情报驱动的
数字风险保护

Cyberint

情报驱动的数字风险保护

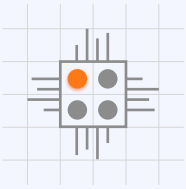
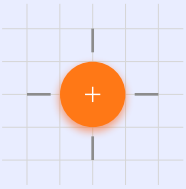
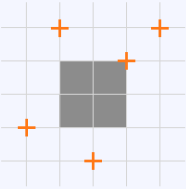
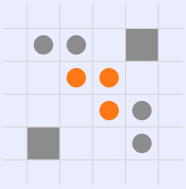
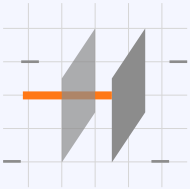
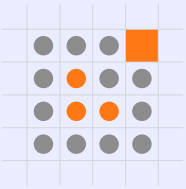
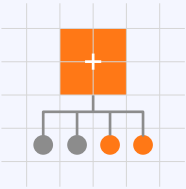
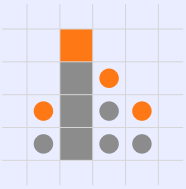
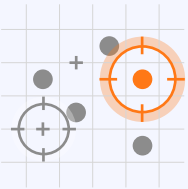
Cyberint利用专有威胁情报平台Argos™与经验丰富的威胁情报分析师的独特组合，提供一种全新的数字风险防护（DRP）方法，给出解决以下挑战的解决方案：

- **确定**应考虑**哪些相关威胁**，以设计有效的网络安全防御计划
- 向董事会和管理层**说明最新的网络风险状况**，并提供明确的行动计划
- **获取预测情报**，以在目标威胁出现之前确定对其进行缓解的意图、技术和工具
- **持续监控**网络犯罪分子可以利用的**数字风险敞口**
- 在**违约行为蔓延**到机构范围之外时**对其进行检测**
- **直观了解**网络之外不断发展的针对您的品牌和客户的**攻击**

CYBERINT解决的业务挑战：

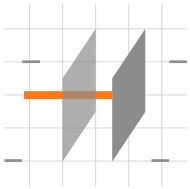
- 品牌保护
- 第3方网络风险
- 数字风险表面监控
- 欺诈
- 数字泄露检测
- 攻击软件检测
- 黑暗网络监控
- 威胁情报

CYBERINT提供

ARGOS™技术	托管服务
 威胁情报	 目标性监控
 黑暗网络监控	 虚拟人工情报
 风险表面映射	 深度调查
 取证画布	 威胁情境分析
 网络钓鱼检测与清除	

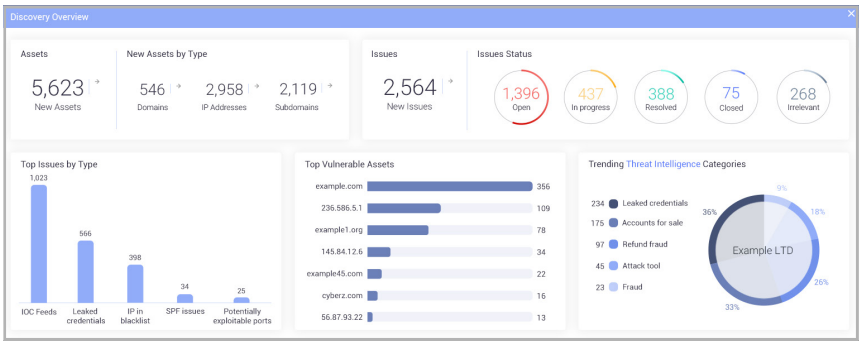
ARGOS™情报驱动的数字风险保护平台

Argos™是一个多租户SaaS平台，设有多个模块：

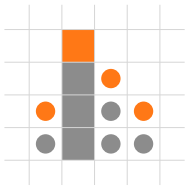


攻击表面映射

Argos™攻击表面映射可识别机构的数字足迹，并持续监控外围区域的资产，从而确保对所述资产的可见性并基于问题的严重程度给予优先解决，突出显示相关的威胁、漏洞和弱点。



Argos™数字风险保护平台，攻击表面监控

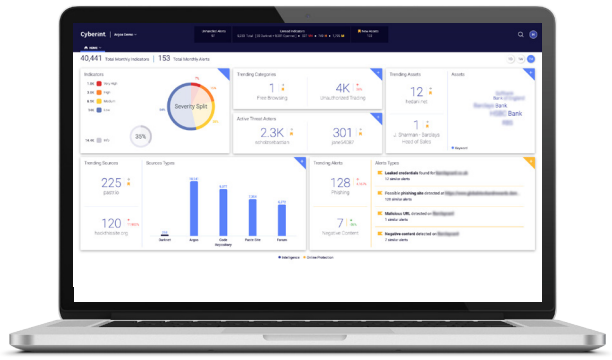


威胁情报的收集与分析

Cyberint对开放、深层和黑暗网络中成千上万个威胁源进行实时监控，从而每天可向Argos™的内部数据湖收集数百万个情报项目。

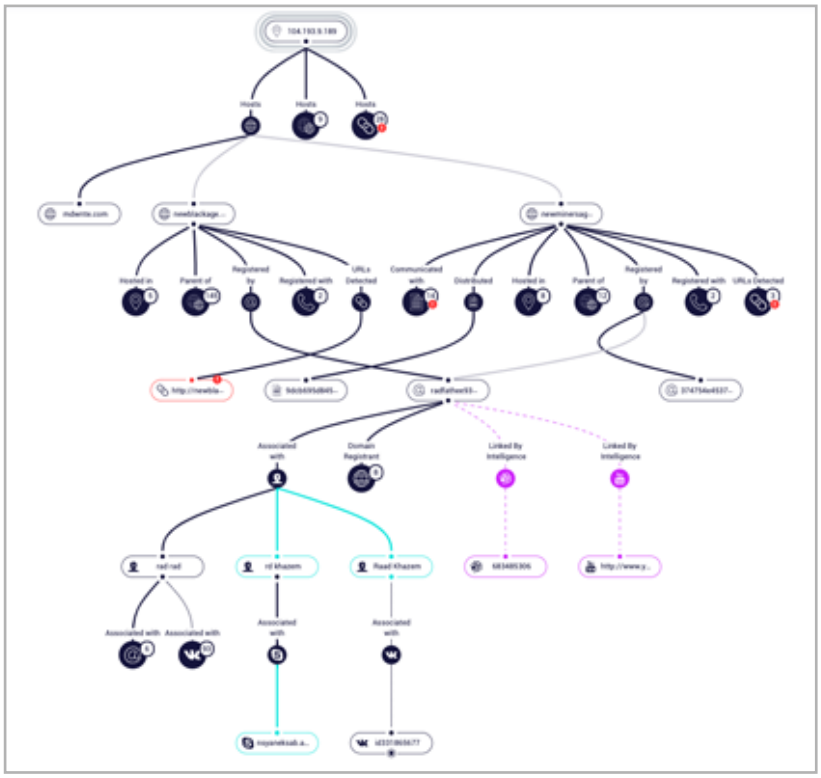
原始情报项目自动与机构的资产（IP、域、品牌、执行程序等）相关联，并根据特定用例进行分类：网络钓鱼、恶意软件活动、证书填充、数据泄露、欺诈活动等。此原始情报采用Cyberint专有的机器学习算法，根据潜在的风险和影响进行优先级排序，从而进行经济高效的智能分析。

自动和半自动分析引擎会生成可操作的情报警报，然后连同以下各项分发给安全团队：深入的分析、丰富的背景、对威胁源起方的分析等，从而使组织能够采取有效的措施。



Argos™数字风险保护平台

取证画布



Argos™数字风险保护平台，取证画布

Cyberint的取证画布模块可以识别和分析威胁源起方，并对他们使用的工具、策略、程序（TTP）进行深入调查。

取证画布用于丰富特定或多个IOC的背景，将多种服务整合于统一的调查平台，以支持各种类型的连接，包括Argos™威胁情报、WHOIS服务、被动DNS、社交发现、恶意代码检测等

主动网络钓鱼检测技术与清除

网络钓鱼仍是数字性机构的主要风险，结果导致账户受到攻击，致使客户流失，对品牌声誉产生负面影响。为应对这一挑战，Cyberint开发了网络钓鱼信标，这是一个专有模块，可以实时查看从机构网站内容中克隆的新建网络钓鱼站点，此为威胁源起方利用的一种有效技术。Cyberint的快速检测功能使我们能够代表机构清除钓鱼网站， 从而快速消除风险。

为您准备的好处

- **减少IT安全风险的阴影**
- **直观了解攻击表面**
- **缩短威胁停留时间**
- **扩展您的团队能力**
- **降低网络安全总拥有成本**

托管服务

适合您需求的定制网络情报服务

增强威胁情报团队

Cyberint提供一项托管数字风险保护计划，使您可以利用我们的Argos™平台及网络威胁分析师团队，从而提高任何CTI计划的质量和性能水平。

与Cyberint分析师团队的合作包括与专职分析师进行日常互动，而该分析师将成为您内部团队的成员。分析师根据其行业知识及对业务需求的深入了解进行配给。

Argos™公开的所有原始情报项目均利用从开放、深层和黑暗的网络中收集的大量数据进行认真验证、关联并归因于实际风险。

我们的分析师团队使用多种语言，因此可以使用各自的语言了解威胁源起方。此外，分析师对网络犯罪“术语”和文化的掌握使您可以识别、验证和缓解最可能会因攻击而产生的威胁。

Cyberint在研究、调查和威胁情报操作方面提供宝贵的人为因素。虚拟人工情报功能（即与威胁源起方的实时交互）可实现更深入的关联，此为有效缓解风险所必需。

CYBERINT研究

Cyberint的网络研究团队探索网络威胁情境的前沿情况，以保持趋势威胁的战略可见性。网络研究团队分析大量数据以创建战略威胁情报报告，从而使决策者能够确定有意义的趋势，获得针对其机构的数字风险的更广泛和更深入的认识。报告包括对当前行业风险、值得注意的威胁源起方、TTP分析结果等的定期分析。

CYBERINT 最新报告

菲律宾金融业
威胁情境报告

下载

REvil - 盗取、加密和拍卖
研究报告

下载

台湾具有针对性的勒索软件攻击
研究报告

下载

与CYBERINT威胁情报托管服务合作的好处

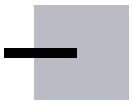
威胁检测
通过预测情报检测威胁

确定严重程度
确定威胁的严重程度并了解‘全局’

虚拟人工情报功能
直接与威胁源起方沟通，将其活动归因于具体行动，获得更多背景信息和情报

识别欺诈操作
识别并提供有关如何应对和缓解风险的可行性情报

实时网络钓鱼检测
实时网络钓鱼网站检测与清除操作



VIP威胁调查
监控高管人员的在线状态，以防止威胁源起方获取个人信息进行恶意使用

映射与监控
映射和监控机构的数字化存在状态，包括证书泄漏、数字漏洞和敏感文件泄漏

Gartner peerinsights™ 4.8 ★★★★★

我们客户的声音

> 托管服务在将调查结果转化为相关信息及针对我们业务的警报方面提供真正的价值。
>
> 大型美国零售商

> 您在使用*Cyberint*之前，实际上对谁试图攻击您的机构并未正确了解。
>
> 大型美国电子商务零售商

联系我们

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

美国
214 W 29th St.
纽约，10001
电话：+1-646-568-7813

以色列
17 Ha-Mefalsim St.
4951447 佩塔提克瓦
电话：+972-3-7286-777

英国
14 Grays Inn Rd., Holborn
WC1X 8HN，伦敦
电话：+44-203-514-1515

新加坡
135 Cecil St. #10-01 MYP
PLAZA 069536
电话：+65-3163-5760

拉丁美洲
巴拿马城
电话：+1-929-399-8495

Cyberint