Cribl | SecurityRisk ADVISORS

>CASE STUDY_

Cribl and Security Risk Advisors

Security Risk Advisors (SRA) is a highly specialized consulting firm that continually develops solutions to cybersecurity's emerging problems. SCALR™ XDR is their turn-key CyberSOC solution that provides a combined SIEM, SOAR, and Data Lake — fully integrating with any EDR. SCALR™ combines Cribl Stream with Microsoft Sentinel and Azure Data Explorer to reduce licensing costs and provide threat hunting services, complete with purple team exercises.

HIGHLIGHTS

- SRA's XDR offering is made possible with the help of Cribl Stream
- Reduce Windows Event Logs by 60% and cut SIEM costs by up to 80%
- Transition from one SIEM to another in as little as 90 to 180 days

As part of their new SCALR™ XDR service, SRA designs, configures, and builds out their customers' security architectures. They perform managed security services, 24/7 monitoring, curated out-of-the-box threat detections, and act as a SOC for critical data sources like cloud alerts, EDR, threat detection alerts, and more.

A turn-key solution like this wasn't possible until SRA decided to implement Cribl Stream.

> "We looked at a few open-source alternatives, but none of them had the enterprise level scalability, capabilities, and features that our clients need for something this critical in their data pipeline. Cribl Stream and Cribl's overall portfolio and innovative direction also just continues to get better."
>
> — Michael Polise, Director of Advisory Services

Giving customers full control over their data

SRA’s proprietary XDR solution is deployed and co-managed within the client’s environment, which allows the client to keep complete control over their data at all times. Data sources get routed to Cribl Stream — all data that are used for generating alerts, correlating events, or otherwise actioned on by a SOC analyst gets forwarded to Microsoft Sentinel.

> **“Everything is provisioned in the client’s environment, so they have full access to everything. They can create their own alerts for themselves and funnel data to their teams internally.”**
>
> — Michael Polise, Director of Advisory Services

Reduced windows event logs by 60%

With the help of Cribl Stream, SRA’s latest offering enables customers to easily collect data from the right sources, develop tailored analytics, and efficiently deliver it to its destination. Stream’s reduction capabilities help them to significantly reduce their overall ingest across all types of data.

> **“We get pretty aggressive with Windows Event Log reduction and often get a 60% reduction or more for those data sources without losing any of the context we need for triggering detection content. Reduction of other sources might be less than that, but we can typically cut out the junk to reduce data volumes by half.”**
>
> — Michael Polise, Director of Advisory Services

> **"Our clients no longer have to choose between accepting the risk of limited visibility or asking for more money. They can onboard all of their sources without incurring additional costs."**

Cut SIEM costs up to 80%

Because of that reduction — and the redirection of some sources to a data lake instead of a SIEM — organizations have the freedom to onboard any sources that may have been waiting on the sidelines. Companies that couldn’t afford to store everything in their previous SIEM can now retain all the data they need and only spend a fraction of what they normally would on a similar solution.

> **“In general, we see 70-80% license cost savings in the tech stack compared to a client’s existing SIEM platform. A recent client had a $900K per year Splunk license that was reduced to $200K after using Cribl Stream to migrate to Sentinel and Azure Data Explorer.”**
>
> — Michael Polise, Director of Advisory

Fast, seamless SIEM migrations

The cost and time savings that SRA gives its customers also allow them to migrate from one SIEM to another, in as little as 90 to 180 days.

> **“In our most aggressive migration, a client moving from Splunk to Sentinel went live in two to three weeks. We can’t move everyone over that fast, but as long as the log sources are redirected, we can typically onboard and go live within a 30-60 day window.”**
>
> — Michael Polise, Director of Advisory Services

Michael and his team started with the out-of-the-box **Cribl Packs** to facilitate this process, then created custom Packs to accelerate SIEM migrations even further.

Improved threat detection

SRA's SCALR™ XDR platform greatly improves the quality of life of SOC analysts. Powered by the flexibility and control of Cribl, SRA's clients can quickly onboard any data source and reduce the noise, simplifying alert triage and threat detection.

> **"SOC analysts can read queries, and focus on threat data that is important to them, and query data in Azure Data Explorer if they need additional information. Our clients can also use Sentinel to automatically pull pertinent data to the front of the screen for an analyst."**
>
> — Michael Polise, Director of Advisory Services

Michael and his team have seen the ADX data lake transform from a focal point for data retention into a critical tool for threat hunting. Typical deployments include 90-day retention in the SIEM, but the cost-effective data lake allows for 12 months of storage or longer, providing more historical data available for reference.

> **"SOC analysts within the client's environment can access everything directly from Sentinel and can query Azure Data Explorer natively from Sentinel, which is great for efficiency and reducing the mean time to respond."**

Purple team validations for increased threat detection maturity

Leveraging the Cribl Stream-Sentinel-Azure Data Explorer tech stack provides instant SOC Maturity by seamlessly facilitating SRA's proprietary detection logic based on industry verticals, to detect common and advanced threats. They also provide a purple-teaming service which validates detection and prevention controls, twice a year.

> **"To validate that our client's tools are functioning appropriately, we perform threat simulations based on TTPs that threat actors perform on a regular basis. We bring red teams and blue teams to the table to perform some of those simulations, then work with clients to improve the detection logic in Sentinel and their cloud-based EDR."**
>
> — Michael Polise, Director of Advisory Services

Stream makes it easy to send the right data to analyze the most important TTPs—instead of trying to tackle all of the MITRE ATT&CK Framework. Clients get a SOC with out-of-the-box run books and threat hunt criteria without having to devote resources towards hiring or home-growing the expertise, only to be set back if staff turns over.

SOAR automation comes included through Sentinel, so organizations don't have to worry about buying another six-figure product. SRA also has SOAR playbooks to build out automation for the clients, elevating their maturity even further. Cribl Stream plays a crucial role in this strategy by shaping and normalizing data from key sources, essential to conducting fast, effective analysis and identifying threats.

Using Cribl Search to improve offerings for non-Microsoft clients

To improve future offerings, SRA is exploring Cribl Search and Data Lake to expand services and infrastructure beyond SCALR™ XDR. With Cribl's federated "search-in-place" queries, on data of any format or location, users can conduct precise analysis and forward results effortlessly. Adding platform-agnostic data warehousing, Cribl's Data Lake delivers unified retention, security, and access control policies across object stores and clouds from one easy management platform. Functionality that will be particularly beneficial for clients using Splunk as a SIEM or for those sending logs to S3, extending SRA's reach beyond Microsoft products.

> **"The easy manageability of Cribl makes it possible to deliver quickly for our clients."**

TL;DR

- Combined Cribl Stream, Microsoft Sentinel, and ADX into a turnkey CyberSOC solution
- Reduced Windows event logs by 60% on average
- Cut SIEM costs up to 80%
- Accelerated SIEM migration by 4-8 weeks on average
- Improved threat detection via additional data source onboarding and noise reduction
- Provide first-time data lake and SOAR capabilities for the majority of customers

ABOUT SECURITY RISK ADVISORS

Security Risk Advisors (SRA) is a Cribl Partner who provides specialized security services including Cribl Engineering and Enablement, Penetration Testing, Purple Teams, Cloud Security, Resilience, Cyber Physical Systems Security, Engineering, and 24x7x365 Cybersecurity Operations. SRA's mission is to "Level Up" every day to protect our clients and their customers. SRA delivers security services to Fortune and Global 1000 companies, innovating technology startups, and mission-oriented non-profits across Healthcare, Pharmaceutical, Retail, Financial Services, and Manufacturing industries. SRA is headquartered in Philadelphia, with offices in Rochester, and Kilkenny, Ireland. SRA is an official partner of Cribl (https://sra.io/cribl/).

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry's leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, Cribl Search, the industry's first search-in-place solution, and Cribl Lake, a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter

CS-0022-EN-1-0524