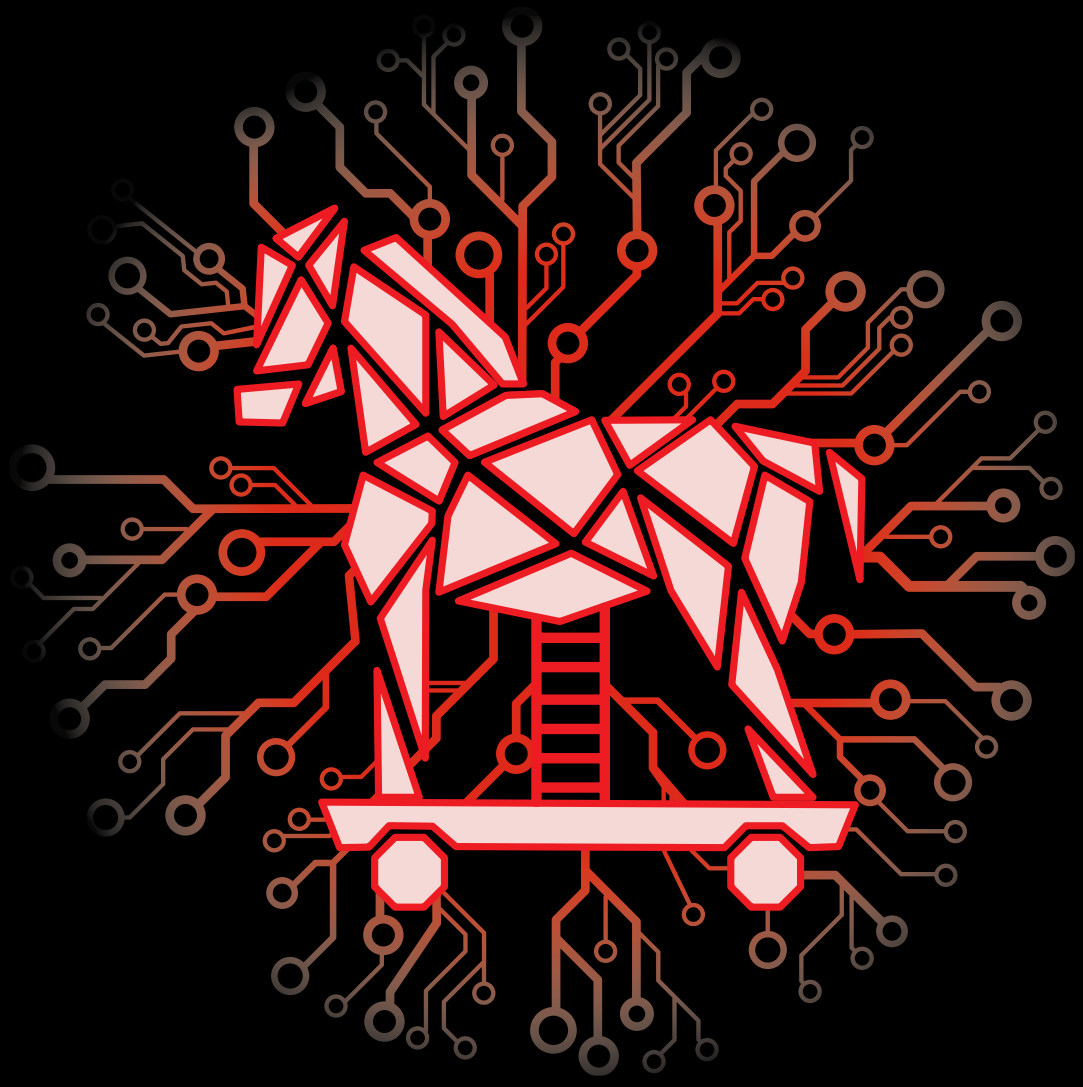
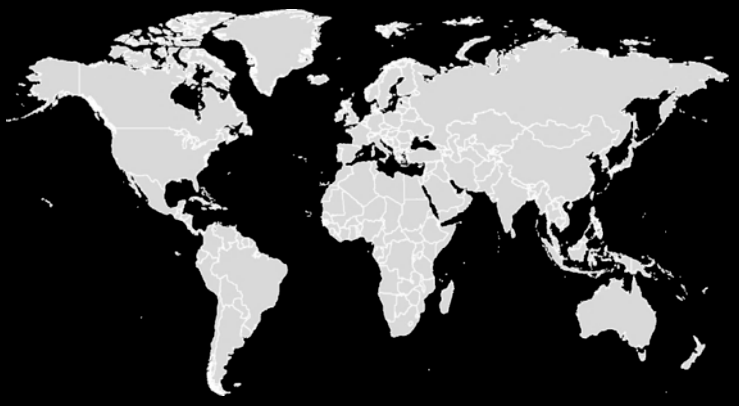
Deloitte.
デロイト トーマツ



Red Team Operations Attackers Report 2020
攻撃者が分析する Red Team Operations

Red Team Opeartaions (RTO) と日本のトレンド2020



COVID-19が及ぼすセキュリティ監視やインシデントレスポンスへの影響

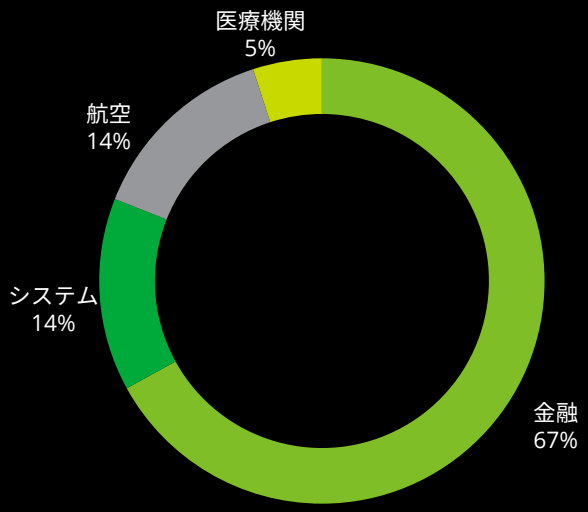
コロナウイルス（COVID-19）の感染拡大により爆発的に増加したリモートワーク環境に対するセキュリティ上の懸念から、日本を含む世界では自社のセキュリティ対策の有効性の確認を求められるケースや、今後懸念が増加すると予想されるエンドポイント対策や端末感染時の監視体制、インシデントレスポンスの有効性にフォーカスを当てた評価を当社のRed Teamと共に確認するニーズが増え始めています。

脅威ベースのペネトレーションテスト（TLPT）を実施するクライアントの増加

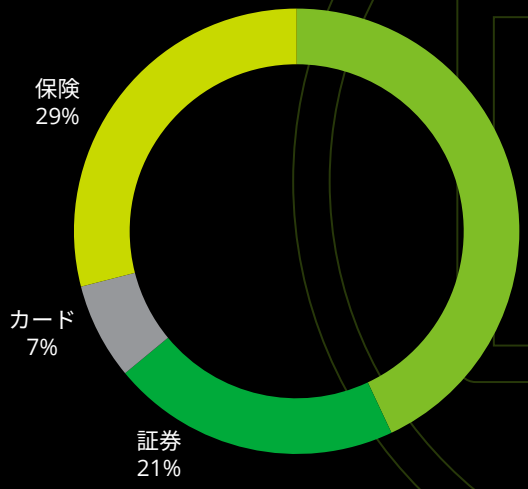
2018年10月に金融庁が発行した、金融分野におけるサイバーセキュリティ強化に向けた取組方針に脅威ベースのペネトレーションテストの実施が明記されました。これを機にTLPTの実施を求めるクライアントが増加しており、2019年はRTOよりもTLPTの実施数が上回る結果になりました。

業界に関する洞察、契約タイプ、および対応の概要

Red Teamを実施した実績のあるクライアントの業態割合
日本国内の実績としては金融業界の割合が最も高くなっています。

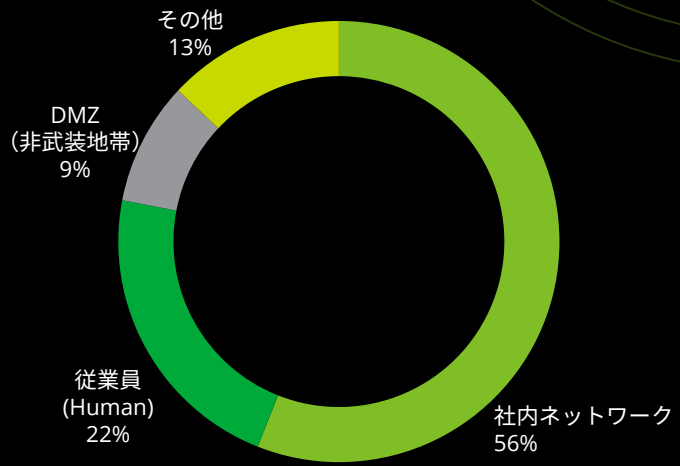


金融業界の中では銀行向けに実施しているケースが40%以上と多く、続いて保険、証券、カード会社に対し、Red Team Operationsに関連した評価を実施しています。



攻撃対象の割合
従業員の業務端末がマルウェアに感染したケースを想定し、OA環境を主な評価の対象とするのが主流になっています。また、昨今ではフィッシングメールを起点としたOA環境の評価等、攻撃対象の範囲に従業員（Human）の要素を含めるケースが増えつつあります。

また脅威情報と絡めて攻撃対象を定めるようなケースも今後増えてくる見込みです。



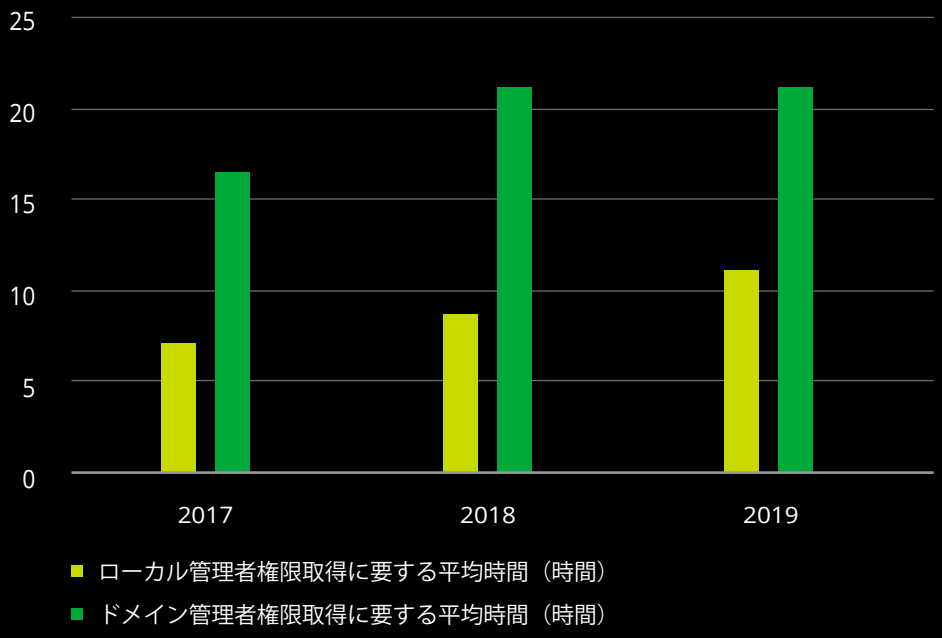
攻撃者のパフォーマンスとクライアントのレジリエンシー

ローカル、ドメイン管理者を巡る攻防

原則として、攻撃目標の達成においてローカル管理者やドメイン管理者等の特権アカウントの取得は避けて通れません。これまで行ってきた評価の傾向として、組織のセキュリティ成熟度と当チームがこれらの権限を取得するために必要な時間には相関関係があり、平均以上に時間を要するケースは攻撃者の活動を制限する対策が有効に機能した結果と言えます。

年ごとの変化ではドメイン管理者権限の取得に要する時間は、増加しています。それは、クライアントの防御チームがより高度になり、組織は、より回復力がついてきています。ローカル管理者権限を取得する時間も伸びており、変化がみられます。

企業の多くはMicrosoft Windows® をベースとした環境を構築しているため、ローカル管理者やドメイン管理者の取得に要する平均時間というのは最も重要な基準の1つになります。ただし、これは唯一の基準ということではなく、信頼できる1つの基準に過ぎません。年ごとに見られるような差異は画期的なセキュリティ対策や監視策の登場、新しい深刻な脆弱性の発見等にも影響するため右のグラフに見られるような傾向は数年で変化するでしょう。



ローカル、ドメイン管理者権限取得率

ローカル、ドメイン管理者共に

96%

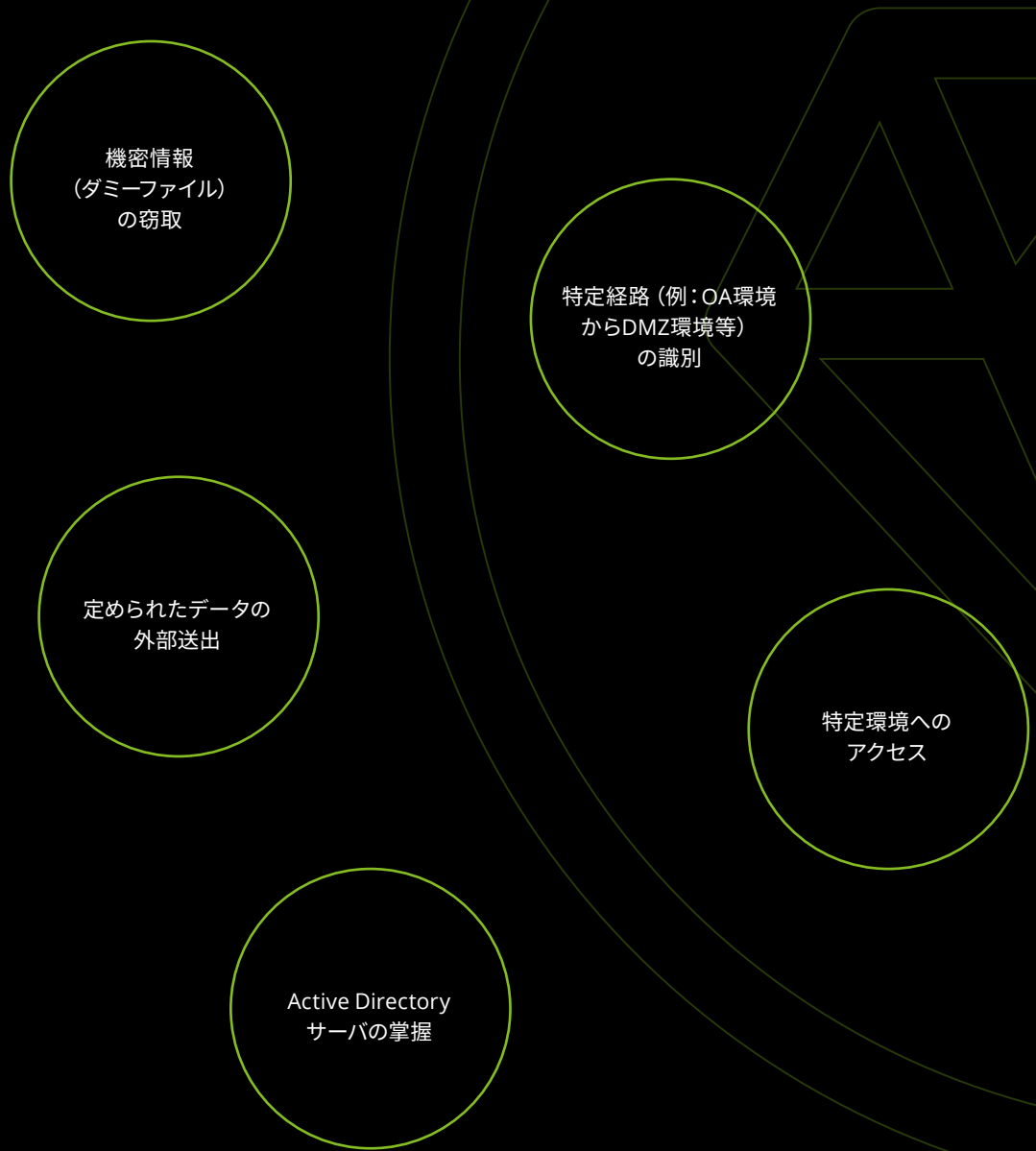
※クラウンジュエルの達成にローカル、ドメイン管理者権限が必要ない場合を除く

攻撃者のパフォーマンスとクライアントのレジリエンシー

攻撃目標の達成率
当チームではRed Team Operationsに関連する評価の94%で1つ以上の攻撃目標を定められた期間内に達成しています。

なお、攻撃目標はクライアントと当チームとの協議によって定められるため、評価ごとに設定される攻撃目標は異なります。

クライアントが選択する攻撃目標例

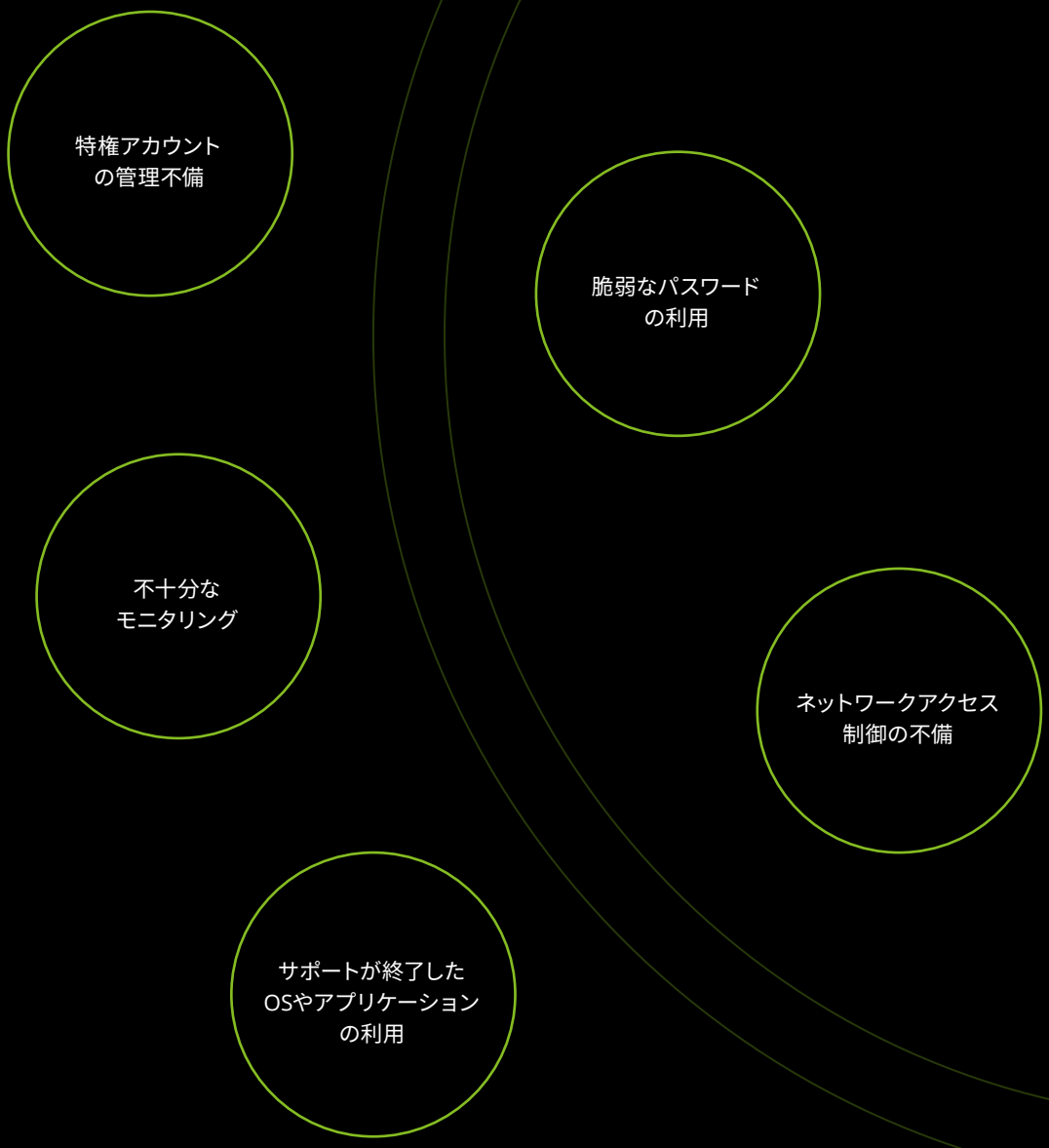


攻撃者のパフォーマンスとクライアントのレジリエンシー

評価毎に識別される発見事項の平均数
当チームでは、平均して8.5件ほどの発見事項をクライアントに報告しています。

ただし、複数回同様の評価を実施しているクライアントは、以前に識別された課題を改善していることからセキュリティの成熟度が向上しており、識別される発見事項の数が前年度より少なくなる傾向になるようです。

クライアントへ報告する発見事項例



業界別および契約タイプ別のクライアントのレジリエンシー

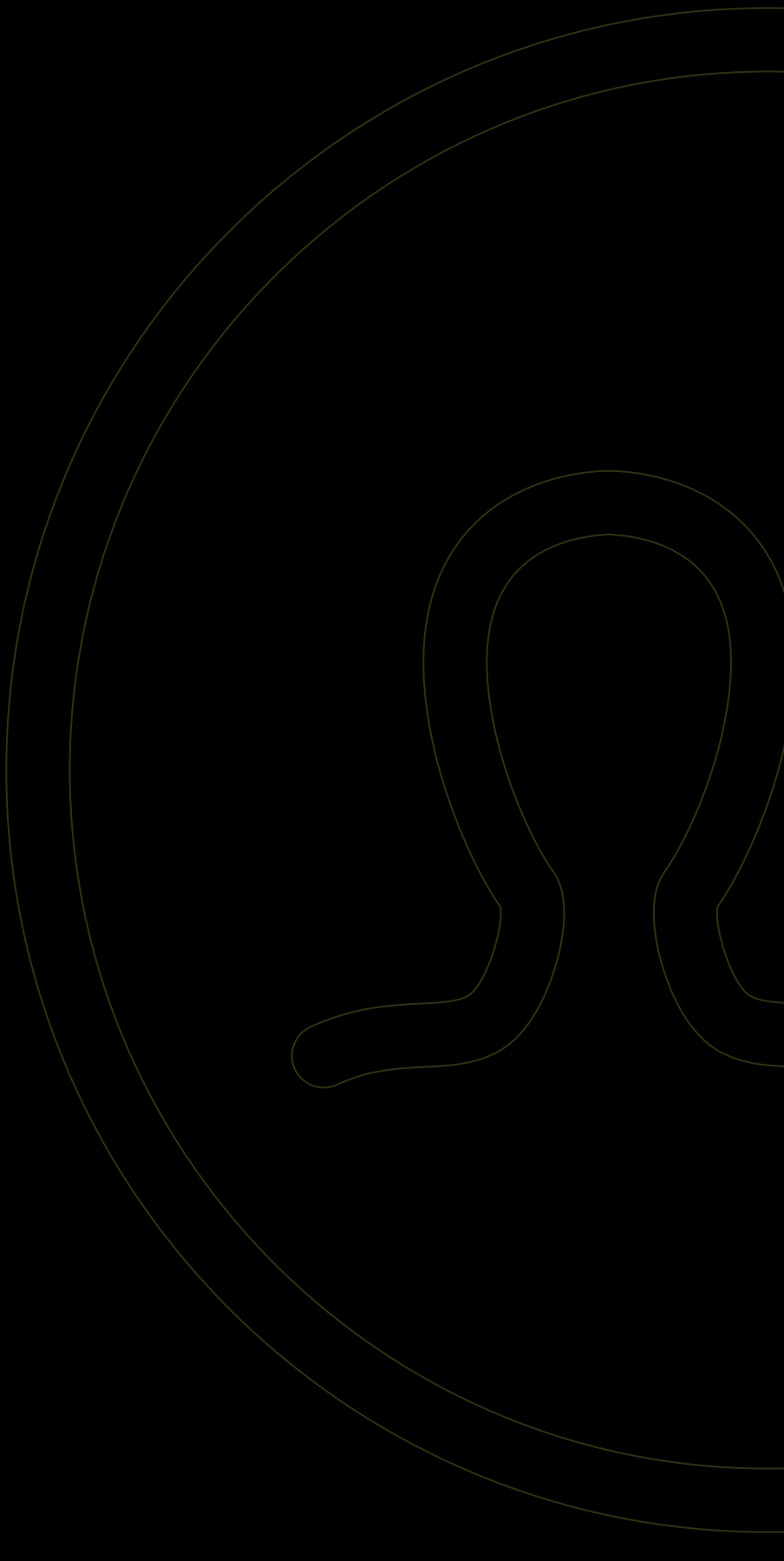
これまでにRed Team Operationsに関連した評価を実施してきたクライアントの業態別に、ローカル、ドメイン管理者権限の取得に要した時間を比較したところ、重要インフラに分類されるような企業はその他の業態と比べてセキュリティの成熟度が高い傾向にありました。

Contacts

野見山雅史 (Masafumi Nomiyama)
masafumi.nomiyama@tohmatsu.co.jp

Ari Davies
ari.davies@tohmatsu.co.jp

Carlo Emmanuele Geraci
carlo.geraci@tohmatsu.co.jp



デロイト トーマツ サイバー合同会社
Mail　ra_info@tohmatsu.co.jp
URL　www.deloitte.com/jp/dtcy
【国内ネットワーク】東京・名古屋・福岡