



Educação, Pesquisa
e Inovação em Rede

ORGANIZAÇÃO SOCIAL DO MCTI

Programa P&D do Hackers do Bem

GT-IMPACTO: Plataforma de Capacitação em Cibersegurança Baseada em Modelagem e Simulação de Aspectos e Impactos Econômicos de Ciberataques

Coordenador Acadêmico: Jéferson Campos Nobre (UFRGS)

<https://inf.ufrgs.br/gt-impacto>

Equipe GT-IMPACTO



Jéferson
Nobre



Laura
Soares



João Davi
Nunes



Henrique
Lindemann



Geancarlo
Kozenieski



Muriel
Franco



Eder John
Scheid



1. Problema

- Gastos globais com Segurança da Informação vão crescer **15%** em 2025^[1]
 - Total projetado de **212 bilhões de dólares**
 - A falta de profissionais de cibersegurança é um dos maiores fatores por trás do investimento no setor

[1] Gartner Forecasts Global Information Security Spending to Grow 15% in 2025. <<https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025>>



2. Contexto do Projeto

- Investimento desses recursos → exige um planejamento de cibersegurança eficiente
- Consultores muitas vezes não tem treinamento sob viés econômico
- **GT-IMPACTO** → capacitação de profissionais com ênfase em **Economia da Cibersegurança**



3. Público-Alvo e Potenciais Clientes

- **Usuários:**
 - Alunos de cursos de cibersegurança
 - Consultores de segurança que desejam aprender sobre modelos econômicos
- **Clientes pagantes:**
 - Organizações de ensino de cibersegurança
 - Instrutores autônomos



4. Antecessor: SECAdvisor [2]

- Ferramenta educacional para planejamento de cibersegurança baseada em modelos econômicos
 - Planejamento de Investimentos
 - Sem uso de relatórios

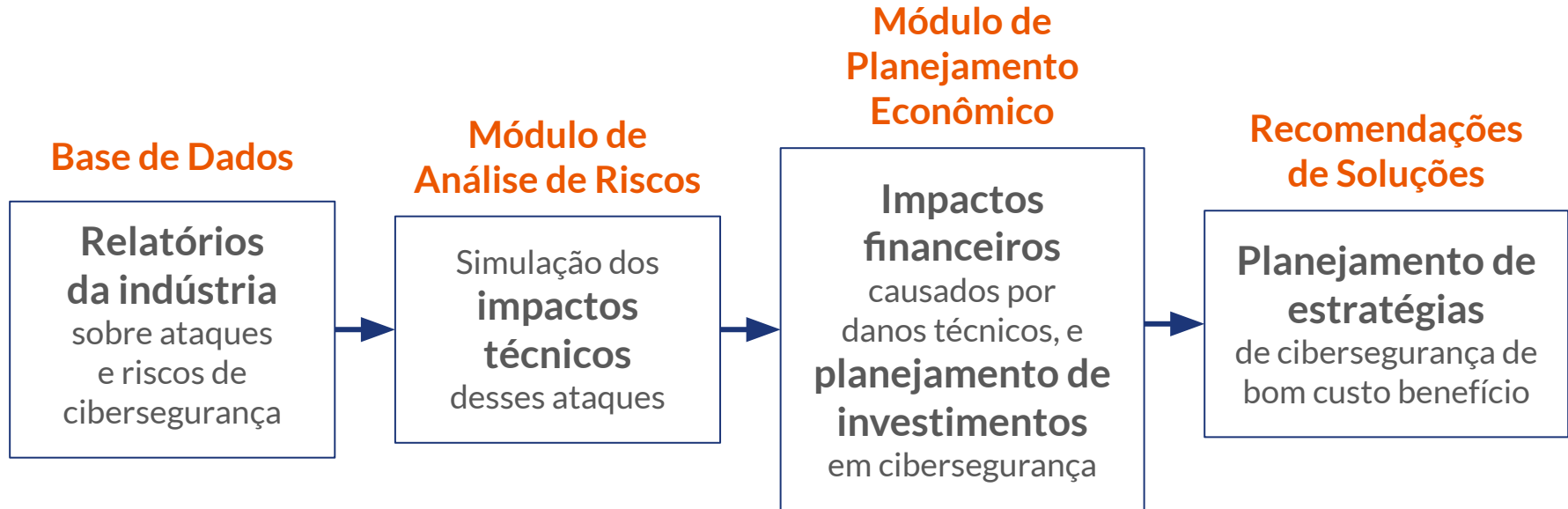
[2] SECAdvisor: A Tool for Cybersecurity
Planning using Economic Models
<<https://doi.org/10.5753/sbseg.2024.240810>>



Módulo de Planejamento Econômico

**Impactos
financeiros**
causados por
danos técnicos, e
**planejamento de
investimentos**
em cibersegurança

5. Plataforma: GT-IMPACTO



6. Proposta de Valor

- Usuário → estudantes e consultores de cibersegurança
- Necessidade
 - Comunicar a gestores e *stakeholders* qual o **investimento ótimo** em cibersegurança
 - Usando modelos econômicos e linguagem de fácil entendimento (\$)



7. Soluções Concorrentes

sem uso de relatórios

Solução	Tipo	Custo (anual)	Simulações	Aspectos Econômicos	Uso Educacional
SECAdvisor	Análise de Riscos, Planejamento de Investimentos	Free, Open-source			
ZERON Cyber Risk Posture Management	Gerenciamento de Riscos	US\$ 6,000 (Startups)			
AttackIQ	Gerenciamento de Vulnerabilidades, Teste de Segurança	US\$ 5,000 (por cada Test Point Engine)			
Qualys VMDR	Gerenciamento de Vulnerabilidades	US\$ 9000 (256 hosts)			
CyCognito Attack Surface Management Platform	Gerenciamento de Assets e Vulnerabilidades	US\$ 30,000 (256 assets)			
Utilis CCS	Treinamento, Resposta a incidentes	Não disponível			
Tanium	Gerenciamento de Endpoints e Riscos	US\$ 36,000			

8. Diferencial Competitivo

- As soluções no mercado:
 - Se concentram no exterior
→ soberania digital
 - São muito caras para o público-alvo
→ estudantes, instituições de ensino e PMEs
 - Não tem foco em economia da cibersegurança e na formação de profissionais



9. Modelo de Receita

- Venda de objetos de software para educação
→ licenças, treinamento
- Eventos customizados



Obrigado! Perguntas?

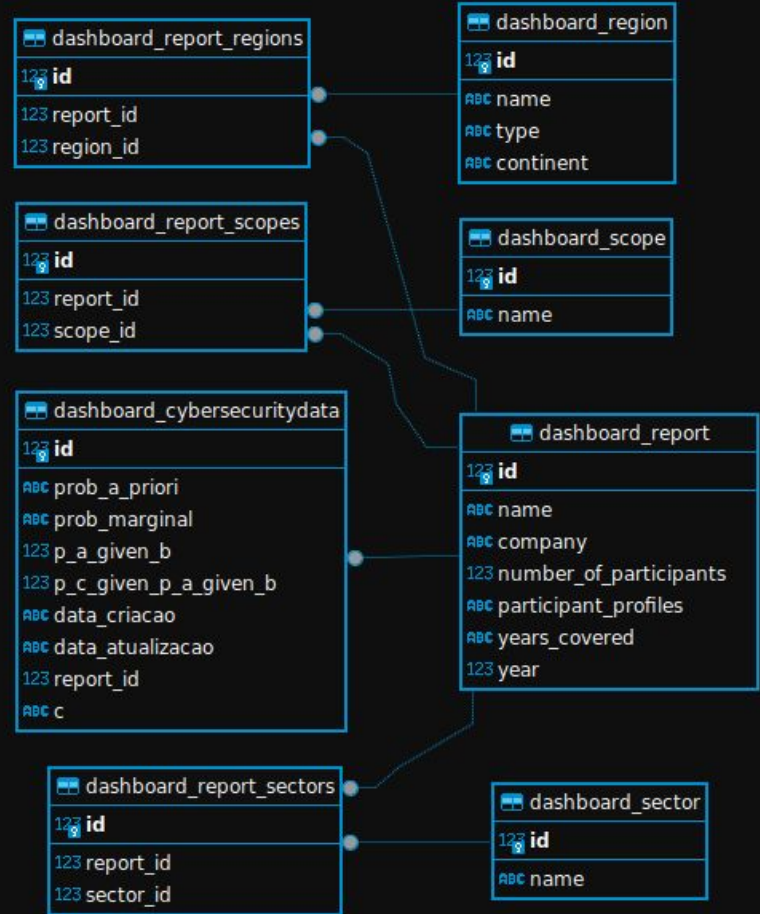
Jéferson Nobre

jcnobre@inf.ufrgs.br



Base de Dados

- Base de dados de relatórios
 - Classificados em Escopo, Região e Setor
 - Apenas relatórios que correspondem ao perfil da empresa sob análise são usados para a visualização de riscos



Dados do Perfil da Empresa

- As características da empresa/cenário são separadas em Perfil Básico e Perfil Avançado
- Com os dados do Perfil Básico, é possível oferecer análises simples de risco baseadas nos relatórios
- Os itens do Perfil Avançado são usados para calcular o escore de risco, que é usado no Planejamento Econômico

dashboard_advancedcompanyprofile	
123	companyprofile_ptr_id
ABC	company_size
123	remote_work_rate
123	global_presence
123	authentication_factors
ABC	cloud_solution_type
123	it_system_monitoring
123	periodic_system_updates
123	data_encryption_in_storage
123	data_encryption_in_transit
123	vpn_for_remote_access
123	cybersecurity_awareness_and_training
123	documented_response_plan
123	response_plan_update
123	operational_recovery_capacity
123	credentials_maintenance
123	vulnerability_identification
123	network_systems_traffic_monitoring
123	threat_identification_process
123	it_records_presence
123	antivirus
123	firewall
123	intrusion_detection_system
123	endpoint_detection_and_response
123	it_security_team

dashboard_companyprofile	
123	id
123	employee_count
ABC	headquarters_country
ABC	industry_type
ABC	name
123	risk_prioritization
123	updated_inventory
123	backup_maintenance
ABC	data_atualizacao
ABC	data_criacao
ABC	headquarters_country_en



Funcionamento da Plataforma

- Cada empresa → um cenário fictício montado pelo instrutor, baseado ou não em empresas reais
- Aluno pode interagir com os dados da empresa e editar parâmetros do cenário para observar seu impacto através de modelos econômicos e visualizações
- Plataforma incorpora ferramentas para aprendizado
 - Fonte das informações apresentadas nos gráficos
 - Informações sobre cálculos e modelos utilizados
 - Ciclo de vida de planejamento em cibersegurança sob um viés econômico

Funcionamento da Plataforma

Para cada cenário, estão disponíveis os módulos da *pipeline* do GT-IMPACTO

MENU

- Dashboard
- Perfil de Empresa >
- Amazon >
 - Perfil de Empresa**
 - Análise de Risco >
 - Gestão Econômica
 - Recomendações
- Configurações
- Fonte de Dados >

Perfil de Empresa de Amazon AVANÇADO

Perfil de Empresa | Análise de Risco | Gestão Econômica | Editar Empresa

Informações da Empresa [Editar]

Nome da Empresa	Amazon
País da Sede	United States
Sector de Atuação	Varejo
Número de Funcionários	1.600.000
Tamanho da Empresa	Grande
Trabalho Remoto	25,0% sim

Dimensão Técnica [Editar]

Inventário Atualizado	sim
Manutenção de Backups	sim
Priorização de Riscos	sim
Fatores de Autenticação	2
Tipo de Solução em Nuvem	WAN

Localizações da Empresa [Editar]

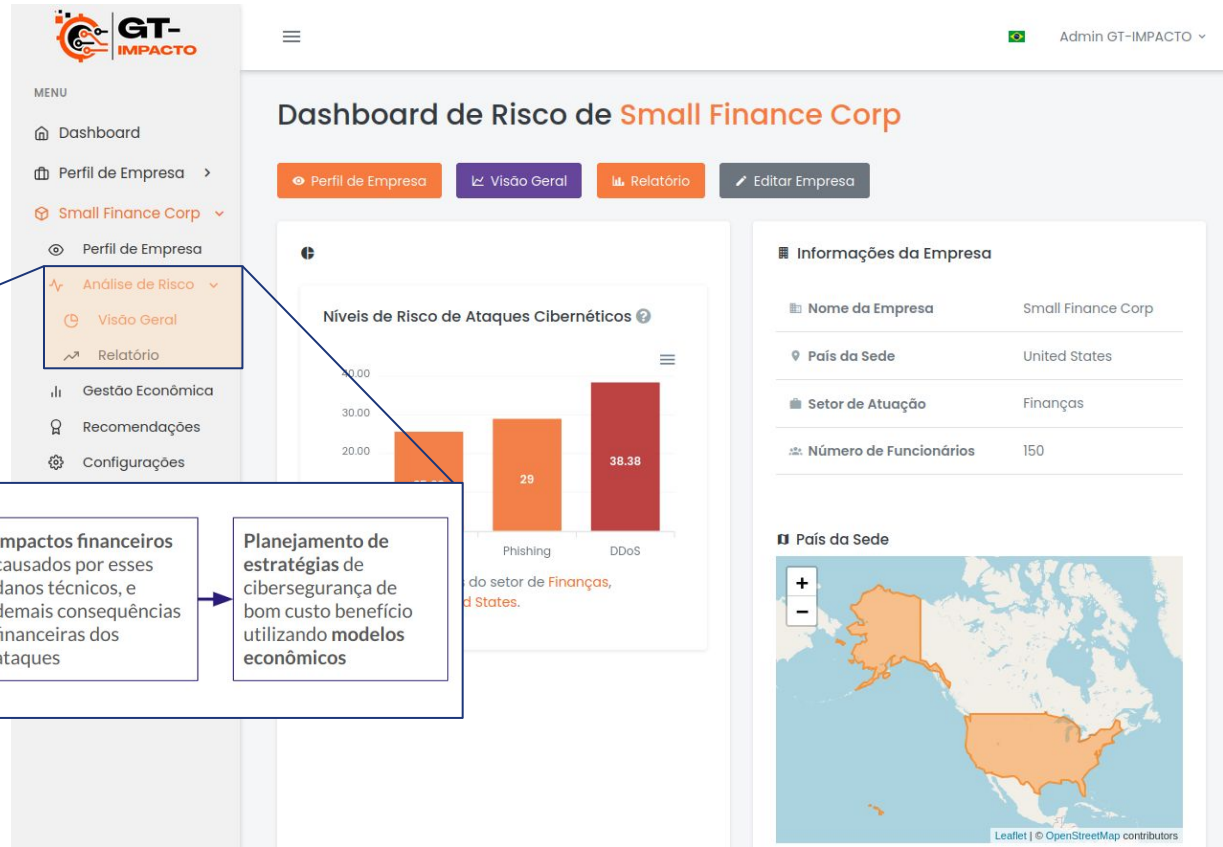
Região	Tipo	Continente
Brazil	País	América do Sul

Flowchart:

```
graph LR; A[Definição de quais são as possíveis ameaças, tipos de ataque, e prováveis consequências de um ataque] --> B[Simulação dos possíveis impactos técnicos desses ataques]; B --> C[Impactos financeiros causados por esses danos técnicos, e demais consequências financeiras dos ataques]; C --> D[Planejamento de estratégias de cibersegurança de bom custo benefício utilizando modelos econômicos];
```

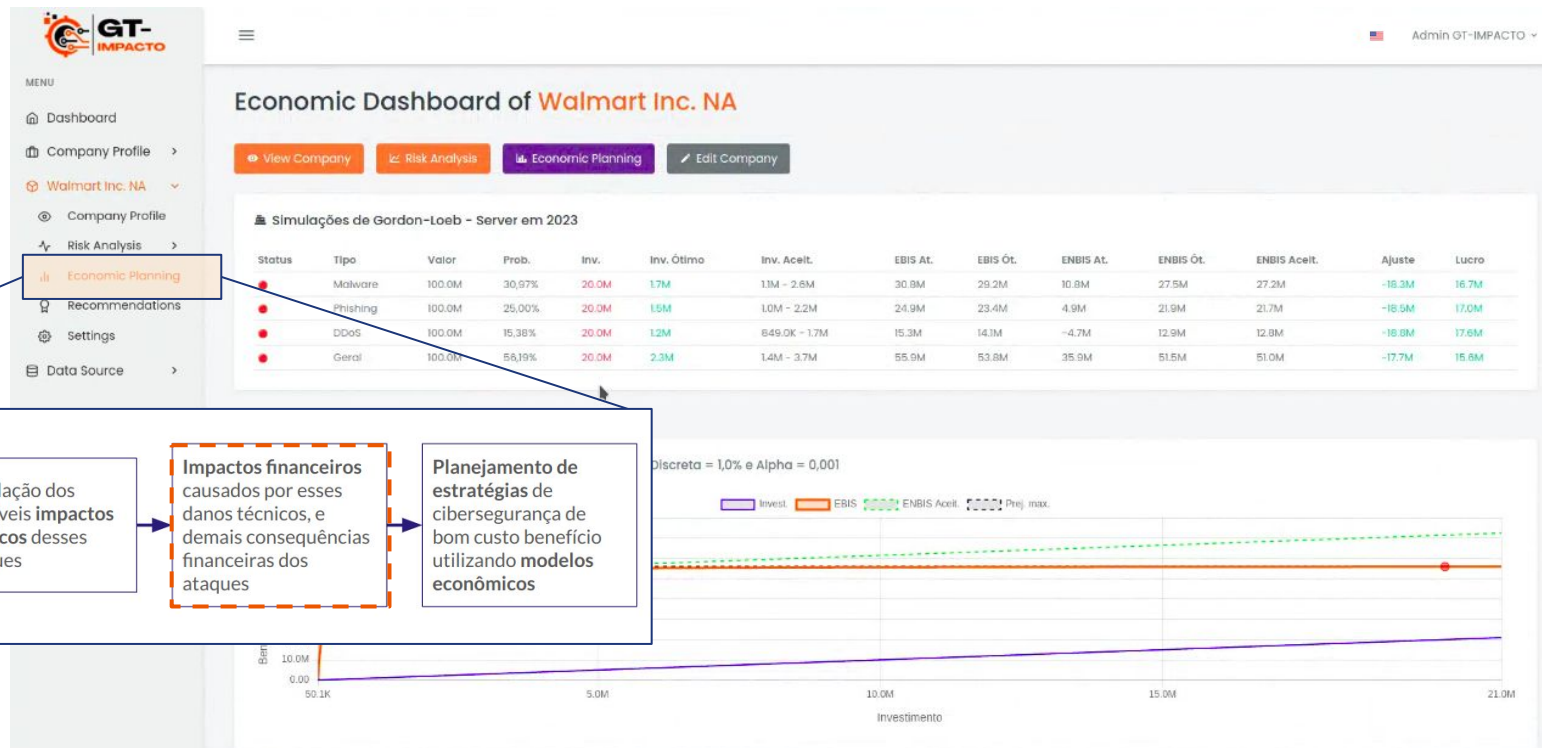

Funcionamento da Plataforma

Módulo de Análise de Riscos baseado nos dados dos relatórios e no escopo do cenário



Funcionamento da Plataforma

Módulo de Planejamento Econômico utilizando Gordon-Loeb



Definição de quais são as possíveis ameaças, tipos de ataque, e prováveis consequências de um ataque

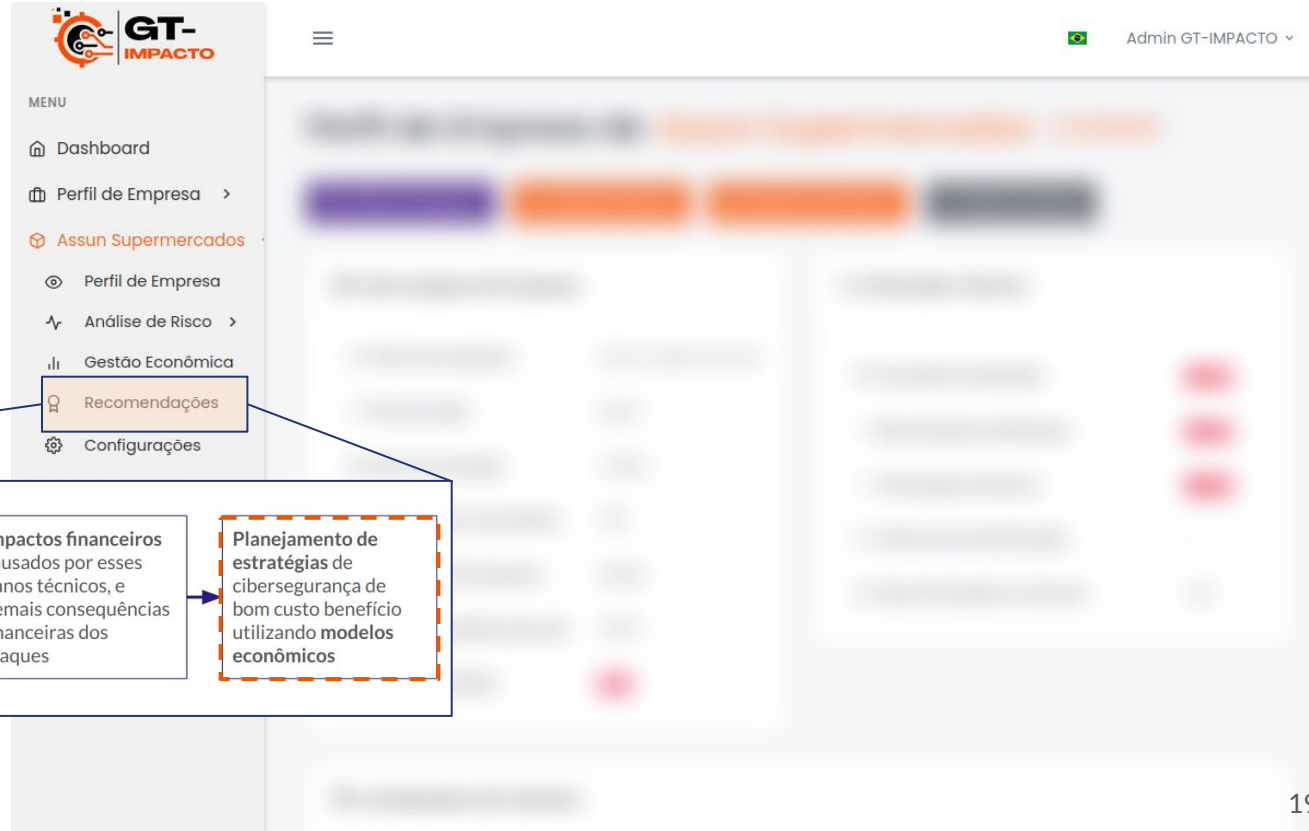
Simulação dos possíveis impactos técnicos desses ataques

Impactos financeiros causados por esses danos técnicos, e demais consequências financeiras dos ataques

Planejamento de estratégias de cibersegurança de bom custo benefício utilizando modelos econômicos

Funcionamento da Plataforma

Módulo de Recomendações de Estratégias de Segurança depende do refinamento dos modelos dos módulos anteriores





Publicações

- Dois artigos sobre o tema do projeto apresentados no **SBSeg24**
 - SIM-Ciber: Uma Solução Baseada em Simulações Probabilísticas para Quantificação de Riscos e Impactos de Ciberataques Utilizando Relatórios Estatísticos
 - SECAdvisor: a Tool for Cybersecurity Planning using Economic Models
- Artigos → versão inicial dos componentes principais do MVP do GT-IMPACTO

Relatórios Utilizados na Base de Dados

Acronis Mid-Year Cyberthreats Report 2023	Acronis
DDoS Threat Landscape Report 2023	Arelion
Healthcare Industry Was the Most Common Victim of Third-Party Breaches in 2022	Black Kite
Retail Cybersecurity Statistics Not To Be Ignored	Fortinet
IBM X-Force Threat Intelligence Index 2024	IBM
M-Trends 2024 Special Report	Mandiant
2022 in review: DDoS attack trends and insights	Microsoft
2023 State of the Phish	Proofpoint
2022 Global Threat Analysis Report	Radware
The State of Ransomware in Financial Services 2023	Sophos
2022: DDoS Year-in-Review Report by StormWall	Stormwall
2024 Data Breach Investigations Report	Verizon