SAFELY ENABLING BUSINESS

SecureDetect SIEM

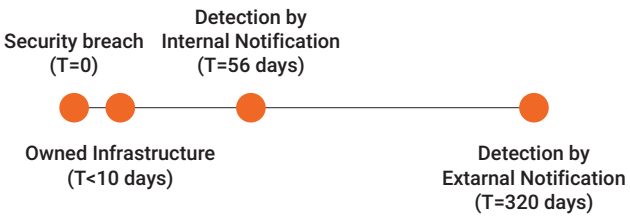
SecureLink are providing SecureDetect SIEM services around the clock to customers ranging from small business to very large global enterprises.

We have customers across all different types of markets including healthcare, government, finance, industry and retail.

We live in an age of increasing reliance on digital systems. As the world becomes more interconnected and organisations move more of their business to the cloud, the threat and scope of cyber-attacks continues to grow rapidly.

High profile data breaches used to be few and far between, hidden away amongst the pages of the tech section of the news or dedicated industry resources. The reality now is that they are common and increasingly frequent.

There is no such thing as 100% protection. So you need to have people, processes and technology in place to be able to detect and respond if and when you get breached.



It is about balance

Most organisations have invested the majority of their security budget into protection, and left little to none for detection and response. As much as protection increases, it will never reach 100% so what do you do with the things you cannot protect yourself against? And how do you detect what you have missed and respond accordingly?

The main challenges that need to be addressed to be able to improve the detection of threats and breaches are:

- **Lack of visibility**
  Data stored in different silos.
- **Lack of understanding**
  Correlation, enrichment and security analytics are complex.
- **Lack of resources**
  Detecting threats requires technology, intelligence and expertise.

This requires people, processes and technology that most companies do not have, cannot find or retain, or cannot afford to invest in.

In an attempt to try and compensate for the lack of people, many organisations find themselves spending more on their SIEM platform, hoping to achieve a higher degree of automation with less human analysis; however, this can only take you so far.

SecureDetect SIEM

Why buy a service?

Increasing numbers of companies today are choosing to buy this as a service. The main benefits of this approach are:

- Lower and more predictable monthly costs
- Access to a larger team of experienced analysts with high levels of skill and expertise
- Global view of threats across geographies, industries and companies of all sizes

The SecureDetect SIEM Service

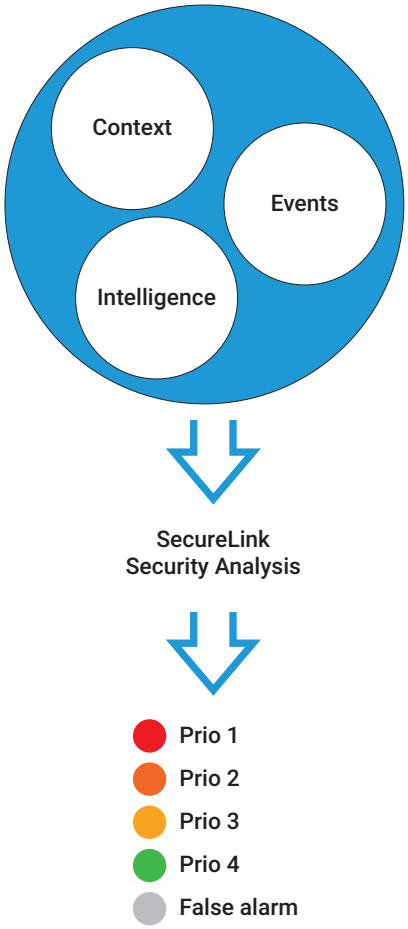
The SecureLink SecureDetect SIEM Service collects events from our customers systems, enriches the events with threat intelligence, adds context and then matches it to a set of use cases for threat detection that is relevant for our customers and their specific environment. This provides a high detection rates and a low amount of false positive alerts.

The indicators created are then forwarded to the security analysts in our Cyber Defence Center (CDC). They will analyse, verify and classify the incident, and then report back to our customers with information about the incident and recommended actions to mitigate it.

Traditional approaches to the managed SOC have focused on collecting as many logs as possible and have utilized baselining exercises, alongside a combination of correlations. These are put together with the intention of "greater visibility", to try and spot anomalous behaviour. This approach does not account for real business requirements and is prone to false positives and soaring costs.

The SecureLink CDC is the next step up from traditional outsourced SOC functions; utilising a business driven, "use case" based approach, the SecureDetect SIEM service provides a set of standard use cases to provide our customers a quick time-to-value, alongside building custom use cases that deliver a defined goal to safely enable your business.

- Do you have a need to increase visibility and detection for your company?
- Are you fed up with your current MSSP not providing actionable advice that helps you to increase your level of security?
- Do you want a service provider that can help you all the way from security advisory to incident response and forensics?



Please contact us to learn more about why we have so many satisfied customers:
www.securelink.net/contact-us