



გამონკვევები და გადაჭრის გზები

LOG360-ის ჭრილში

Since 2015

გაპოზიციონირება

ლოგების ანალიზისას, თანამშრომლის მიერ, შეცდომების მექანიკურად დაშვება (მათ შორის, გამორჩენილი უსაფრთხოების ლოგები) და ათასობით წყაროებიდან ლოგების თავმოყრის სირთულე;

Custom აპლიკაციებიდან, ლოგების ავტომატურად შეგროვება (აპლიკაციები, რომლებსაც არ აქვთ ლოგების ავტომატური ფორვარდინგის ფუნქცია);



ორგანიზაციაში, არსებულ სისტემებში (Soft/Hard) წარმოქმნილი

პრობლემებისა და გამომწვევი მიზეზების უმოკლეს დროში აღმოჩენის სირთულე, რაც შემდგომში იწვევს სამუშაო პროცესის შეჩერებას (დაუნთაიმს);

სხვადასხვა წყაროების ლოგებს შორის, კორელაციის აღმოჩენის სირთულე და თითოეული წყაროს ლოგების დაარქივება;

ლოგების მიხედვით, თანამშრომელთა სამუშაო ქცევის, უჩვეულო გამოვლინების აღმოჩენა.

გადაჭრის გზები

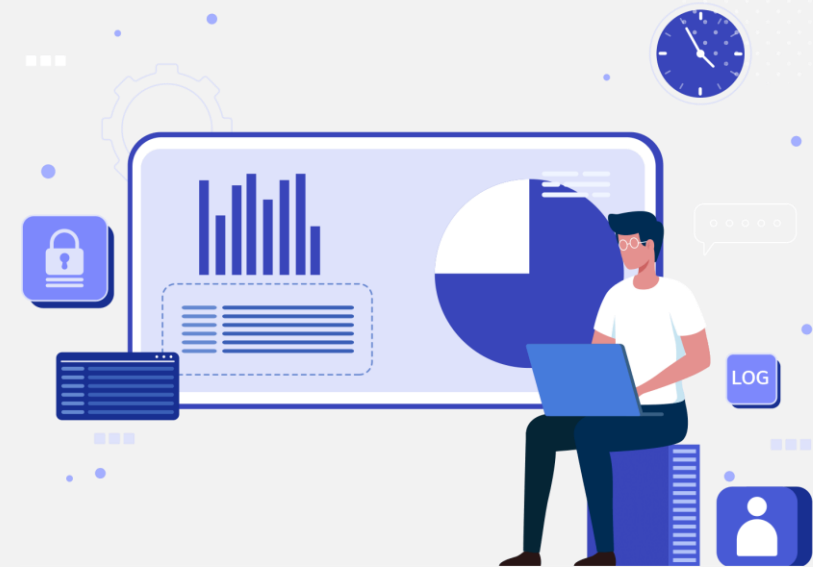
- ✓ შეძლებთ ათასობით ლოგში მარტივად აღმოაჩინოთ თქვენთვის საჭირო/პრობლემური ჩანაწერი, რომელიც აფერხებს ბიზნეს პროცესებს (დაუნთაიმის შემცირება);
- ✓ შეძლებთ ლოგების სორტირებას თქვენთვის საჭირო ფილტრებით, თანამშრომლის მიერ მექანიკური შეცდომების დაშვების (კრიტიკული ლოგის უყურადღებოდ დატოვება) თავიდან ასაცილებლად;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

LOG360

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

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, აკონტროლოთ, ავტომატიზირებულად მიიღოთ ინფორმაცია კოლერაციებისა და უჩვეულო შემდებების შესახებ და ამ ყველაფრის დახმარებით, უზრუნველყოთ ორგანიზაციის შეუფერხებელი მუშაობა და უსაფრთხოება.



მადლობა

E-mail: sales@syntax.ge

Phone: (032) 2 88 00 99

Since 2015