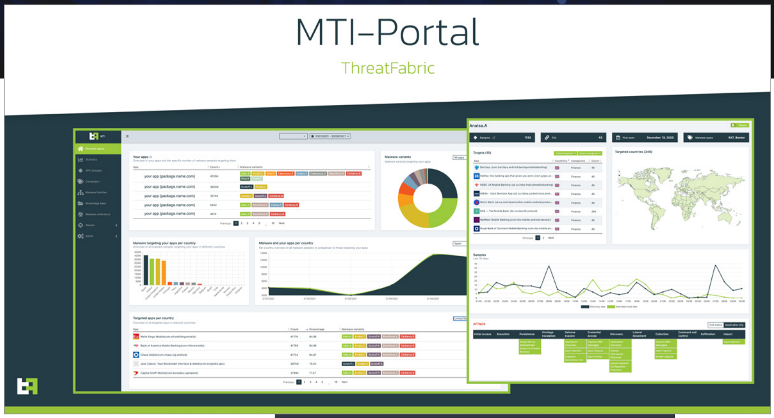
THREATQUOTIENT™

THREAT FABRIC

THREATQUOTIENT AND THREATFABRIC

Technology Segment: Intel Feeds



Threat actors motivated by financial gain always follow the money and have certainly followed the massive shift to mobile banking. Mobile threats are in constant evolution and many financial institutions have already suffered from mobile-based fraud by malware. By utilizing ThreatFabric's Intelligence for Mobile Banking and the ThreatQuotient platform, customers gain global visibility on the mobile threat landscape and the ability to monitor malware campaigns targeting mobile banking apps in real-time.

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ data-driven security operations platform is both open and extensible, supporting the integration of disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

MTI (MOBILE THREAT INTELLIGENCE) BY THREATFABRIC

Threat Fabric's MTI (Mobile Threat Intelligence) feed provides global visibility and context on the mobile banking threat landscape. It is the threat intelligence solution to use to protect personal data, customers and brand from financially motivated threat actors. It includes the strategic overview of threats and context as well as all relevant technical indicators.

With ThreatFabric MTI Feed, customers can gain global visibility on the mobile threat landscape and monitor malware campaigns targeting their mobile banking apps in real-time.

INTEGRATION HIGHLIGHTS

Get started immediately with a real-time and continuous feed of actionable indicators

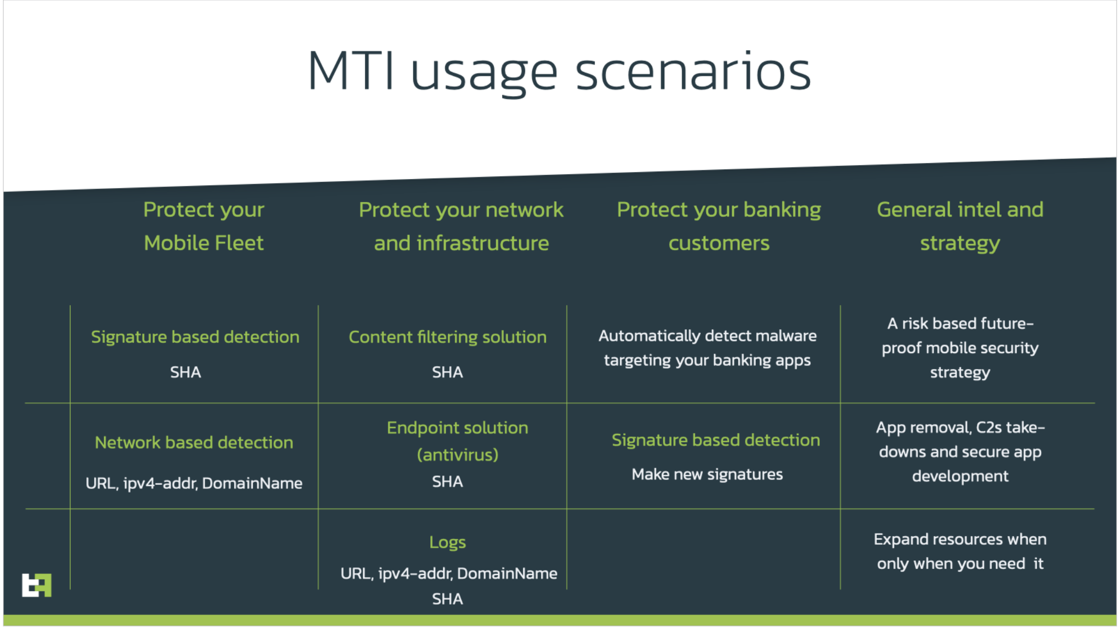
Continuous operational intelligence, allowing you to be preventive instead of reactive

Expand your resources during investigations with our experts when needed

INTEGRATION USE CASES

The Integration supports a variety of use cases such as:

- **Protect your banking customers:** If you perform in-depth research on the relevant malware samples, you can grow your intelligence capability and build your own detection rules to detect malware on the endpoints.
- **Protect your network & infrastructure:** If you have a Firewall, filtering proxy, IDS or IPS solution, you can can use the fields which contain "URL", "ipv4-addr" or "DomainName" in order to detect and block possible infection campaigns.
- **Protect your mobile fleet:** If you have your own mobile fleet and manage it from a central tool (such as MDM) and if you have a signature-based detection solution deployed, you can use all the information in the fields which contain "Hashes" in order to detect the malware instances.



MTI usage scenarios

Protect your Mobile Fleet	Protect your network and infrastructure	Protect your banking customers	General intel and strategy
Signature based detection SHA	Content filtering solution SHA	Automatically detect malware targeting your banking apps	A risk based future-proof mobile security strategy
Network based detection URL, ipv4-addr, DomainName	Endpoint solution (antivirus) SHA	Signature based detection Make new signatures	App removal, C2s take-downs and secure app development
	Logs URL, ipv4-addr, DomainName SHA		Expand resources when only when you need it

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage, vulnerability prioritization and threat intelligence management. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.

For more information, visit www.threatquotient.com.

ABOUT THREATFABRIC

ThreatFabric makes it easier than it has ever been to run a secure mobile payments business. With the most advanced threat intelligence for mobile banking, financial institutions can build a risk-based mobile security strategy and use this unique knowledge to detect fraud-by-malware on the mobile devices of customers in real-time.

Together with our customers and partners, we are building an easy-to-access information system to tackle the ever growing threat of mobile malware targeting the financial sector.

For more information, visit www.threatfabric.com or email info@threatfabric.com.