

6 მიზეზი

თუ რაბომ სჭირდებო თქვენს ორბონიზაციას  
**LOG360**



სახელმძღვანელო

2023

Since 2015

## თუ ამ გამოწვევიდან თქვენს ორგანიზაციაში 3 მათგანს მაინც აწყდებით:

- 1 კომპანიაში, არსებულ სისტემებში (Soft/Hard) წარმოქმნილი პრობლემებისა და გამომწვევი მიზეზების უმოკლეს დროში აღმოჩენის სირთულე, რაც შემდგომში იწვევს კომპანიის სამუშაო პროცესის შეჩერებას (დაუნთაიმს);
- 2 ლოგების ანალიზისას, თანამშრომლის მიერ, შეცდომების მექანიკურად დაშვება (მათ შორის, გამორჩენილი უსაფრთხოების ლოგები) და ათასობით წყაროებიდან ლოგების თავმოყრის სირთულე;
- 3 სხვადასხვა წყაროების ლოგებს შორის, კორელაციის აღმოჩენის სირთულე;
- 4 თითოეული წყაროს ლოგების დაარქივება;
- 5 Custom აპლიკაციებიდან, ლოგების ავტომატურად შეგროვება (აპლიკაციები, რომლებსაც არ აქვთ ლოგების ავტომატური ფორვარდინგის ფუნქცია);
- 6 ლოგების მიხედვით, თანამშრომელთა სამუშაო ქცევის, უჩვეულო გამოვლინების აღმოჩენა.

**მაშინ, კომპანია სინთაქსი LOG360-ის საშუალებით, არსებული გამოწვევების გადაჭრის გზებს გთავაზობთ.**

**LOG360 (Unified SIEM tool & SOAR solution) - წარმოადგენს ერთიან კონსოლს, სადაც შესაძლებელია სხვადასხვა წყაროდან, ორგანიზაციის ლოგების ავტომატურად თავმოყრა და მათი მართვა.**

- 1 შეძლებთ ათასობით ლოგში მარტივად აღმოაჩინოთ თქვენთვის საჭირო/პრობლემური ჩანაწერი, რომელიც აფერხებს ბიზნეს პროცესებს (დაუნთაიმის შემცირება);
- 2 შეძლებთ ლოგების სორტირებას თქვენთვის საჭირო ფილტრებით, თანამშრომლის მიერ მექანიკური შეცდომების დაშვების (კრიტიკული ლოგის უყურადღებოდ დატოვება) თავიდან ასაცილებლად;
- 3 შეძლებთ თქვენთვის საჭირო ლოგების ავტომატურ კორელაციას (Eventlog Analyzer), რაც დაგეხმარებათ სწრაფად დააიდენტიფიციროთ თქვენს IT ინფრასტრუქტურასთან დაკავშირებული პრობლემები და შეამციროთ უსაფრთხოების გამონწვევა;
- 4 შეძლებთ შემოსული ლოგების არქივების ნახვას ნებისმიერ დროს (ლოგები ავტომატურად არქივდება 24 საათში ერთხელ, ხოლო 7 დღეში ერთხელ ხდება კომპრესაცია);
- 5 შეძლებთ თქვენი ინდივიდუალური პროგრამული უზრუნველყოფებიდან (რომელსაც არ აქვს ლოგების ავტომატური მინოდების ფუნქცია) ავტომატურად მოაქციოთ ლოგები ერთიან სივრცეში;
- 6 შეძლებთ მომხმარებლის ქცევის (დრო, სიხშირე, მუშაობის ჩვეული შაბლონი) ავტომატურ შესწავლასა და უჩვეულო ქცევის შემთხვევაში, სისტემაში ავტომატურად მიღებული შეტყობინების ნახვას.

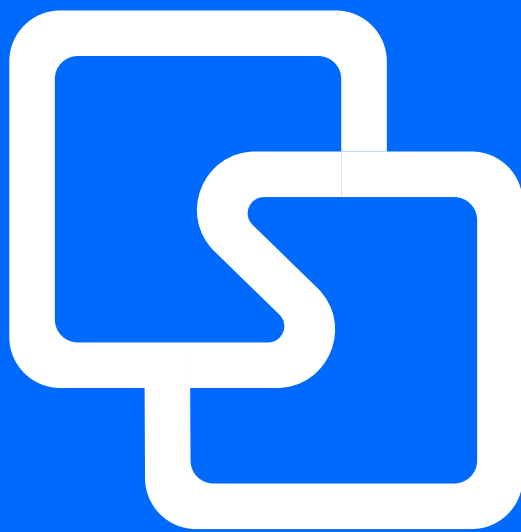
## LOG360 შედგება:

- EventLog Analyzer
- AD Audit Plus
- Exchange Server Auditing
- M365/Azure AD Auditing
- User & Entity Behavior Analytics (UEBA)



## შეჯამება

**ManageEngine LOG360** - შესაძლებლობას მოგცემთ ერთიან სივრცეში მოაქციოთ ათასობით ლოგ ფაილი, აკონროლოთ, ავტომატიზირებულად მიიღოთ ინფორმაცია კოლერაციებისა და უჩვეულო ქმედებების შესახებ და ამ ყველაფრის დახმარებით, უზრუნველყოთ კომპანიის შეუფერხებელი მუშაობა და უსაფრთხოება.



**დამატებითი ინფორმაციის მისაღებად  
დაგვიკავშირდით**

**E-mail: [sales@syntax.ge](mailto:sales@syntax.ge)**

**Phone: (032) 2 88 00 99**

**[WWW.SYNTAX.GE](http://WWW.SYNTAX.GE)**