SOCを劇的に効率化
AI分析オプション

LogStare

- ログステア -

ログ分析は ”誰でも” できる時代へ
知識も 技術も 経験も 今まで以上に必要としません

従来のログ分析

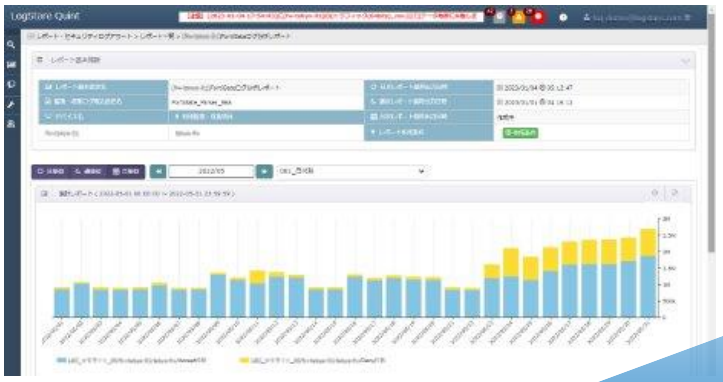
人が目視確認してログレポートの不審な箇所に見当をつけ、ドリルダウン分析で詳しくログを確認。

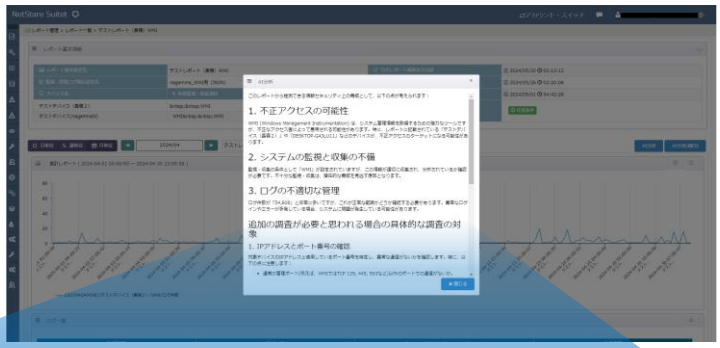
個人の主観に左右される

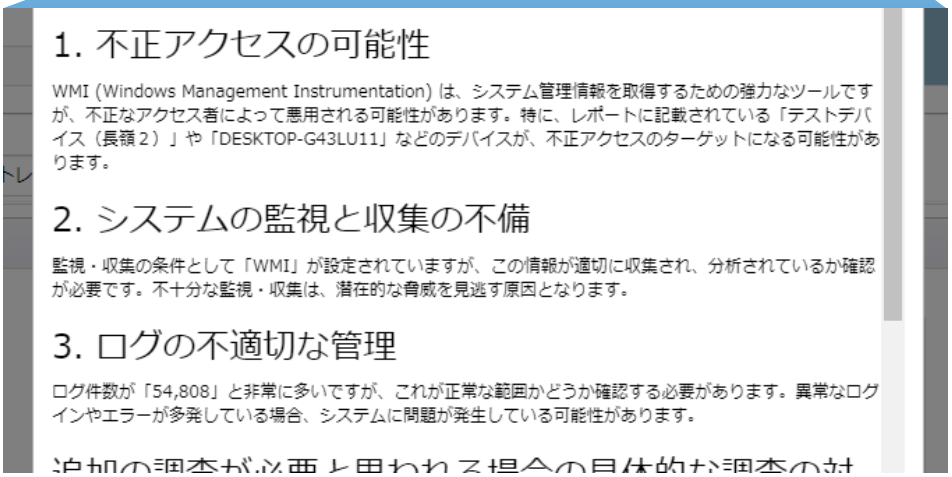
これからのログ分析

AIがログレポートの不審な箇所を見つけ、何を調べれば良いか助言。AIの助言通りに人がログを確認。

誰でもできて結果が均一







- 👍 ログ分析業務の平準化
- 👍 人材育成コスト削減
- 👍 人的ミスの防止
- 👍 属人化の防止

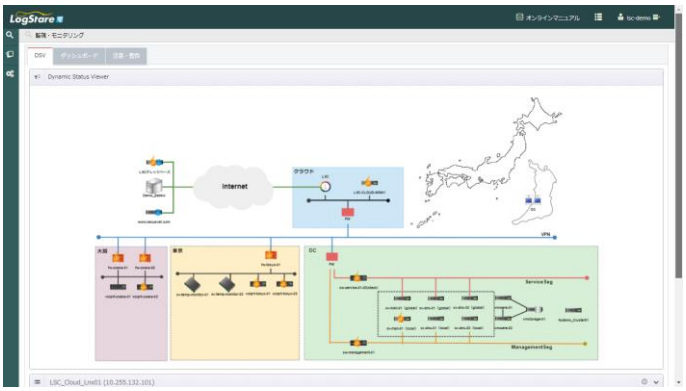
※記載の機能および画面は開発中のものであり予告なく変更することがありますのでご了承ください

株式会社LogStare（ログステア）　www.logstare.com　東京都中央区明石町8-1 聖路加タワー40F

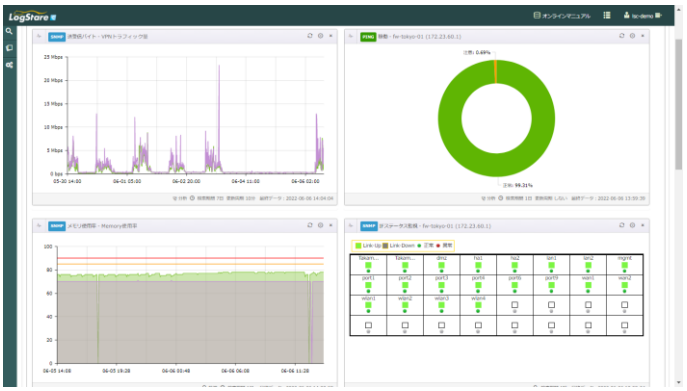
あらゆるログを一カ所に集めて運用を効率化

LogStare（ログステア）は、企業のあらゆるITシステムのログを一か所に集め、IT管理者の運用業務を支援することを目的としたマネージド・セキュリティ・プラットフォームです。
ログ管理とネットワーク監視の機能を併せ持ち、AWSやMicrosoft 365などのクラウドから、オンプレのセキュリティ装置やサーバーまで統合管理。障害のボトルネック発見と早期解決を実現します。

リアルタイム監視で
システムの稼働状況を一目で把握



重要なモニタリング項目を
ダッシュボードで効率的に監視



AIログ分析を実現するSOC監修のログパーサー

常時1.1万台を監視するSOCが監修したログ分析テンプレートを搭載。様々なシステムのログフォーマットを自動的に解析して見やすく成形（パース）し、レポートやアラートを出力します。
このログ分析テンプレートがあるからこそ、AIによるSOC目線のログ分析が実現します。

生ログ

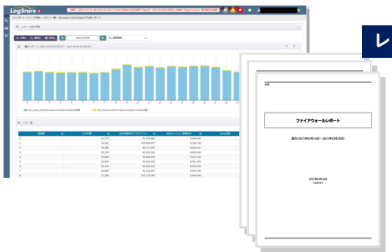
```
Mar 21 04:04:20 192.168.130.2 date=2021-03-21: time=04:04:19 devname="dgw-ngx" devid="FGT50E3U17017766" logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vdom-123" eventtime=1616267060687588743 tz="+0900" srcip=192.168.123.226 srcname="Chromecast" srcport=38067 srcintf="lan" srcintfrole="lan" dstip=172.217.161.35 dstport=443 dstintf="lan5" dstintfrole="wan" sessionid=49044312 proto=17 action="accept" policyid=8 policytype="policy" poluuid="d2b55da0-8ab7-51ea-5b6b-c8ea0aa9a50f" service="C_UDP443" dstcountry="Japan" srccountry="Reserved" trandisp="snat" transip=192.168.133.1 transport=38067 duration=210 sentbyte=3654 rcvdbyte=1777 sentpkt=6 rcvdpkt=5 vwlid=2 vwlquality="Seq_num(1), alive, sla(0x0), cfg_order(0), cost(0), selected" vwlname="general" appcat="unscanned" srchwvendor="Google" devtype="Media Player" srcfamily="Chromecast" osname="Chrome OS" mastersrcmac="6c:ad:f8:de:7c:a6" srcmac="6c:ad:f8:de:7c:a6" srcserver=0
```

パース

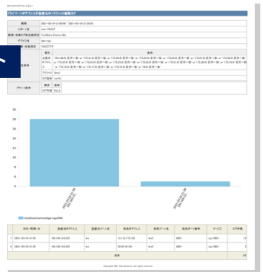
DB

ログ日時	デバイス名	監視・収集	アプリケーション名	デバイス名	デバイスID	ログ種別	ログ種別詳細	バーチャルドメイン	送信元IPアドレス	送信元ポート番号	送信元インタフェース名	送信元ゾーン名
2021/03/21 04:04:19	dgw-ngx	FWログです	Parser_56a	dgw-ngx	T50E3U17017766	traffic	forward	vdom-123	192.168.123.226	38067	lan	lan

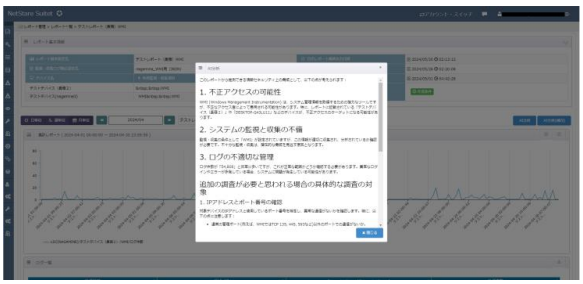
レポート



アラート



AI分析



CHECK!

AIが分析しやすいログレポートやアラートを標準で出力できるのがLogStareの強み。生ログだけではAIも上手く分析できず、結局は人依存になってしまいます。

開発元
LogStare
株式会社LogStare
www.logstare.com
東京都中央区明石町8-1 聖路加タワー40F

ログステア