TATA COMMUNICATIONS

TATA

“HOW CAN WE SAFELY STEM THE EVER-RISING CYBERATTACK TIDE?” ENQUIRED MAJOR FINANCIAL SERVICES FIRM.

TATA COMMUNICATIONS SIEM SOLUTION AUTOMATED SECURITY MONITORING AND MANAGEMENT.

> **“Cybersecurity is a fast-changing environment. Lack of comprehensive and up-to-date oversight led to sleepless nights. Now, Tata Communications SIEM means we’re always on top of the situation. That protects our investors, our people and our corporate reputation.”**

Spokesperson for Major Financial Services Firm

CHALLENGE

To replace a mixture of unintegrated security point products, this major financial services firm was looking for a cybersecurity solution to collect and action event data company-wide for vulnerability awareness and visibility of normal and aberrant behaviour.

SOLUTION

Tata Communications SIEM (security information and event management) was chosen as an on-premise system that uses industry-leading technology to aggregate every security-related event across the financial services firm’s IT estate, including remote sites and mobile users.

RESULTS

The Tata Communications SIEM platform monitors some 300 devices. At peak traffic, it inspects around 2,000 security-related events every second. Those events are automatically stored, sifted and compared for evidence of threat patterns or breaches of security policy.

1 million cyber events
monitored daily

Up to 60 alarms
dealt with each day

300 devices
supervised

Firefighting consigned
to history

PREPAREDNESS PARAMOUNT FOR PRIME CYBERATTACK TARGETS

“We conducted a detailed market evaluation of cybersecurity solutions. Tata Communications was chosen based on a trusted relationship and their understanding of our market dynamics. The company’s stability was another significant factor. We are confident they’ll be available anytime we need them.”

Spokesperson for Major Financial Services Firm

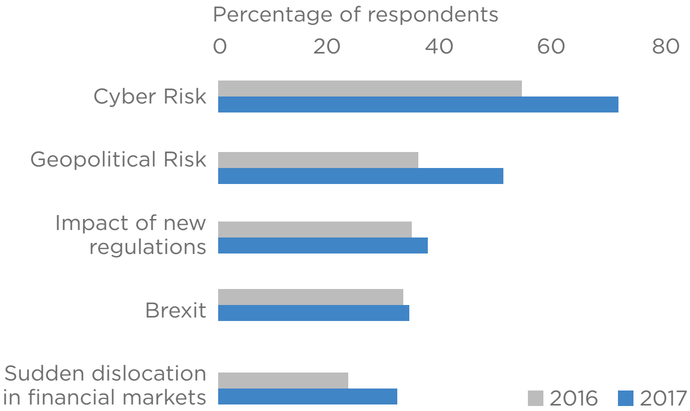
CORPORATE REPUTATION CANNOT BE A CASUALTY

Investors’ safety comes first

Banks are prime cyberattack targets. That’s no secret. Corporate reputations can be won or lost on institutions’ preparedness to combat professional hackers and other malcontents. That’s why on behalf of investors, with billions of dollars-worth of assets under its custody, this major financial services firm must always stay several steps ahead of digital criminals. Nothing less will do.

Assuring vulnerability awareness

In need of a complete cybersecurity overhaul – to replace a mixture of unintegrated point products – the major financial services firm was looking for a solution to collect and action security-related incident data on a company-wide basis. This would not only provide vulnerability awareness, including visibility of normal and aberrant end-user behaviour, but also bring external intelligence to bear on a database of extraordinary cyber events as they occurred.



IMF 2017 survey of rising risks to financial institutions’ stability

Source: https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx

✓ Trusted relationship with industry understanding assures value

THE MOST VALUABLE OUTPUT: ACTIONABLE INTELLIGENCE

“The Tata Communications SIEM solution helps us deal with a vast range of attack patterns and vectors. Among others these range from blacklisted domains and IPs, and communication over vulnerable ports – to signature, authentication and brute-force attacks. On average up to 60 alarms are generated daily, but the SIEM solution keeps us safe.”

Spokesperson for Major Financial Services Firm

SECURITY OPERATIONS CENTRE KEEPS WATCH AROUND THE CLOCK

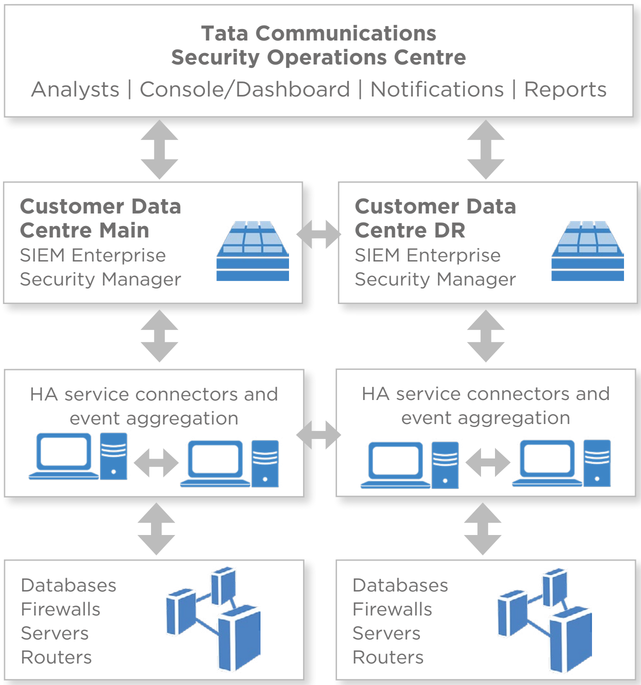
Guaranteed up to date

The major financial services firm chose an on-premise Tata Communication SIEM monitoring and application management service. Placed on the customer’s sites, this solution benefits from remote monitoring managed from the TATA Communications SoC (security operations centre). To enhance the company’s security posture, new use cases are regularly proposed and deployed based on upcoming threats.

Securing people, processes and technologies

Providing 24/7 monitoring of the financial firm’s cybersecurity, the Tata Communications global SoC offers immediate alerts for urgent matters. Meanwhile, a regular meeting deals with longer-term issues such as baselining and user behaviour profiling.

For situational awareness, the SoC tracks known threat conditions and analyses security data in real time for new threats. Assuring the cybersecurity of people, processes and technologies under an overarching security policy, fast responses are provided. This enables detection of and response to cyberthreats in real time before serious damage can be done. The SoC also supervises performance against SLAs, where exceeding the target is the norm.


Tata Communications
Security Operations Centre
Analysts | Console/Dashboard | Notifications | Reports
Customer Data Centre Main
SIEM Enterprise Security Manager
Customer Data Centre DR
SIEM Enterprise Security Manager
HA service connectors and event aggregation
HA service connectors and event aggregation
Databases
Firewalls
Servers
Routers
Databases
Firewalls
Servers
Routers

Tata Communications on-premise SIEM system logical architecture

☑ **The SoC enables ultra-fast detection speed and false positives elimination**

PRECISE PINPOINTING AND IMMEDIATE ALERTS

“With SIEM, security scares are relentlessly managed and mitigated. That means one of the most significant results is we’ve stopped firefighting.”

Spokesperson for Major Financial Services Firm

Real-time quarantine action

The Tata Communications SIEM platform monitors some 300 devices including servers, network components, firewalls and desktops. At peak traffic, it inspects around 2,000 security-related events every second, equating to as many as one million events per day.

Those events – be they internally or externally oriented – are automatically stored, sifted and compared for evidence of threat patterns or breaches of security policy. A severe threat’s location is precisely pinpointed, and real-time quarantine action taken to stop it in its tracks.

- Remote on-premise situation monitoring by Tata Communications SoC
- Event patterns analysed for emerging threat signatures
- Serious damage anticipated and avoided
- Oversight of security policy breaches

EXPLORE OTHER WAYS WE CAN HELP

LEARN ABOUT
Tata Communications SIEM

SEE
Other Tata Communications case studies like this

DISCOVER
The Tata Communications Spotlight Programme

SOCIALISE
Follow us on leading social networks. Keep up with business and technology news and views. Join in the conversation.