本レポートの主な知見

- この 12 か月間（2023 年 1 月～ 12 月）では、全体で 29% の Web 攻撃が API を標的にしており、API はサイバー犯罪者の重点領域となっています。
- API に対する攻撃には、「Open Web Application Security Project（OWASP）API Security Top 10」 お よ び「OWASP Top 10 Web Application Security Risks」で挙げられているリスクが含まれます。攻撃者は、SQL インジェクション（SQLi）やクロスサイトスクリプティング（XSS）など、効果が実証されている手法を用いて、標的への侵入を果たしています。
- API のふるまいのベースラインを確立せずに異常な API アクティビティを検知することは困難であるため、ビジネスロジックの悪用が重大な懸念事項となっています。API アクティビティの異常を監視するソリューションを持たない組織は、データスクレイピング（認可された API を使用して内部からデータをゆっくりとスクレイピングする、新しいデータ漏えいベクトル）などのランタイム攻撃のリスクにさらされています。
- API は現在、ほとんどのデジタルトランスフォーメーションの中核となっています。そのため、ロイヤルティ詐欺、悪用、認可、カーディング攻撃など、業界の動向や関連するユースケースを把握することが非常に重要です。
- 組織は、再設計を避けるために、セキュリティ戦略プロセスの初期段階で、コンプライアンス要件や新たな法規制を考慮する必要があります。