



SECURING YOUR DATA

In the field of cyber security, engineers are flooded with data. Information, logs, and alerts are delivered faster than any individual or team can meaningfully interpret. Teams become numb to the magnitude of information, leading to what is commonly called "alert fatigue", i.e., ignoring important alerts because they are masked by the flood of irrelevant information. Furthermore, to truly gain useful insights from the available data, cyber security professionals must be able to combine data from multiple, diverse sources in unexpected ways. To address these needs, Layer 3 Communications has developed a **Security Information Event Management (SIEM)** system.

“ Layer 3 Communications is one of Cypress-Fairbanks Independent School District's premiere strategic partners working to provide highly-complex technological solutions supporting a \$1.2 billion bond. Layer 3 Communications' commitment to excellence coupled with their advanced knowledge in delivering cost effective, innovative technologies is one of the underlying advantages that CyFair is most proud of as we are building the largest smart education network in the nation! ”

- Frankie Jackson, Cypress-Fairbanks Independent School District

The basic concept of every SIEM system is to analyze relevant data from more than one source, identify changes in the normal operating environment, and take appropriate action. For example, when a known malicious behavior is discovered, a SIEM might capture additional information, generate an alert and direct other security controls to stop a given activity.

Our SIEM ingests data at an enormous rate, and enriches that data in real time, including geographical and network information, as well as, correlation with both in-house and 3rd party threat intelligence feeds. The system then uses a combination of pattern matching

rules and statistical correlation to establish relationships between event log entries. In addition, continual advancements of our SIEM allows us to include user and entity behavior analytics (UEBA) and automate our security orchestration and automated response (SOAR).

As in all of Layer 3 Communications' solutions, the real key to our capabilities lies not in the technology, but rather in the expertise of the people behind the tools. Our team of cyber security experts combine decades of experience in the field with a unique knowledge of networking concepts to provide unparalleled insight and analysis.

REALITY CHECK

— \$301.00 —
AVERAGE COST
PER EMPLOYEE
TO REMEDIATE
A SUCCESSFUL
CYBER ATTACK

— 24/7 —
DO YOU HAVE
ENOUGH SKILLED
CYBER ANALYSTS
TO FILL A 24/7
STAFFING PLAN?

— \$6 TRILLION —
ESTIMATED AMOUNT
TO BE SPENT GLOBALLY
ON CYBERSECURITY
BY 2021