

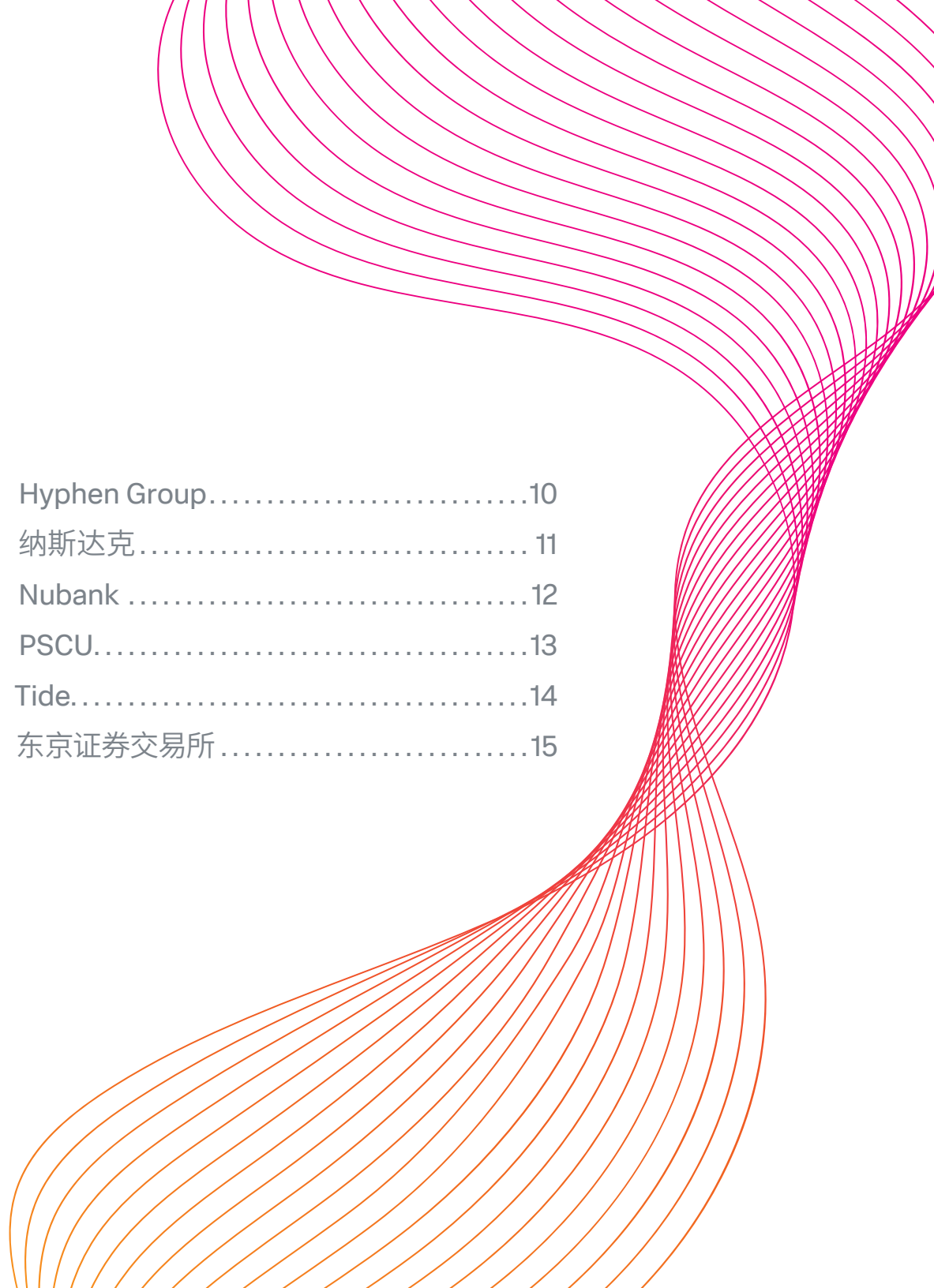
依靠 韧性

领先的**金融服务机构**如何建立安全的系统、
可靠的支付平台和消费者信任



目录

不小的变化.....	3	Hyphen Group.....	10
发挥作用的韧性	5	纳斯达克.....	11
2C2P	6	Nubank	12
Aflac	7	PSCU.....	13
au Kabucom.....	8	Tide.....	14
东亚银行	9	东京证券交易所.....	15



不小的变化

金融服务业至少占全球经济的 20%，是世界上最重要和最有影响力的行业之一。它也是转变最快的领域之一，也是不可预测的领域之一。

对于金融服务机构来说，唯一不变的是变化。随着客户期望、竞争、安全威胁和地缘政治趋势的变化，法规也在以极快的速度变化。虽然保持客户信任和保护敏感数据是金融公司的核心优先事项，但这项工作只会变得越来越困难。随着产品的扩展、平台的发展和客户接触点的增加，这些组织面临着越来越多的安全和性能违规风险，而一次停机都会带来高昂的代价。

Splunk **调查了**超过 2100 名各行业的安全、IT 和开发运维领导者，金融服务业成为停机成本最高的行业，每年高达 1.41 亿美元，比各行业的平均水平高出 5400 万美元。将这一惊人的价格与停机导致的声誉损失和监管后果结合起来，会给任何金融机构带来潜在的灾难性后果。

因此，在一个不断变化的行业中，您如何先于重大问题采取行动以确保正常运行时间？您如何挫败坏人来保护您和客户的数据？您如何转向满足下一个监管要求？您如何跟上时代的发展？



投资于数字韧性

为了确保系统全天候保持安全可靠，领先的金融公司正在将数字韧性作为重中之重，他们正在使用 Splunk 的统一安全性和可观察性平台来实现这一目标。

从 **Aflac** 在短短六个月内阻止了 200 多万次威胁，到 **纳斯达克** 调整其业务模式以加速创新，这些有远见的组织正在使用 Splunk 来降低风险 - 从维持运营和检测金融犯罪到增强安全态势和提供实时合规报告。

通过依靠 Splunk 平台来了解其复杂环境的各个方面，领先的金融公司正在其组织中释放强大的成果，包括确保法规遵从性 (**2C2P**)、将威胁响应速度提高 5 倍 (**Tide**) 以及加快新产品上市时间 (**Nubank**)。无论未来如何，在构建数字韧性基础的过程中，这些组织都为自己的持续成功做好了准备。

金融服务行业可能不可预测，但有了 Splunk，您将准备好迎接下一个挑战。



Splunk 是我们云之旅的战略合作伙伴。Splunk 平台是了解我们客户的业务进展以及他们如何使用我们产品的关键部分，因此我们可以更快地将创新交给他们。”

- Brad Peterson, 纳斯达克执行副总裁兼首席技术官/
首席信息官

发挥作用的韧性

全球 80% 的大型银行、支付公司、市场运营商和监管机构都是 Splunk 的客户, 原因有很多。

在接下来的几页中, 我们将介绍一些精选的金融服务机构, 它们正在使用 Splunk 来保持其系统的安全性和可靠性, 同时更好地为客户服务。



2C2P 保护全球支付并确保合规性

在当今快节奏的世界中，敏捷性的重要性毋庸置疑，2C2P 提供了一个支付平台，为全球企业提供东南亚地区在线、移动和线下渠道的安全支付。为了确保为客户提供最佳的灵活性，2C2P 的强大平台接受 250 多种支付方式，并运营一个跨越 400000 个物理接触点的替代支付网络。

因为要管理如此多的复杂性，2C2P 面临着越来越多的本地和国际合规性挑战。“我们必须收集和存储 90 天的日志数据，用于事件调查，以履行网络安全保护义务。”2C2P 的 IT 基础设施和安全高级经理 Kavin Tantipongsakul 说。“但这变得非常困难，因为不同的来源以惊人的速度生成不同类型的日志。” 最重要

通过转向 Splunk 平台，2C2P 实现了其目标，即提高工作效率、维护法规合规性、应对网络威胁和数据泄露，同时实时监控运行状况。



的是，该公司还必须遵守《个人数据保护法》，这是东南亚一部通用的数据保护法，用于管理个人数据的收集、使用、披露和传输。

为了简化流程，2C2P 转为求助 Splunk，以获得对其 AWS 云环境、分布式系统和虚拟专用网络中运营的全栈可见性，这有助于显著简化法规遵从性。“以前，当审计员提出请求时，我们必须手动从日志文件中收集数据，需要几天或一周的时间才能做出响应。”Tantipongsakul 说。有了 Splunk，这种收集和分析现在已然成为一个自动过程，只需几分钟便可完成。

Splunk 平台还帮助该公司查明和调查新的威胁，同时从单一控制台监控其分布式 IT 系统的运行状况。Tantipongsakul 说：“我们对 Splunk 充满信心，不仅因为它在市场上的领先地位，还因为我们对该平台的灵活性有着第一手的经验。”



由于 Splunk，我们的服务平台现在运行得更加安全可靠，这增加了我们客户的信心和满意度。这给了我们前所未有的商业价值。”

- Kavin Tantipongsakul, 2C2P IT 基础设施和安全高级经理



Aflac 加强威胁情报, 在六个月内便阻止了 200 万次威胁

作为美国领先的自愿保险提供商, Aflac 深知在灾难面前保持韧性的重要性。随着 Aflac 进入新市场并提供新服务, 该公司必须不断调整其安全计划, 以应对不断变化的威胁形势。由于这些威胁在数量和速度上的增长, Aflac 转向 Splunk 来保护其客户、近 10000 名员工和品牌声誉。

第一项议程: 加强 Aflac 的威胁情报平台, 以更快地检测和应对攻击。“我们的概念验证实际上是将 Splunk Enterprise Security [ES] 用于我们的威胁搜索用例, 其价值实现时间远远超出了我们的预期。”Aflac 的安全运营和威胁管理副总裁 D.J. Goldsworthy 表示。

凭借这一经过验证的价值, Aflac 采用了 Splunk ES 和 Splunk 用户行为分析 (UBA) 作为其 SOC 的核心。现在, 由大约 40 人组成的六个团队依靠 Splunk 平台来管理广泛的安全用例, 包括威胁搜寻、威胁情报、安全运营、事件响应、应用安全、安全管理和欺诈。“我们计算出, 在进行报告方面, 我们每个月节省了 40 多个小时, 在过去, 这些报告需要手动完成, 而现在已经实现了全



我们能够在很短的时间内凭借非凡的表现来检测高级威胁。Splunk 让我们变得更加灵活, 使我们能够迅速向所有利益相关方展示价值。”

- D.J. Goldsworthy, Aflac 安全运营和威胁管理副总裁

自动。”Goldsworthy 说。“通过 Splunk, 我们看到了投资的直接回报。”

Aflac 在五个月内部署了由 Splunk 支持的新威胁情报系统, 比计划提前了整整一个月。该系统提供战术和战略功能, 增加自动化以提高每日威胁数据馈送的效率, 从而节省时间并减少错误。在六个月的时间内, Aflac 阻止了 200 多万个安全威胁, 误报不到 12 个。

这种安全级别意味着, Aflac 可以持续保护投保人的敏感信息, 同时主动让公司做好防御下一代威胁的准备。

Splunk 是 Aflac SOC 的核心, 六个团队 (约 40 人) 依靠该平台来增强安全性、提高日常效率、减少错误并在威胁不断加剧的世界中提高韧性。



在六个月内
阻止了
200 万次
安全威胁

通过取代手动
流程, 每月节
省 40 小时

2 周即可
实现企业就
绪型实施

au Kabucom 自动执行 DevSecOps, 以应对网络安全挑战

作为三菱 UFJ 金融集团 (MUFG) 的一部分, au Kabucom Securities 为日本超过 110 万客户提供在线经纪服务。为了实现自动化 DevSecOps 的目标, 该公司需要一种方法来防范潜在的破坏性网络安全威胁, 同时经济高效地可视化和分析其所有数据。

“尽管我们有一个网络安全任务组来监控风险, 但 2017 年的 DDoS 爆发表明, 整个公司需要更强的防御和更大的信息透明度。”au Kabucom Securities 系统开发部系统总经理助理兼 IT 战略组副总经理 Yoichi Ishikawa 表示。“在我们能够通过将安全性纳入开发和运营来采用 DevSecOps 之前, 我们必须首先分析我们一直在生成但没有正确利用的暗数据。”

凭借增强的可见性、高级预测分析以及简化的威胁调查和自动响应, au Kabucom Securities 现在可以轻松应对安全挑战。

自动完成时间密集型活动以减轻团队压力

通过更快地响应关键问题来提供更好的客户体验

为更好的分析和决策制定提供更有价值的

借助 Splunk 平台, au Kabucom 团队现在可以在更快地调查和响应关键问题的同时防止威胁。“我们作为在线交易平台的新地位意味着, 数据管理比以往任何时候都更加重要。”Ishikawa 说。“凭借在金融界的显赫履历, Splunk 将帮助我们从未开发的数据资产中获取最大价值, 从而不断提升竞争力。”

通过识别可疑行为、触发警报和分析日志以自动采取纠正措施, Splunk 平台帮助 au Kabucom Securities 实现了完全自动化 DevSecOps 的目标。该团队现在有效填补了应用程序开发和操作中的安全空白, 在推出新配置之前, 获得了所需的信心和韧性。



Splunk 使我们能够充分利用数据来发展我们的安全计划, 并保持对网络安全挑战的韧性。

— Yoichi Ishikawa, au Kabucom Securities Co., Ltd 系统开发部系统总经理助理兼 IT 战略组副总经理

东亚银行确保数字韧性的全球安全管理

东亚银行有限公司 (BEA) 是香港主要的上市金融服务集团, 拥有 100 多年历史, 通过遍布全球的 150 多个网点提供全面的金融服务。

十多年来, BEA 一直依靠 Splunk Enterprise Security 来监控其内部基础设施, 并再次与 Splunk 合作, 在其所有国际分支机构中实现安全信息和事件管理 (SIEM) 的标准化。这让东亚银行成为香港首间使用基于云的 SIEM 的银行机构, 并在此过程中获得了对监察业建环境的全面可见性。

凭借触手可及的全球可见性, BEA 的香港 IT 团队可以从任何地方实时获取安全数据。相反, 此前每个海外网点的团队都需要建立自己的 SIEM 系统进行安全监控和分析, 如果有任何关于安

Splunk 从三个方面提升东亚银行的数字韧性, 包括实时故障排除、紧贴威胁情报, 以及在云环境中保持灵活性。所有这些都为东亚银行的客户打造更好的服务体验。

设置国内 SIEM
只需 1 个月,
而之前需要
几个月

全面掌握
分布式国际
环境

更快的问题调
查和响应得益
于自动化

全性的问题, 都要特别联络香港总部。现在, 总部可以轻松地与每家子公司共享 Splunk 仪表盘。这使所有团队都能全面了解其安全状况, 帮助他们跟上不断变化的威胁形势, 并在小麻烦变成大问题之前主动解决它们。

借助 Splunk SOAR, BEA 的安全分析师可以轻松应对每个警报, 并通过实时态势感知和及时的威胁情报主动避免潜在问题。分析人员无需再处理重复的手动工作流程, 能够腾出时间去实现更具策略意义的计划, 专注实施关键任务。

“数字韧性是我们金融科技战略不可或缺的一部分。”东亚银行信息技术部和金融科技发展部主管 Stephen Leung 表示。我们致力提升网络安全、推动创新文化, 在日新月异的数字世界中茁壮成长, 促进金融科技的蓬勃发展。Splunk 使我们在自动化的领域上迈进一大步, 实现恰当的系统监控与修补程式部署, 同时优化安全程序的编排, 简化威胁检测与响应。”



Splunk 使我们能够走在数字化转型趋势的前面, 而不仅仅是跟上它们。”

— Stephen Leung, 东亚银行有限公司信息技术部及金融科技发展部主管

Hyphen Group 部署基础设施的速度提高了 8 倍，可以更快地发布新产品和服务

Hyphen Group 是东南亚领先的金融科技公司，希望通过提升其开发运维渠道来弥合软件开发和 IT 运营之间的差距。特别是在该集团收购个人金融社区平台“Seedly”之后，它不得不生产更多代码并部署额外的基础设施来应对新产品的推出。

但是，由于缺乏开发运维可见性，使得诊断和解决 Hyphen Group 复杂环境中的问题变得越来越困难。“我的工程主管不得不在凌晨两三点来上班，因为他们是唯一知道如何挖掘错误日志的人。”Hyphen Group 首席技术官 Shannon Murphy 表示。这些复杂性意味着，对关键问题（例如主要基础设施中断）进行故障排除通常需要几个小时。

借助 Splunk 可观察性云，Hyphen Group 能够主动发现整个前端和后端堆栈中的问题，同时改进定向故障排除，使 Murphy 和他的团队能够在不到三分钟的时间内，生成用于解决问题的自动脚本。通过单一平台全面了解 IT 环境，也有助于公司内从工程设计到基础设施运营的各个团队顺利合作。这些新发现的效

率为战略性业务计划（例如更新现有软件和开发新产品）腾出了宝贵的时间。

Hyphen Group 的新可观察性能力帮助基础设施部署速度提高了八倍。例如，该公司仅用 45 天就推出了新的保险平台，这在以前可能需要一整年才能完成。Hyphen Group 的客户也受益于更长的正常运行时间，让他们高枕无忧。当客户遇到孤立的错误时，例如 Hyphen Group 的内容管理平台上的网页中断，Hyphen 团队使用 Splunk 可观察性云在后台识别和分析问题，然后使用这些发现自动解决未来的类似问题。

以前，诊断和解决 Hyphen Group 复杂环境中的问题（例如重大停机）需要几个小时，而现在，该公司可以更快地修复问题和部署基础设施，从而延长正常运行时间，加快上市速度，并为客户带来更好的结果。



Splunk 有助于简化问题解决流程，并使我们的开发人员和基础设施运营团队能够专注于为业务增加价值。”

- Shannon Murphy, Hyphen Group 首席技术官

解决问题
只需几分
钟，而不是几
小时

基础设施部署
速度提高
8 倍

以前所未有的效率发布 275 个
软件更新

纳斯达克看好未来市场生态系统的创新

1971 年，纳斯达克作为世界上第一个电子交易所跃上交易舞台。在接下来的几年里，纳斯达克成为了创新的象征 - 这一声誉吸引了全球市值最大的四家公司，它们都在纳斯达克上市。

纳斯达克在 21 世纪初就开始了云转型，而彼时，大多数组织尚未考虑向云迁移。随着业务的变化，纳斯达克不得不重新思考其一些基础流程，转向 DevOps 运营模式，以提供创新，例如纳斯达克云数据服务，该服务通过一套 API 为客户提供实时交易数据。虽然纳斯达克已经依赖 Splunk 平台进行 IT 运营和安全保护，但该企业还是求助于 Splunk，在整个云之旅中保持韧性，在整个过程中保持对其不断发展的混合环境的可见性。

凭借 Splunk 平台，纳斯达克确保了其主要交易平台和 3900 多家纳斯达克上市公司的可靠性，同时发布了重新定义未来市场生态系统的创新解决方案。

安全转移到基于开发运维和 SaaS 的运营模式，**加快创新速度**

加快新产品和解决方案的**上市时间**

通过统一不同系统的数据，**迅速做出更明智的决策**

在疫情期间，这种可见性尤为难能可贵，因为查看、理解和处理实时客户数据的能力变得更加重要。“新冠肺炎在我们的市场创造了令人难以置信的参与度，无论是在交易量还是波动性方面。即使我们 98% 的员工现在都在远程工作，我们也需要知道我们的环境中每分钟都在发生什么。”纳斯达克首席技术官兼首席信息官 Brad Peterson 说。“Splunk 最具战略意义的用途是让我们实时了解历史交易量期间我们的市场情况。”

凭借这些见解，纳斯达克的领导者继续制定产品战略，调整业务模式，并提供重新定义未来市场生态系统的创新解决方案。“我们永远不会有一套同质的基础设施、应用程序和操作系统。”Peterson 说。“因此，我们需要一个解决方案，让我们能够在异构环境中做我们最擅长的事情 — 构建特定于资本市场、市场数据、交易和交易后数据的应用程序。这是 Splunk 的专长。”



Splunk 是我们云之旅的战略合作伙伴。Splunk 平台是了解我们客户的业务进展以及他们如何使用我们产品的关键部分，因此我们可以更快地将创新交给他们。”

- Brad Peterson, 纳斯达克执行副总裁兼首席技术官/首席信息官



Nubank 扩大了运营规模, 同时更快地推出产品并简化数字银行业务

Nubank 作为一家 100% 的数字银行, 允许客户只需使用一款应用程序来管理他们的财务, 无需分行或账户费用。从信用卡和数字账户到保险单和非接触式支付, Nubank 的产品对客户的日常生活至关重要。但这些高风险也意味着 Nubank 的数字平台必须安全无虞, 并且全天候可用。

虽然 Nubank 基于微服务的应用程序有助于减少代码基数, 使工程师更加敏捷, 但它们也增加了系统的复杂性。为了支持快速增长, 同时确保安全性和韧性, 工程师需要了解这一复杂的环境。借助 Splunk Cloud Platform, Nubank 获得了其系统的端到端视图, 允许工程、安全和合规团队主动监控数据、更高效地协作和更快地解决问题。

“Splunk 对我们的可观察性战略至关重要。”Nubank 的高级工程总监 Cat Swetel 说。“有了 Splunk, 我们说的是同一种语言。当我们想调查一些事情时, 我们会去同一个地方, 所以我们不必投入大量额外的精力, 互相学习我们使用的工具。Splunk Cloud Platform 为我们提供了灵活性和敏捷性, 使我们能够快速响应客户需求。”



Splunk 平台有助于保持我们的系统正常运行, 更加安全和合规, 这为 Nubank 提供了拨号音, 当客户需要我们时, 我们始终在线。”

- Matt Swann, Nubank 首席技术官

在短短三年内, Nubank 已经将其产品组合从两种扩展到 20 多种, 帮助客户轻松地进行网上银行业务。随着 Nubank 的持续增长, Splunk 在帮助该数字银行扩大客户获取和收入规模, 同时控制成本方面发挥着举足轻重的作用。“Splunk 是 Nubank 平台的基础构件。”Swann 说。“无论是服务记录、安全性还是合规性, 我们都使用 Splunk 来捕获和维护信息, 通过这些信息提供的见解, 我们可以了解如何运营业务, 以及我们需要为客户提供什么。”



通过 Splunk, Nubank 安全地扩展了其运营, 同时使系统更具韧性, 更快地推出新产品, 并简化了数百万客户的数字银行业务。

通过端到端的系统可见性**加快上市时间**

更强的创新和扩展能力 - 三年内**从两种产品增加到 20 多种产品**

通过**统一安全和工程团队, 更快地解决问题**并简化协作

PSCU 将 MTTA 速度提高了 99%，以更快地解决问题并防止故障

PSCU 是美国首屈一指的支付信用联盟服务组织。PSCU 充分利用数字技术的优势，支持 1500 多家信用合作社取得成功，每年的交易量超过 38 亿笔。

为了更好地使其信用合作社与银行竞争，PSCU 旨在改善关键的 IT 性能指标，例如平均确认时间 (MTTA)，这是一种在收到警报时实际上表示“我正在处理”的信号。MTTA 是减少停机时间和建立韧性系统的关键指标，因为它触发了事件响应，从而降低了平均修复时间 (MTTR)。

“我们的服务和产品能够为我们的信用合作社所有者所用，这一点至关重要。”PSCU 的 IT 运营经理 Earl Diem 说。PSCU 已经是 Splunk 基本用例的长期客户，例如安全监控和支付卡行业 (PCI) 合规性，并通过 Splunk On-Call 解决了 MTTA、MTTR 和问责制

为了完成让客户满意的使命，PSCU 依靠 Splunk 来确保 PCI 合规性、更快地检测错误和解决事件，从而实现更快的创新和无缝性能。

MTTA 缩短 99% — 从四个小时缩短到不到两分钟

通过改进的协作和企业功能完成 **38 亿笔交易**

1500 多家信用合作社通过移动监控和实时警报获得支持

方面的挑战。现在，随时待命的团队可以通过自动化和深入的事件管理路由、协作和审查来更快地发现和解决问题。

在使用 Splunk On-Call 一年后，PSCU 将 MTTA 从 4 小时减少到 20 分钟。两年后，MTTA 下降到两分钟

以内。“Splunk On-Call 通过一个工具将所有经理聚集在一起。”Diem 说。“我们知道我们在做什么，我们都使用相同的上报计划。它推动了问责制。”现在，质量保证和开发运维团队也在使用 Splunk On-Call，帮助团队快速检测新软件版本中的错误，同时在性能下降演变为故障之前进行检测。

通过利用 Splunk 平台的强大功能，PSCU 更好地完成了让客户满意的使命。“无论你做什么，都会经历失败。”Diem 说。“越早知道，越早修复，就能更好地保护你的用户体验。”



使用 Splunk On-Call 的 12 个月中，我们的平均确认时间从 4 小时减少到 20 分钟。现在，我们的业务已经开通三年，我们的响应时间不到两分钟。”

— Earl Diem, PSCU IT 运维经理



通过自动化, Tide 将检测和响应威胁的速度提高了 5 倍

Tide 为中小型企业提供了一种简单、集中的开户、存取资金和管理现金流的方式。由于 Tide 的移动优先模式, 客户可以从任何地方访问他们的账户, 这样他们就可以“回去做他们喜欢的事情”。

鉴于公司处理的财务数据的敏感性, 确保交易安全对于赢得和留住客户至关重要。随着其客户数量迅速增长到 470000 多家 (并且还在增加), Tide 需要一种方法来帮助其威胁检测和响应 (TDR) 团队扩大规模, 更快地响应事件, 以确保客户数据的安全。

在 Splunk 的帮助下, Tide 的六人 TDR 团队始终领先于威胁, 轻松地与其他技术团队共享有关系统安全的信息。“有了 Splunk SOAR, 可以轻松培训我们的工程师, 并招募他们加入 TDR 团

借助 Splunk 平台的 SIEM 和 SOAR 功能, Tide 团队可以快速发现并减少任何可疑活动, 以保护客户数据免受不断变化的威胁。

高达 **95%** 的事件响应自动化

响应安全威胁只需几分钟, 而以前需要几个小时

借助 SOAR, 响应速度提高了 **5 倍**

队。”Tide 产品安全工程师 Devyani Vij 表示。“这意味着我们正在有效扩大保护我们基础设施的人员数量, 并为我们的数据安全提供更高水平的保证。”

与其他金融机构一样, Tide 必须在任何可疑活动或风险行为引发问题之前识别出它们, 无论是有意还是无意。“Splunk SOAR 帮助我们的工程师识别不同类型的威胁和漏洞, 因此我们可以尽快发现它们, 并专注于如何减轻它们。”Vij 说。

当事件发生时, 团队使用 Splunk SOAR 轻松检测并做出响应。在采用 Splunk 之前, 团队必须手动调查警报, 这意味着一个事件可能需要几个小时来调查, 并且需要团队成员在清除错误警报并采取行动之前使用多种工具。现在, 可以快速而轻松地完成调查, Tide 能够自动处理高达 95% 的警报, 从而提高效率。Chuhan 说, “通常只需几分钟就可以解决问题, 而不是花费数小时调查事件。”



我们现在可以看到所有的工具和资源, 无论是自主开发的还是第三方应用程序。这些信息提高了安全意识, 并为我们在整个企业中采取的行动提供了信息。”

- Ojasvi Chauhan, Tide 威胁检测工程师,



东京证券交易所轻松掌控混合云复杂性



东京证券交易所 (TSE) 由日本交易所集团 (JPX) 所有, 除了发布股票价格和报价之外, 还提供证券和衍生产品交易的市场设施。作为日本最大的证券交易所, TSE 致力于在其运行的每个应用程序上提供卓越的用户体验。

但是, 当 JPX 不得不将大约 30 个内部和外部信息系统迁移到云中时, TSE 的混合云环境迅速变得极为复杂。虽然 TSE 多年来一直依赖 Splunk 来管理其交易和核心系统, 但 Splunk 综合监控功能开启了新的机遇, 增强了前端监控和自动化运营, 帮助 TSE 在云时代保持韧性。

“作为一个基于 SaaS 的解决方案, Splunk 综合监控允许我们从小规模起步, 快速发展, 对我们当前的系统没有任何改变。”Okada 说。“通过监控 Web 服务、应用程序运行状态、浏览器性能和用户响应时间, Splunk 使我们能够高效、经济地管理云环境中的所有系统。”



Splunk 综合监控正是我们实现无缝且经济高效的前端监控所需要的。我们期待通过 Splunk, 战略性地推进整个集团的 IT 运营。”

- Akimitsu Okada, 东京证券交易所应用集团总经理。

凭借对所有信息系统的全面了解, TSE 现在可以主动检测故障点, 并快速解决正常运行时间和性能问题。通过使用 Splunk 从前端应用程序自动收集数据, 该团队可以轻松识别以前难以发现和修复的公共云问题, 帮助 TSE 提供流畅的用户体验。“只需添加云服务的 URL, 我们就可以立即查看网站显示性能。”Okada 说。“我们可以在控制台上发现公共云故障, 找出它是否影响基础设施的任何部分, 并快速隔离问题。”

为了在不断发展的网络世界中保持繁荣, TSE 计划将 Splunk 综合监控的使用“横向”扩展到其他类型的系统, 并“纵向”探索更深入的功能。随着 TSE 朝着 JPX 提高业务灵活性的愿景大步前进, Splunk 将继续在现在和未来的成功中发挥关键作用。

东京证券交易所通过使用 Splunk 开启新机遇、增强前端监控和自动化运营, 在云时代保持韧性。



了解 Splunk 如何提高金融服务机构的韧性。

了解更多



Splunk, Splunk> 和 Turn Data Into Doing 是 Splunk Inc. 在美国和其他国家/地区的商标和注册商标。所有其他品牌名称、产品名称或商标均属于其各自所有者。©2023 Splunk Inc.保留所有权利。