softline®
Мы всё сможем
30 лет в ИТ

Добрый SOC

Дёмин Максим
Руководитель отдела Информационной Безопасности
Мултон Партнерс

Задача по закрытию списка направлений ИБ

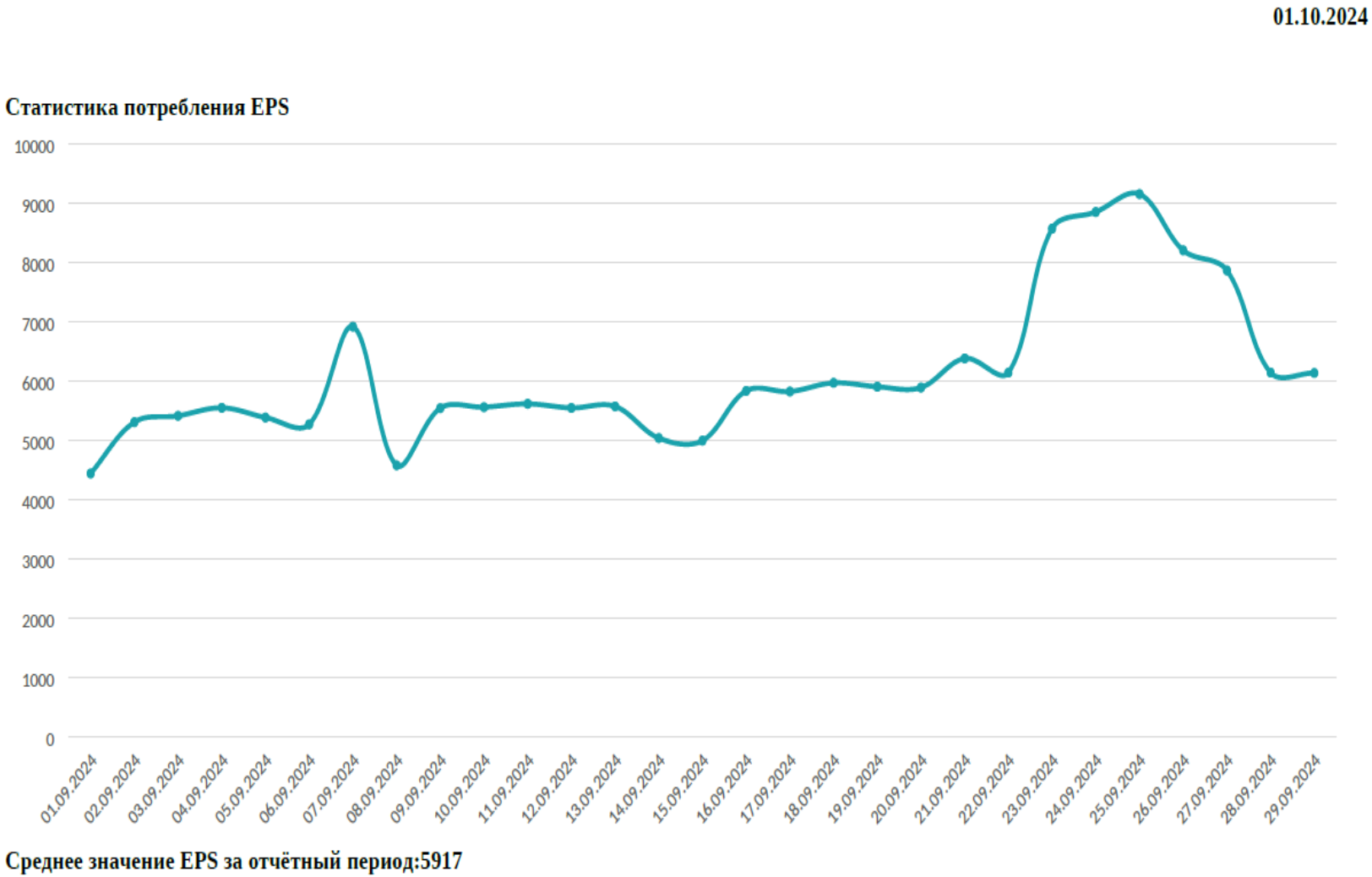
Сервисы и решения для выбора SOC

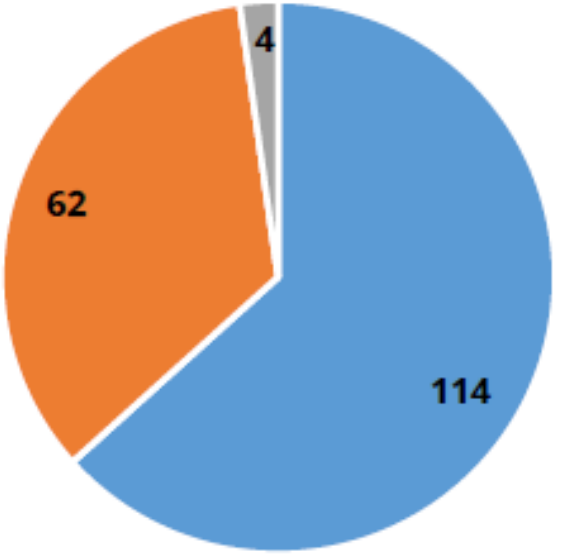
- Incident response IT and OT (not Cyber Crisis)
- Penetration testing
- Network traffic platform management
- Table-top
- Cyber Incident response (IR) & Crisis Management RFP
- Threat hunting service
- Cyber Security monitoring (IT) RFP
- Threat Intelligence service
- Cyber Security monitoring (OT - plants)
- Threat Intelligence service (basic)
- Vulnerability management
- EPM Solution
- Email AntiSpam
- VPN for employees
- Priviledged Access Management
- VDI for externals
- Global Phishing&Awareness Campaign Replacement
- Hardening on Servers

Факторы выбора поставщика услуг SOC

- Инфраструктура основных функциональных компонентов
- Динамичное изменение количества подключенных площадок и масштабирование инфраструктуры SOC со значительным увеличением EPS
- Анализ киберугроз как услуга (регулярный мониторинг и анализ веб-пространства на предмет наличия скомпрометированной информации о Клиенте, служба удаления поддельных веб-сайтов)
- Возможность дополнительного включения услуг EDR, тестирований на проникновение
- Использование лицензий EDR и SIEM

Статистика SOC



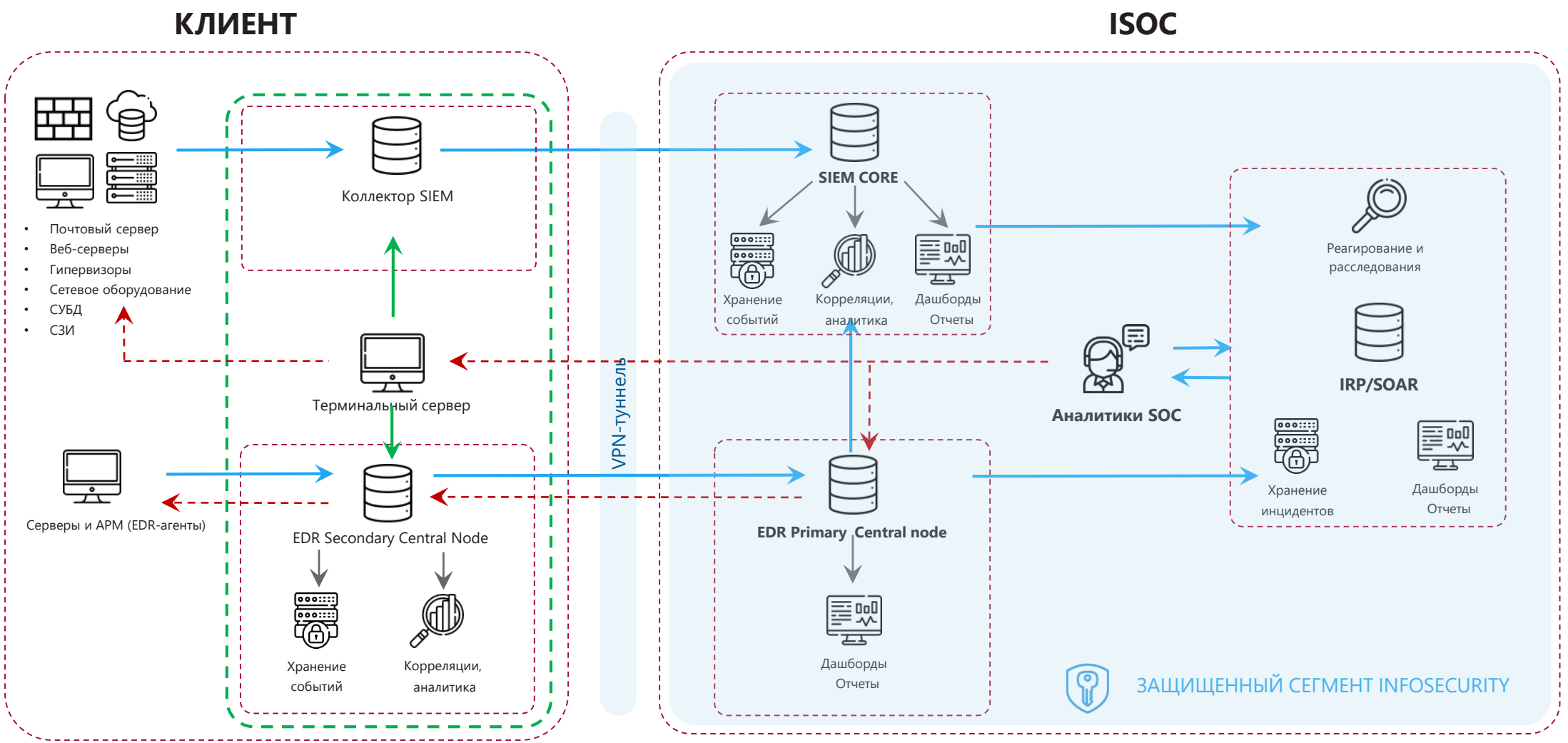


Вердикт - Количество

- Подозрение на инцидент не подтверждено. Легитимная активность (True Positive) - 114
- Подозрение на инцидент не подтверждено. Угроза нейтрализована (True Positive) - 62
- Не определен - 4, в работе.

Всего: 180

Архитектура ISOC



Передача информации

Активное реагирование

Администрирование и поддержка работоспособности

Подключение к ISOC

Источники:

1. Серверы Windows
2. Серверы Unix-like
3. Рабочие станции
4. Почтовые серверы
5. Контроллеры доменов
6. СУБД (Windows)
7. СУБД (Unix-like)
8. Гипервизоры (Vmware, VirtualBox и т.д.)
9. Сетевое оборудование
10. Wireless LAN
11. Система обнаружения вторжений IDS/IPS
12. Иные источники DNS

Срок постановки на сервис ~ 2,5 месяца

Zscaler

Claroty - xDome

Q&A