ANALYTICA42

DATASHEET

A42 Velocity

Success for your SIEM/SOAR

Are you making full use of your SIEM/SOAR?

Your logging and analytics capabilities are only one piece of the security puzzle. Unless you're mapping those alerts to a framework (like the MITRE ATT&CK framework), you're just seeing noise—you don't know what's important or how to tune your security protocols.

Companies with a mature threat detection capability go way beyond automated alerts to customize CTI according to environment and goals, and cusomize bahvioral patterns, fine tuning the results to improve decision making. So, how mature is your threat detection?

Only 20%

of security operations practitioners describe their organizations as having a mature security practice

Source: https://www.siemplify.co/resources/the-road-to-security-operations-maturity-a-cyentia-research-report/

A42 Velocity raises your security maturity!

- The A42 Velocity approach enables customers to fully maximise the use of their SIEM & SOAR platforms. Developed by security experts with over 80+ years of combined experience, Velocity can be adopted by any organization regardless of the maturity level of the SIEM/SOAR platform.
- Velocity aligns your Security SIEM/SOAR investment to your business / operations
- Velocity defines clear achieveable goals to measure success

Inhibitors to Success

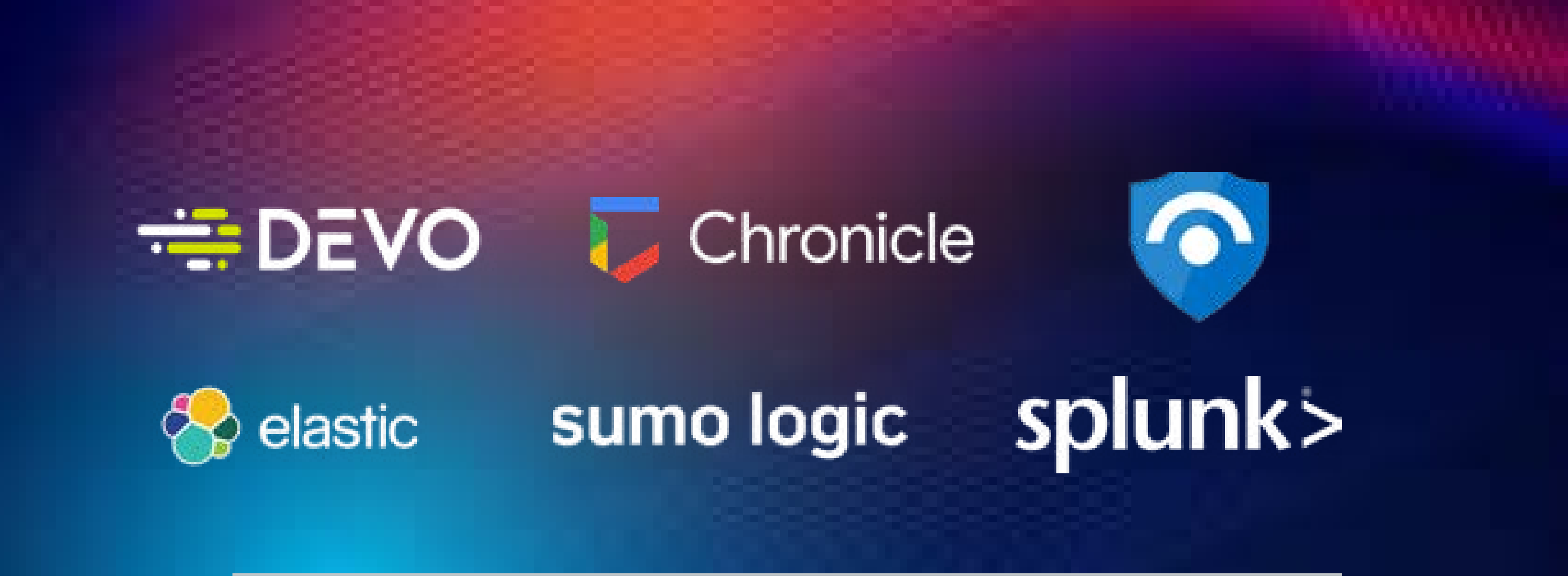
44.4%

Lack Expertise

27.8%

Inadequate Staffing

The top two inhibitors to enterprise SIEM adoption cited were lack of expert manpower (44.4%) and inadequate staffing (27.8%). The two next most common inhibitors were inability to fully complete setup & overall complexity.



Velocity Support Options

GETTING TO KNOW YOU:

- Use Case Workshops
- SIEM/SOAR Detections and Response Capability Analysis
- Defining/Extending your Roadmap

THE BASICS:

- Installation/Configuration
- Data ETL Services (SIEM Migration)

EXECUTING YOUR ROADMAP:

- Use Case Content Research
- SIEM Detections, SOAR Playbooks Dashboards, Reporting Development
- Testing and Validation

OPERATIONALIZE:

- Automation / Integration Services
- Implement Content Change Control Management Process

EXTENDING THE PARTNERSHIP:

- Co-Managed SIEM
- Staff Augmentation/Cross Train
- Threat Hunting

Use Case Knowledge Base

Use Cases to address below but not limited:

Cloud, End-point, Network, SaaS Applications, Windows, Firewall, Custom Application

Content Sources:

Analytica42 Content Repository

OpenSource, Current Events, Public Research, A42 R&D

Custom Detections to address your unique applications

Velocity Results

“Analytica42 is a great partner and became an integral part of our security team. With their Analytica42 Velocity program they significantly accelerated our SIEM Detections capability to help us accelerate the maturity of our program. We would recommend Analytica42 to anyone needing to mature their SIEM/SOAR capability.”
-Major Regional Bank

“After the Analytica42 Use Case workshop, we realized we were completely blind in monitoring one of our core applications. Analytica42 didn’t just identified the issue, they were able to ingest our unique datasource, parse it,

and build critical detections!” - Major Crypto Exhange

ATT&CK®

Contact us to find out how we can increase your organization’s security maturity.

www.analytica42.com