SIREN

Unit 3, GTC
Mervue Business Park
Galway, Ireland

+353 (091) 704 885
info@siren.io

CG CRUMPTON GROUP LLC

Executive Summary

Crumpton Group is a strategic advisory company based in Washington, DC that serves Global Fortune 500 executives and other elite Clients across industries and verticals. Their intelligence-driven consulting services enhance business leaders' ability to make effective, high-stakes decisions on strategy, investments, and operations in complex foreign markets.

The company operates within high volume, highly valuable and sensitive data environment that requires the upmost levels cybersecurity defense. The Crumpton Group required an innovative and cost-efficient solution for threat-hunting related scenarios where the risk profile for the end customer is volatile and difficult to foresee. Since implementing the Siren Platform™, the company has seen benefits including:

- Future proofed solution at the right price point
- Real-time insights across data sources
- Increased spacial awareness for investigators

Why Siren

"[Siren is the] most feature rich solution at the right price point, with inherent future proofing in terms of how the platform scales" – Jeremy Turner, Cybersecurity Program Manager

The Crumpton Group uses the Siren Platform to analyze large pools of data on behalf of their clients which needs to be actionable in real-time. The ground-breaking innovation brought by Siren into the market, that leverages existing well-known open source technologies and adapts them to effectively operate in enterprise grade cybersecurity environments at a competitive price point meant that Siren was the company's choice for their future threat-hunting activities.

Case study highlights

Industry

- Cybersecurity

Use cases

- Threat-hunting
- Zero-day response
- Cybersecurity risk intelligence

Challenges

- Needed to analyse large amounts of data effectively and at a competitive price point
- Required real-time insights into security device generated data
- Required ability to quickly leverage new data sets

Business impact

- Ability to meet growing requirements from customers at a competitive price point
- Analyst provided with greater context and special awareness
- Greatly increased turn-around times when integration new and varied data sources
- Real-time insights from disparate data sources

Data sources

- Registry access data
- Networks data
- Security device
- End-point detection systems

Siren Products

- Siren Investigate
- Siren Federate
- Siren Alert

Leveraging state-of-the-art technology at a competitive price point

Innovation in the cybersecurity space has been lackuster by the industry leading vendors, meaning that mainstream solutions have an inherent innability to meets the dynamic and ever-increasing demands of modern security operation centers (SOCs), both in terms of cost and their ability to effectively handle, analyze and leverage vast ammounts of data.

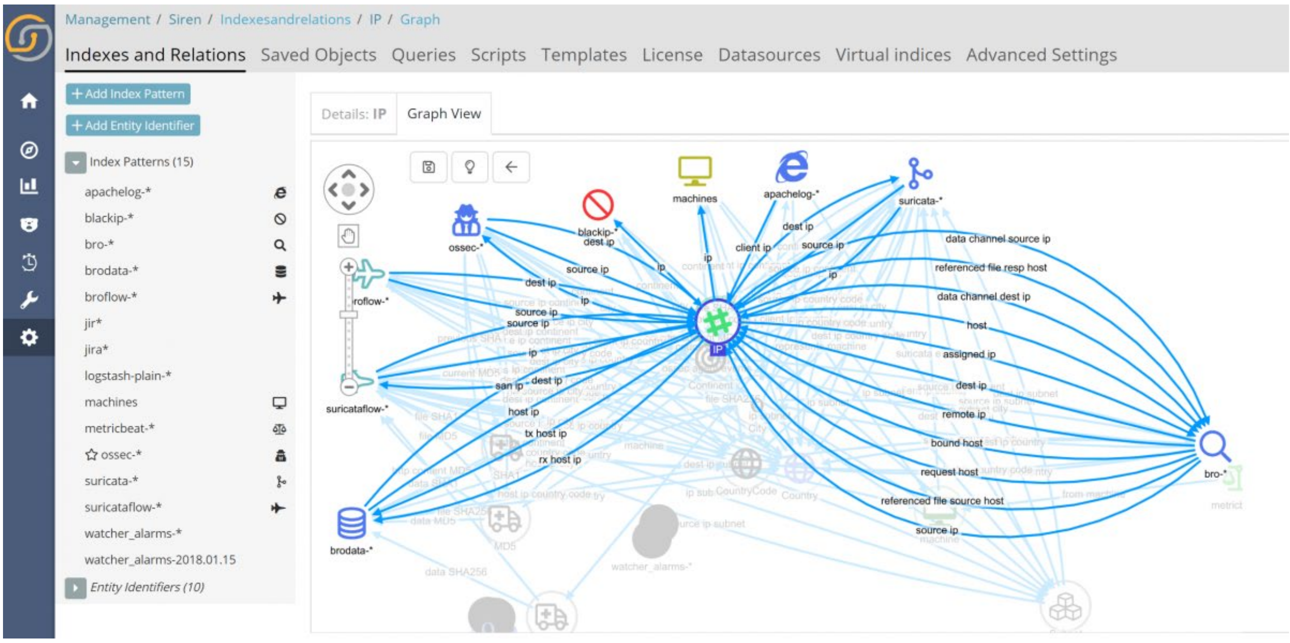
With terabyte's worth of data having to be analyzed on regular intervals, current mainstream approaches, hinder the investigative prowees of operators by creating a backlog of queries to execute if indexing at read time, requiring considerable up-front effort in terms of understanding the underlying schema within the data when forced to enrich data at ingestion time and/or being highly dependent on hardware investments to scale effectively.

> *"When it comes to scenarios with terabytes worth of log data created daily that need to be analyzed, it's a one-horse race regarding all the solutions out there...with Elasticsearch and Siren coming way ahead of any other player in the space"*
>
> ***Jeremy Turner** – Cybersecurity Program Manager*

From siloed datasources to valuable insights quickly and effectively

With the Siren Platform's patented back-end federation capabilties, Crumpton Group's analysts can run queries and create joins in real-time thus bypassing the data-enrichment operational bottle necks that occur either when perfoming this task at ingestion time or at read time.

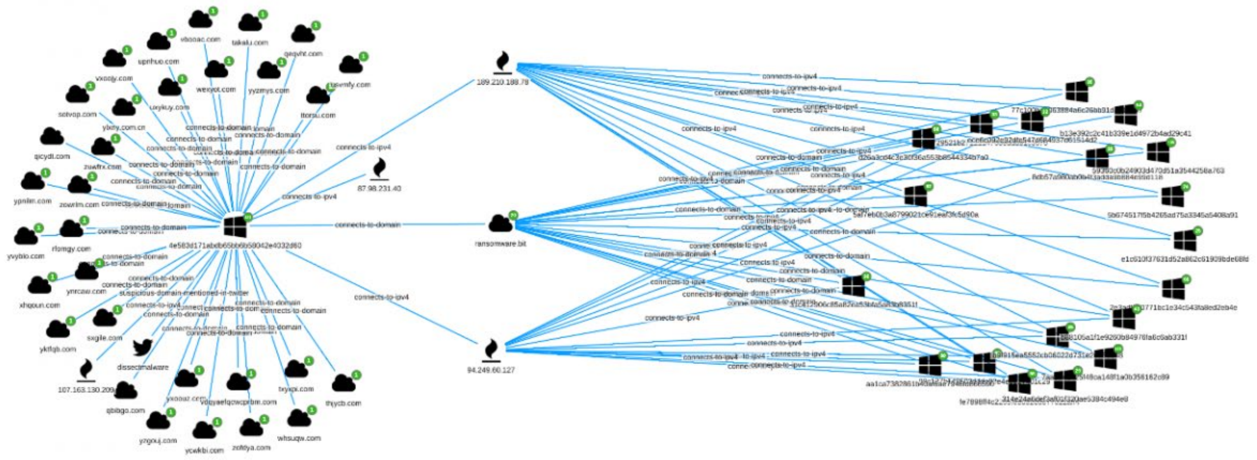
Moreover, the company can now bring all the data into a single pane of glass quickly, monitor logs and associated data across the entire monitoring infrastructure through the use of a dynamic schema, the Siren Data Model, thus ensuring quick time to value.



Providing context in a world of data chaos

Crumpton Group's analyst are now able to effectively and efficiently search through data and leverage Siren's advanced link analysis capabilities to, under a single ecosystem, effectively create a knowledge graph of threats and associated records thereby greately increasing the spacial awareness of operators.

"Providing the analyst with context through graph browser [Siren's link analysis component], is what creates intelligence & insight for Zero-Day scenarios" – Jeremy Turner, Cybersecurity Program Manager


vbooac.com
takalu.com
qeqvht.com
upnhuo.com
vxooly.com
weiqot.com
yyzmys.com
tasvmfy.com
uxykuy.com
solvop.com
ylxhy.com.cn
ttorsu.com
qicydl.com
zuwfrx.com
ypnlm.com
zowrim.com
yvyblo.com
rlomgy.com
4e583d171abdb65bb6b59042e4032d80
ynrcaw.com
xhqoun.com
sxgile.com
ykflqb.com
dissectmalware
107.163.130.209
qbibgo.com
yxoouz.com
vbqyaelqcwcpnbm.com
txyiqi.com
thjycb.com
yzgouj.com
ycwkbi.com
zofdya.com
whsuqw.com
87.98.231.40
connects-to-domain
connects-to-ipv4
suspicious-domain-mentioned-in-twitter
189.210.188.78
ransomware.bit
94.249.60.127
b13e392c2c41b339e1d4972b4ad29c41
d26a3cd4c3c30f36a553b8544334b7a0
59393c0b24903d470d51a3544258a763
5af7eb0b3a8799021ce91eaf3fc5d90a
5b67451715b4265ad75a3345a5408a91
e1c610f37631d52a862c61909bde68fd
b88105a1f1e9260b84976fa6c6ab331f
314e24a6def3af01f320ae5384c494e0