SAFEHILL

safehill.com

SECUREIQ CASE STUDIES

OVERVIEW

Risk doesn't live in individual findings - it lives in the connections between them.

Most breaches today don't happen because defenders lack tools. They happen because defenders can't see how small, everyday exposures connect into real attack paths.

Across healthcare, finance, SaaS, manufacturing, and consumer brands, we see the same pattern repeat: an external exposure, an implicit trust relationship, and an unseen path into critical systems.

SecureIQ exists to surface those paths before attackers exploit them. We continuously discover external and internal exposures, validate which ones are actually reachable, and show defenders exactly which fixes remove attacker options.

Instead of reacting after compromise, teams use SecureIQ to make informed remediation decisions ahead of time - breaking attack chains before they turn into incidents.

CASE STUDY #1

REGIONAL HEALTHCARE PROVIDER

(Leaked Credentials → Forgotten Access → Internal Network Compromise)

Threat actors identified valid employee credentials circulating in dark web infostealer logs. During reconnaissance, they discovered an overlooked external login service originally deployed for legacy access. Using the exposed credentials, attackers authenticated successfully without exploiting a vulnerability.

Once inside, attackers followed trusted internal network paths that led directly to sensitive healthcare systems supporting patient services. The exposure chain relied on valid identity and existing trust relationships, so the organization had no clear pre-breach view of how a single credential exposure translated into internal reach.

By the time leadership understood the access path, attackers had already reached critical systems. Remediation began under pressure rather than as a planned risk reduction activity.

Key Highlights

SecureIQ Capabilities:

- Exposed credential detection correlated to enterprise identities
- External attack surface discovery of forgotten login services
- Identity-aware attack path modeling from internet to internal systems
- Prioritized remediation guidance based on reachable critical assets

MITRE ATT&CK:

T1078 → T1133 → T1021

Compliance Context:

HIPAA, HITECH, FDA Cybersecurity Guidance, NIST CSF

CASE STUDY #2

FINANCIAL SERVICES FIRM

(Stored Credentials in AD → Privilege Escalation → Domain Compromise)

Threat actors gained initial access to the internal network through exposed or improperly stored credentials within Active Directory. Several systems contained embedded credentials in autologon configurations and user account description fields. With this level of access, attackers were able to move laterally between systems and harvest additional credentials from memory and local security databases.

Through credential dumping and privilege chaining, attackers ultimately obtained access to a domain administrator account, resulting in full domain compromise. What began as poor credential hygiene escalated into enterprise-wide control due to unmonitored privilege relationships and inherited access paths within Active Directory.

The organization lacked visibility into how stored credentials and delegated administrative rights combined to create escalation pathways. Remediation required urgent containment, credential rotation, and broad privilege restructuring rather than a structured, risk-prioritized hardening effort.

When the access path was finally recognized, remediation required emergency changes to access controls and segmentation rather than a controlled, prioritized hardening effort.

Key Highlights

SecureIQ Capabilities:

- Continuous auditing of Active Directory for stored credentials and insecure account attributes
- Mapping of trust relationships across internal infrastructure
- Attack path analysis mapping lateral movement and privilege escalation routes
- Risk-based prioritization of remediation efforts to prevent domain compromise.

MITRE ATT&CK:

T1078 → T1133 → T1068

Compliance Context:

PCI-DSS, SOX, GLBA, NIST CSF, ISO 27001

CASE STUDY #3

MANUFACTURING & CRITICAL INFRASTRUCTURE OPERATOR

(Credential Exposure → Hidden Trust Relationships → Operational Impact)

Threat actors identified valid engineering credentials and discovered an exposed management interface tied to operational systems. Authentication succeeded because the access pattern looked legitimate and relied on existing trust assumptions.

Once inside, attackers leveraged trust between engineering and corporate environments to expand access and approach operationally sensitive systems. The organization did not have a clear, continuously updated map of trust-driven attack paths across environments.

The result was a rapid escalation from low-privilege access to high-consequence operational risk, forcing remediation under business continuity pressure.

Key Highlights

SecureIQ Capabilities:

- External asset discovery of exposed management interfaces
- Internal trust relationship mapping across IT/OT
- Privilege escalation path analysis
- Segmentation risk identification

MITRE ATT&CK:

T1078 → T1087 → T1021

Compliance Context:

NIST CSF, IEC 62443, ISO 27001

CASE STUDY #4

SAAS TECHNOLOGY COMPANY

(Outdated Software → Known Vulnerability → Internal Access)

Threat actors scanning the internet identified an externally exposed application running outdated software with a well-documented vulnerability. The system remained unpatched due to ownership ambiguity and incomplete visibility into legacy assets.

Attackers exploited the vulnerability to gain initial access without needing credentials. That compromised system had connectivity to internal services that were never intended to be internet-adjacent, creating a direct bridge into the internal environment.

The organization's problem wasn't a lack of patching policy - it was not knowing this system existed, how exposed it was, and what internal paths it enabled.

Key Highlights

SecureIQ Capabilities:

- Continuous external asset discovery and ownership attribution
- Detection of outdated and vulnerable software
- AI + human exploitability validation
- Attack path modeling from vulnerable asset to internal systems

MITRE ATT&CK:

T1190 → T1021

Compliance Context:

SOC 2, ISO 27001, GDPR

CASE STUDY #5

CONSUMER BRAND WITH GLOBAL WEB PRESENCE

(Hijacked Subdomain → Brand Trust Abuse → Internal Exposure)

Threat actors identified an abandoned subdomain still delegated via DNS but no longer controlled by the organization. They hijacked the subdomain by reclaiming the underlying cloud resource, then hosted malicious content under a trusted brand domain.

Because the subdomain looked legitimate to users, it was used for high-conversion phishing and credential harvesting. Some harvested credentials were later reused to attempt access into internal services where password reuse and permissive access paths existed.

The organization's challenge wasn't "phishing awareness" - it was dormant internet-facing brand infrastructure that silently became attacker-controlled.

Key Highlights

SecureIQ Capabilities:

- Continuous subdomain and DNS enumeration
- Detection of dangling or hijackable subdomains
- Brand-linked attack surface monitoring
- Correlation of external abuse to internal access paths

MITRE ATT&CK:

T1583 → T1566 → T1078

Compliance Context:

GDPR, CCPA/CPRA, SOC 2

CASE STUDY #6

ENTERPRISE SERVICES ORGANIZATION

(Shadow IT → Misconfiguration → Internal Reachability)

Threat actors discovered an internet-exposed cloud service spun up by a business unit outside formal IT processes. The service was misconfigured, allowing unauthenticated access to internal APIs and sensitive functionality.

Because the asset was unknown to security teams, it remained ungoverned and unremediated. Attackers used it to enumerate internal resources and move laterally toward higher-value systems.

The breach path was enabled by a common reality: modern environments change faster than centralized inventory and governance can keep up.

Key Highlights

SecureIQ Capabilities:

- Discovery of unknown and shadow IT assets
- Misconfiguration detection across cloud and on-prem
- Internal reachability analysis
- Human-validated penetration testing

MITRE ATT&CK:

T1190 → T1087 → T1021

Compliance Context:

SOC 2, ISO 27001, NIST CSF

CASE STUDY #7

TRAVEL & HOSPITALITY

(Legacy System Exposure → Third-Party Trust → Operational Risk)

Threat actors identified an externally exposed legacy system supporting booking-related integrations and vendor connectivity. The system ran outdated components and relied on implicit trust with internal operational networks to function smoothly.

Attackers exploited the exposed service to gain a foothold and then leveraged trusted network relationships to reach internal systems supporting customer data workflows and voyage operations. The organization lacked a clear view of how third-party-connected systems created internal reachability.

The result was an avoidable escalation path: a single exposed legacy endpoint enabling access into higher-impact internal operations.

Key Highlights

SecureIQ Capabilities:

- External attack surface discovery of legacy and third-party systems
- Detection of outdated and vulnerable software
- Trust relationship and internal reachability mapping
- Prioritized remediation of high-impact operational paths

MITRE ATT&CK:

T1190 → T1021

Compliance Context:

PCI-DSS, GDPR, NIST CSF, ISO 27001

CASE STUDY #8

MARKETPLACE/ GIG ECONOMY

(API Exposure → Authorization Weakness → Data Access)

Threat actors identified exposed API endpoints supporting marketplace workflows. An authorization weakness allowed access beyond intended user scope, enabling enumeration of user profiles and transaction-related data.

Because the endpoints were legitimate and business-critical, they remained online while the organization lacked confidence about true exploitability and impact. Attackers used the weakness to expand the accessible dataset and probe related services.

The organization's real gap wasn't "having APIs" - it was not having continuous validation of which exposed endpoints could be abused and what they could reach.

Key Highlights

SecureIQ Capabilities:

- External API discovery and exposure analysis
- Misconfiguration and authorization weakness identification
- AI + human validation of exploitability and impact
- Attack path modeling from exposed APIs to sensitive systems

MITRE ATT&CK:

T1190 → T1087

Compliance Context:

GDPR, SOC 2, ISO 27001, PCI-DSS

CASE STUDY #9

ENTERTAINMENT & LIVE EVENTS

(Subdomain Takeover → Brand Abuse → Credential Harvesting)

Threat actors found an abandoned promotional subdomain still delegated via DNS to a decommissioned cloud resource. They reclaimed the underlying resource and took control of the subdomain.

With a trusted brand domain in hand, attackers hosted phishing pages that targeted fans, artists, and internal partners. The campaign harvested credentials and created follow-on attempts against internal services where account reuse and permissive access patterns existed.

The organization's exposure wasn't only phishing - it was dormant brand infrastructure that created an attacker-controlled trust anchor.

Key Highlights

SecureIQ Capabilities:

- Continuous subdomain and DNS enumeration
- Detection of dangling or hijackable subdomains
- Brand-linked attack surface monitoring and prioritization
- Correlation of brand abuse risk to internal access exposure

MITRE ATT&CK:

T1583 → T1566 → T1078

Compliance Context:

GDPR, CCPA/CPRA, SOC 2

CASE STUDY #10

CPG, FOOD & BEVERAGE

(IT/OT Trust → Lateral Movement → Operational Disruption)

Threat actors gained a foothold in a corporate IT-facing system that was internet-reachable and connected through trusted pathways to manufacturing and logistics environments. The trust existed for operational efficiency but created unintended lateral movement potential.

Attackers leveraged internal connectivity and trust to move closer to systems supporting production scheduling, distribution workflows, and operational continuity. The organization lacked a continuously updated picture of which corporate-to-operations trust paths were most dangerous.

The operational risk wasn't purely "OT security" — it was the hidden bridge between IT and operations that attackers could traverse.

Key Highlights

SecureIQ Capabilities:

- External asset discovery across IT and OT-adjacent systems
- Trust relationship mapping between corporate and operational networks
- Cross-environment attack path analysis and prioritization
- Remediation guidance focused on breaking high-impact bridges

MITRE ATT&CK:

T1021 → T1046

Compliance Context:

FDA FSMA, NIST CSF, ISO 27001

CASE STUDY #11

LIFE SCIENCES & BIOPHARMA

(Research Platform Exposure → IP Risk)

Threat actors identified an externally exposed research collaboration platform used for R&D workflows and partner coordination. Access controls were permissive enough that attackers could probe for sensitive data access opportunities.

Even without deploying malware, attackers could leverage valid access patterns and weak segmentation to approach datasets and documents tied to intellectual property and regulated research records. The organization lacked an always-current understanding of which external research platforms created direct paths to high-value IP.

The risk wasn't "having collaboration tools" - it was not continuously proving what those tools exposed, and how quickly exposure translated into IP impact.

Key Highlights

SecureIQ Capabilities:

- External asset discovery of research and collaboration platforms
- Identity and access path modeling to sensitive R&D data
- Risk prioritization based on IP impact and reachability
- Validation workflows (AI + human) to confirm exploit paths

MITRE ATT&CK:

T1078 → T1083

Compliance Context:

FDA 21 CFR Part 11, HIPAA (adjacent), ISO 27001, NIST 800-53

CASE STUDY #12

HIGHER EDUCATION

(Shadow IT → Misconfiguration → Student Data Exposure)

Threat actors discovered a cloud service deployed by a department outside central IT governance. The service was internet-exposed and misconfigured, enabling access to data and functions beyond intended users.

Attackers used the exposure to enumerate accounts and locate systems tied to student and staff records. The institution lacked a unified, continuously updated view of shadow IT assets and what internal services those assets could reach.

The failure pattern was common in higher education: decentralized technology decisions creating hidden exposure and compliance risk.

Key Highlights

SecureIQ Capabilities:

- Discovery of shadow IT assets across departments
- Cloud misconfiguration detection and prioritization
- Internal reachability analysis to protected student/staff systems
- Human validation to confirm real-world exploitability

MITRE ATT&CK:

T1190 → T1087

Compliance Context:

FERPA, GLBA, NIST 800-171

CASE STUDY #13

HEALTHCARE SERVICES

(Credential Exposure → Internal Clinical Systems)

Threat actors obtained valid employee credentials and discovered an externally accessible clinical support system used for operational workflows. Authentication succeeded using valid identity, creating an access foothold that looked normal.

Attackers then followed internal network paths toward systems supporting patient services and administrative operations. The organization did not have a clear map of reachable internal assets from that external entry point, delaying prioritization of access revocation and pathway remediation.

The result was a predictable escalation: credential exposure plus external access plus internal trust equals avoidable clinical system risk.

Key Highlights

SecureIQ Capabilities:

- Exposed credential correlation to clinical access systems
- External asset discovery and monitoring of clinical-facing services
- Internal attack path modeling to patient-service systems
- Prioritized remediation guidance to break high-risk pathways

MITRE ATT&CK:

T1078 → T1021

Compliance Context:

HIPAA, HITECH, NIST CSF, FDA Cybersecurity Guidance

CASE STUDY #14

PROFESSIONAL SERVICES: ARCHITECTURE / ENGINEERING / CONSTRUCTION

(VPN Exposure → Project Data Access)

Threat actors identified an externally exposed VPN gateway that provided broad access into internal resources. Using valid credentials obtained through exposure or reuse, attackers established an authenticated session.

Once connected, attackers moved toward project collaboration systems containing sensitive design files, client data, and bid-related documents. The organization lacked a continuously updated view of which access points produced the highest internal blast radius.

The problem wasn't "having remote work" - it was remote access posture plus internal reachability to sensitive project data.

Key Highlights

SecureIQ Capabilities:

- External access point discovery (VPN, remote gateways)
- Configuration and exposure risk analysis
- Internal reachability mapping to collaboration and file systems
- Prioritized remediation focused on reducing blast radius

MITRE ATT&CK:

T1133 → T1078

Compliance Context:

SOC 2, ISO 27001, NIST CSF

CASE STUDY #15

AI / TECHNOLOGY

(Cloud Misconfiguration → Model & Data Exposure)

Threat actors identified a misconfigured cloud storage and inference environment supporting AI workloads. The misconfiguration exposed data and services that were intended to be private, including datasets and internal APIs.

Attackers used the exposure to access training data and probe model-related assets, increasing the risk of IP loss and downstream abuse. The organization lacked continuous validation of which cloud assets were exposed and what sensitive resources were reachable from them.

The risk wasn't just "cloud misconfigurations" - it was misconfigurations that directly exposed the company's differentiating AI assets.

Key Highlights

SecureIQ Capabilities:

- Cloud asset and storage discovery
- Misconfiguration detection across AI-related infrastructure
- Attack path analysis to models, datasets, and internal APIs
- Validation workflows (AI + human) to confirm exposure and impact

MITRE ATT&CK:

T1530 → T1083

Compliance Context:

SOC 2, ISO 27001, GDPR, emerging AI governance frameworks