

SIEM Craft™

Security Data. **Engineered.**™

CYBERSECURITY CONSULTING

Get the full value out of your Sumo Logic SIEM

Independent consulting for the Sumo Logic Cloud SIEM and the Log Analytics Platform — cleaner log onboarding, sharper detections, and honest coverage reporting.

WHY SIEM CRAFT

Subject-matter experts, for the people on call

SIEM Craft is an independent consultancy. Our only interest is that you get the full value of your Sumo Logic SIEM investment — with proper visibility and the detections that matter actually in place.

01 **Built around your requirements**

We work from the security requirements specific to your business, not a generic industry baseline.

02 **Your environment, your data**

We work alongside you inside your tenant, with credentials you provide, under NDA. Nothing leaves it that does not need to, and never without your prior approval.

03 **Plain language**

Every engagement ends in reports an engineer can act on and a CISO can read in ten minutes.

04 **Independent**

No vendor ties. We recommend what works best for you, not what a vendor is selling.

05 **Enablement, not dependency**

We document the work and train your team as we go, so your people can run and extend it after we leave.

WHAT WE DO

From raw logs to reliable detections

Most SIEM problems are plumbing problems: logs that never arrive, parsers that quietly stop matching, rules that fire on everything or nothing. We fix the plumbing, then make the detections count.

01

Log source onboarding

Get the right sources into Cloud SIEM, parsed and mapped. Collector and source-category design, custom parsers and mappings for products that have none, dashboards and queries for Log Analytics.

Outcome No gaps in visibility; failed records sharply reduced or eliminated.

02

Log value & data tiering

Send the right logs, and pay for them the right way. Use-case-driven log review, then a tiering plan matched to each source's security value and retention obligations.

Outcome Reduced credit consumption and a documented, compliance-aware retention model.

03

Detection engineering

Rules that fire for the right reasons. A review against MITRE ATT&CK and your real log sources, tuning that silences noise without blinding you, and custom detections built around your use cases.

Outcome Coverage leadership can read, and noise down without new blind spots.

04

SIEM health audit

Know what your SIEM is actually doing. A fixed-scope assessment of what is sending, parsing and firing, and where the gaps are — with an executive summary and a prioritized fix list.

Outcome A clear, prioritized picture a CISO and an engineer can both act on.

05

Training & enablement

Leave your team able to run it without us. Hands-on, role-based sessions in your own environment, with runbooks and documentation your team keeps.

Outcome Your people can run and extend the work after we leave.

HOW WE ENGAGE

Ways to work together

Start with a short project, keep us on a retainer, or embed an engineer with your team. We shape the engagement around how you want to work.

Fixed-scope project

A defined deliverable and timeline — an onboarding, an audit, a detection build — scoped up front and handed off complete.

Monthly retainer

Ongoing detection engineering and SIEM care, so coverage keeps pace as your environment and the threats change.

Staff augmentation

An experienced engineer embedded with your team for a quarter, working as part of your security operation.

Not sure which fits? A short scoping conversation is usually enough to tell — and scoping calls are complimentary.



SIEM Craft™

Security Data. Engineered.™

Tell us what your SIEM is not telling you.

A short conversation is usually enough to know whether we can help. No slide deck, no sales process.

SALES	sales@siemcraft.io
WEB	siemcraft.io

SIEM Craft — an independent consultancy, not affiliated with Sumo Logic, Inc. Security Data. Engineered.