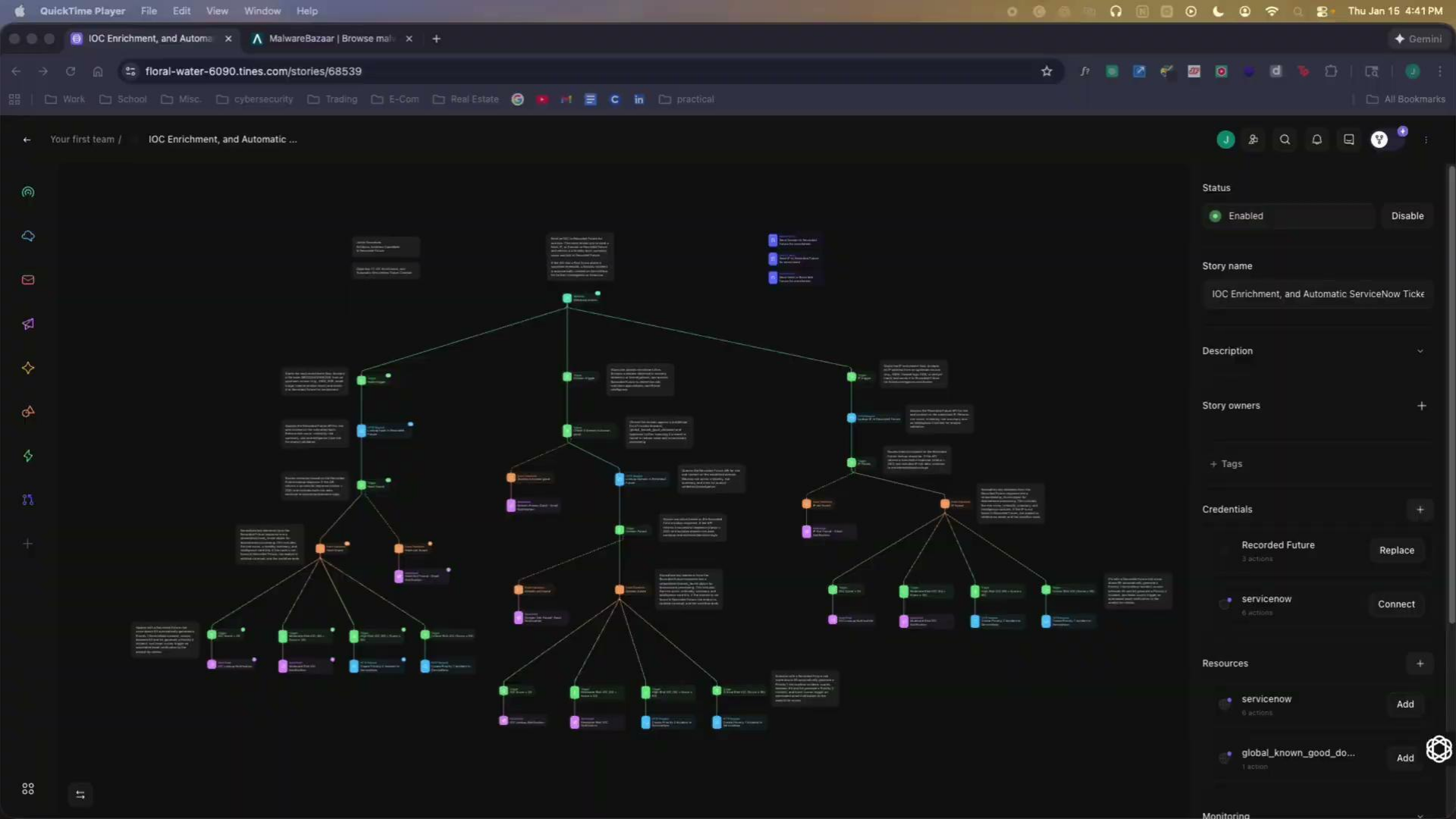
Impact to Existing Processes

- Analysts submit hashes, IPs, or domains into a single automated workflow
- Recorded Future intelligence is retrieved via API and normalized automatically
- ServiceNow tickets are created only when risk thresholds are met, and email notifications are used for low to moderate risk indicators

Measurable Outcome, and Key Benefits

- Faster analyst triage with immediate threat context
- Reduced investigation effort for low-risk indicators, while preserving analyst visibility for moderate-risk findings
- Consistent, risk-based incident creation in ServiceNow




QuickTime Player File Edit View Window Help
Thu Jan 15 4:41 PM
IOC Enrichment, and Automa
MalwareBazaar | Browse mal
Gemini
floral-water-6090.tines.com/stories/68539
Work School Misc. cybersecurity Trading E-Com Real Estate practical
All Bookmarks
Your first team /
IOC Enrichment, and Automatic ...
Status
Enabled
Disable
Story name
IOC Enrichment, and Automatic ServiceNow Ticke
Description
Story owners
Tags
Credentials
Recorded Future
3 actions
Replace
servicenow
6 actions
Connect
Resources
servicenow
6 actions
Add
global_known_good_do...
1 action
Add
Monitoring

Microsoft Sentinel + Recorded Future API

This use case enhances Microsoft Sentinel by embedding Recorded Future threat intelligence directly into SIEM detections. By correlating external risk-scored intelligence with internal telemetry, Sentinel alerts are prioritized based on real-world threat activity rather than raw log signals alone, enabling faster and more accurate analyst decisions.

Operational Challenge Addressed

- SIEM alerts generated with limited external threat context
- Manual analyst validation of suspicious IPs and domains
- Difficulty prioritizing alerts tied to active threat infrastructure

Impact to Existing Processes

- Recorded Future intelligence ingested into Sentinel as TI indicators
- Sentinel analytics correlate TI with endpoint, network, and identity logs
- Alerts arrive pre-enriched with risk scores and supporting evidence

Measurable Outcome, and Key Benefits

- Reduced alert fatigue through intelligence-based prioritization
- Faster analyst triage inside the Sentinel console
- More accurate detection of high-confidence malicious activity

Microsoft Sentinel + Recorded Future API (cont)

Use Case Overview

This use case focuses on enhancing detection and alert prioritization within Microsoft Sentinel by embedding Recorded Future intelligence directly into the SIEM. By ingesting risk-scored threat intelligence as native Sentinel indicators, security teams gain external context that helps distinguish high-confidence threats from background noise.

Rather than relying only on raw telemetry or static rules, Sentinel detections are evaluated using Recorded Future risk scores, evidence, and confidence, enabling more accurate and intelligence-led security operations.

Workflow Summary

In this workflow, Recorded Future intelligence is integrated into Microsoft Sentinel using the official Recorded Future custom connector and Azure Logic Apps. RiskLists and Security Control Feeds are periodically pulled via API and ingested into Sentinel as native Threat Intelligence indicators, following Microsoft's TI schema.

Once ingested, Sentinel correlates these intelligence-backed indicators with internal telemetry such as firewall logs, endpoint activity, and network traffic. This allows Sentinel to generate alerts and incidents that are already enriched with Recorded Future risk scores, evidence, and confidence, enabling analysts to prioritize and investigate threats directly within the SIEM without manual enrichment or tool switching.

API Usage Summaries (Both Use Cases)

Use Case #1 (Tines)

On-demand Recorded Future API lookups are initiated via webhook-triggered workflows. Each IOC submission results in a single enrichment request to the appropriate Recorded Future endpoint (hash, domain, or IP). No bulk polling, scheduled ingestion, or continuous synchronization is performed.

Estimated Daily Usage

- ~100–200 API calls per day
- Scales linearly with alert and analyst activity
- Reduced through early exits and risk thresholds

Use Case #2 (Microsoft Sentinel)

This use case primarily relies on scheduled bulk API interactions rather than per-alert enrichment. Recorded Future RiskLists and Security Control Feeds are retrieved at defined intervals (e.g., hourly for detection-focused lists and daily for prevention-focused feeds) using the Recorded Future API through Azure Logic Apps.

Estimated Daily Usage

- ~50–100 API calls per day
- Predictable and stable due to bulk ingestion

Closing Remarks

- Demonstrated how Recorded Future intelligence can be operationalized across existing security workflows
- Showed how automation reduces manual effort while improving investigation consistency
- Highlighted risk-based escalation to focus response on high-impact threats
  Leveraged existing platforms to avoid adding tools or operational complexity
- Delivered practical, scalable use cases with measurable security outcomes
- Positioned threat intelligence as a decision-support layer, not just an enrichment source