COALFIRE

DATASHEET

Security operations

Enhance your security posture with SIEM engineering

Coalfire's team comprises industry experts in the field of security information and event management (SIEM) technologies. We provide subject matter expertise in Splunk and the Elastic Stack as the two best-of-breed tools.

With decades of experience with Splunk and Elastic Stack, our experts can create custom content for your environment. Whether compliance, security, and operations are your focus, or you want to enhance your security posture with log analytics and awareness, we will build a SIEM solution that fits your needs.

COMPLIANCE EXPERTISE

We have developed in-house compliance and security applications to assist in certification audits for Splunk and the Elastic Stack SIEM tools in accordance with NIST control families, which can be applied to all levels of FISMA, Cybersecurity Maturity Model Certification (CMMC), and FedRAMP certifications. Our compliance advisors also build and consult on Splunk and Elastic Stack SIEM solutions for other frameworks, including HIPAA, PCI DSS, SOC, ISO, and HITRUST.

INDUSTRY PARTNERSHIPS

Through our partnership with Elastic, we developed an application to help clients meet the needs of the Department of Defense's CMMC. Coalfire's CMMC Application powered by Elastic can be installed in an Elastic Stack environment built by Coalfire on-premise or in the cloud.

SECURITY-FIRST MINDSET

Our goal is to enhance your security posture in every aspect. By building a SIEM or log aggregation tool, you've taken the first step toward realizing a more in-depth view of your environment's infrastructure. With decades of security experience, we design and optimize your SIEM environment to create enhanced dashboards, reports, and alerts to ensure your security program is highly effective and relevant.

BEST PRACTICE SIEM

Our SIEM experts have the certifications and experience to back up your environment build process. We combine our comprehensive experience with best-practice recommendations from each SIEM vendor to create a robust toolset that enhances your security posture and prepares you to administratively maintain your SIEM environment logically.

WHAT CAN A SIEM DO FOR YOU?

- Create a holistic view of your environment
- Centrally collect, store, and analyze logs from perimeters to endpoints
- Monitor for security threats and alert you accordingly

HOW CAN COALFIRE HELP YOU?

- We can build a Splunk or Elastic Stack SIEM environment to create a single tool capable of analyzing all the data in your environment.
- Using the SIEM tool, we build custom dashboards, visualizations, alerts, and reports to meet the requirements of compliance frameworks and your organization.
- We can use the SIEM tool to create custom alerts to increase security and operational posture.
- After building a SIEM tool, we provide continuous maintenance and operations of that tool to decrease your staff overhead for the care and feeding of the tool.

SIEM ENGINEERING SERVICES

- Complete architecture design and build of Splunk or Elastic Stack on-premise or in the cloud
- Consulting services for pre-existing Splunk or Elastic Stack environments
- Optimization of pre-existing Splunk or Elastic Stack environments
- Building of custom dashboards, visualizations, and alerts
- Data ingestion and parsing of log sources to the SIEM tool
- Hosting workshops to determine the best SIEM tool for your needs
- Continuous monitoring and optimization of your SIEM environment

CERTIFIED TECHNICAL EXPERTS IN LEADING CLOUD, ENCRYPTION, VIRTUALIZATION, AND CONTINUOUS MONITORING SOLUTIONS

EFFECTIVELY INTEGRATE SECURITY INTO YOUR ENVIRONMENT.

Learn more about Coalfire's cyber engineering services.

Coalfire.com | 877.224.8077

About Coalfire

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit **Coalfire.com.**