AT A GLANCE

- Cloud Native platforms give natural scale and resilience
- True vendor agnostic log ingestion, parsing and storage
- Siemplify SOAR platform automating actions across numerous vendors
- A modular approach to security, with each service adding unique benefits
- 365 days retention with options to store for longer offline
- Instant search of any logs within the platform
- Running on core Google infrastructure rather than public cloud, so allows you to keep control of your cloud spend.
- Unlimited volume of log volume and sources

SEP2.security

SEP2.security is SEP2's modular MDR (Managed Detection and Response) service. It is based on the Google Chronicle SIEM platform, bolstered by the functionality of the Google Siemplify SOAR (Security Orchestration, Automation and Response) and allows for your security team to get top-tier insight into potential threats, with the SEP2 Security Intelligence Services team at the helm to respond to and assess events.

The technical elements of the platform are cloud-native, with multi-tenancy built in with each customer having their own encrypted space within the system. Using the same underlying platform as the core Google Search, Chronicle provides near-instantaneous access to security and event data within an organisation, with online retention of the data for 12 months.

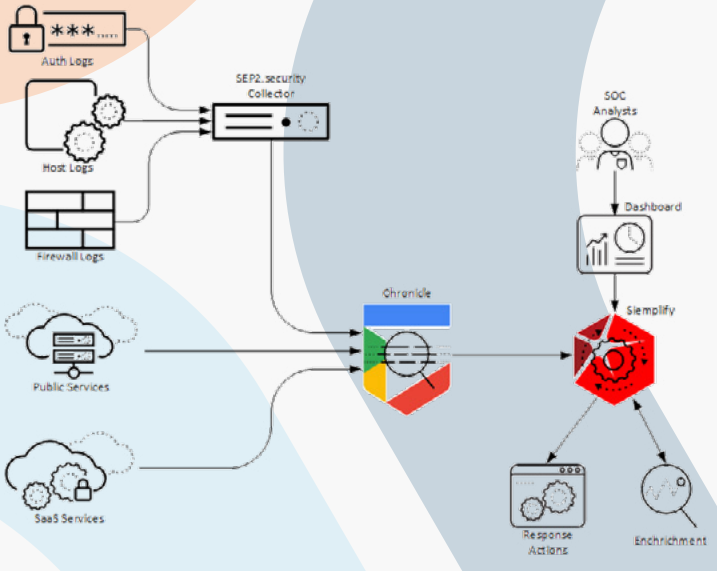
MDR is generally focused around an EDR (Endpoint Detection and Response) or XDR (eXtended Detection and Response).

SEP2.security allows for you to bring your own EDR, or gain this capability if you do not already have it.

The architecture allows for a light touch, or no touch, deployment of on-premise systems, in many cases requiring only a single lightweight virtual machine to be deployed for hybrid/on-premise organisations – or in some fully cloud based organisations – no new compute resources required at all.

Using the expertise of SEP2 and Google, we are able to parse logs from an a huge number of sources. Any data added to the system will be used to enrich detection and correlation rules within the SOAR platform.

The licensing of the solution is a flat, per-user model. There are no limits to the volume of log data that can be consumed, across as many log sources as is needed.



ADDITIONAL OPTIONS

- Endpoint Detection and Response
- Network Detection and Response
- Darkweb Monitoring
- Vulnerability Management
- Vulnerability Response
- Incident Response
- User Awareness Training
- Team CISO
- Mail Security

51A St Paul's Street
Leeds
LS1 2TE
0330 043 7372

A service that grows with you

SEP2.security is designed to be modular, adding more protective layers as your organisation requires. Building on top of the base MDR platform, optional elements within the SEP2.security offerings can include:

- Advanced Network Detection capabilities, using sensors to capture internal network traffic for the added visibility
- Endpoint Detection and Response
- Managed user-awareness training and phishing simulations
- Dark and Deep web monitoring for internal asset exposure and potential data loss events
- Vulnerability scanning and remediation service

Tech Driven, People Powered

The service element, delivered by the SEP2 team, brings the technology into your environment in a way that meets your needs.

Building on top of the well-established SEP2 Wingman model, the SEP2.security service provides the elements of services needed to see the benefits from the technology in scope. This includes 24x7 alerting and investigation, functions of incident response, event triage, and analysis.

Each service is discussed and agreed on a per-customer basis, as no two organisations are exactly alike, making it truly fit your organisations needs.

Who are SEP2?

SEP2 are an award-winning cyber-security specialist.

We align ourselves with world-class cyber-security vendors, whose solutions cannot be bettered. However, only by supporting our customers with the very best engineers, analysis and consultants can we get the best out of these solutions.

This is why we say: SEP2 offer a tech-driven service powered by passionate and honest people.

We are here to beat the bad guys. We're here for good.

ISO 27001 ISOQAR REGISTERED

CYBER ESSENTIALS

CRN CHANNEL AWARDS 2020 WINNER Rising Star Award (Reseller)