How Dow cut its Sentinel bill by dropping firewall noise before ingest

Dow's cyber team used to pay to ingest firewall data just to find out what was in it. Now it decides what reaches Sentinel first, and the same pipeline feeds Dow's own AI agents.

Key challenge

Dow managed Sentinel costs with 1,000+ manually built KQL rules that couldn't scale across the enterprise.

Key result

Realm replaced all 1,000+ KQL rules in 72 hours and delivered a 3x return.

The company

Global materials science

Scope: IT and OT

Scale: A large, global technology footprint

SIEM: Microsoft Sentinel

Destinations: Sentinel, enterprise data platform

Everything went into Sentinel, and the team couldn't see what it was paying for.

Joe Lykowski, Cyber Defense Leader at Dow, runs a cyber operations team that covers the whole company, from enterprise and cloud down to the systems that run its plants, and all of that data flows into a large, global security environment.

For years the team paid to ingest that data, then dropped much of it afterward through more than 1,000 KQL and data collection rules that Matthew Madigan, who focuses on SIEM engineering, had built by hand. It worked, but it was hard to sustain and couldn't tell anyone what they were ingesting, dropping, or paying for. Joe's goal for this year was to simplify it.

Firewall logs, from several vendors across cloud, on-premises, and plant networks, were the hardest part. Plant operations teams rely on the same logs, and no one could say what was safe to drop without losing something operations needed.

> **"I can't dictate what a 30-year-old firewall payload structure looks like. I can't even see it until I pay for it."**
>
> **Matthew Madigan**, Cybersecurity Manager focused in SIEM Engineering, Dow

Outcomes

3x
return on every $1 Dow spends on Realm

>50%
less Palo Alto firewall volume into Sentinel, on top of the team's own cuts

1,000+
hand-built KQL and data collection rules replaced in **72 hours**

7 days
to deploy, with some sources live sooner

Why Dow took a chance on a startup

Dow had talked with a leading pipeline vendor for a year or two. "Every time we tried to approach their product, we just went, 'Oh, this is going to be a big project,'" Joe says. A trusted former partner pointed them to Realm, which mattered, because "typically we wouldn't give a startup really the time of day." Dow tested Realm against other pipelines and chose it for how much it reduced and how little it took to run. Matt started with the firewalls and found Realm no harder to stand up than a Syslog server with an agent.

Seeing the data before Sentinel bills for it

Realm sits between Dow's sources and Sentinel. It parses each firewall's logs and normalizes them to one schema, so Matt sees what every source contains before any of it is ingested. Realm's Clarity AI recommends what to cut and shows each change's effect on volume before it goes live, which gave Matt confidence he wasn't cutting anything detection engineering needed.

Realm identified additional unnecessary telemetry that had previously gone unnoticed.

Within 72 hours, Realm had replaced the 1,000+ rules. Palo Alto volume into Sentinel fell by more than half on top of the team's own cuts, and Joe sees room to optimize further.

Realm also watches every input and output feed, which made the manual checks the team had built in Sentinel to catch a silent log source unnecessary.

> **Our people that pay the Sentinel bill, they're singing our praise. Our bill has significantly dropped, and it's real.**
>
> **Joe Lykowski**
> Cyber Defense Leader, Dow

A second job for the same pipeline

Dow was also working out how to put the right security data in front of AI. It wanted its own agents working on Palo Alto firewall data in Dow's enterprise data platform, and raw vendor logs would have needed a normalization project first. Realm skips that step. It sends each event as one structured record with the raw log included, so Dow's agents work on it directly and can check any answer against the original event. Dow brought the platform and the model. Realm brought data they could use.

By the numbers

Measure	Before Realm	With Realm	Result
Reduction logic	1,000+ KQL and data collection rules, kept up by hand	Decided before ingest, in one place	**Replaced in 72 hours**
Palo Alto firewall logs	Already trimmed, contents unseen until billed	Every event type visible before a change goes live	**>50% further cut**
Firewall data in Dow's enterprise data platform	Raw vendor logs, normalization needed first	One structured record per event, raw log included	**Agents work on it directly**

See what's in your data before your SIEM bills for it.

Pick one source and start a 7-Day Data Assessment. We'll show you what it contains and how much you can cut, on your own data.

Start an assessment → realm.security

About Realm Security

Realm Security gives security teams independent control over their telemetry before it reaches the SIEM, data lake, or AI agent. The platform understands what each source produces and what each downstream system needs, then guides teams on what to retain, cut, or route. Headquartered in Boston, Realm deploys in about a week and typically cuts SIEM ingestion costs by 50% or more.

REALM. SECURITY

www.realm.security
LinkedIn: /company/realm-security
X: @Realm_Security

© 2026 Realm Security, Inc. All rights reserved. All other brand names, product names, or trademarks belong to their respective owners.