

How To Guide

The Cyber Threat Assessment Program



The Cyber Threat Assessment Program (CTAP)

What is CTAP?

The Fortinet Cyber Threat Assessment Program (CTAP) is a framework designed to assist you with offering your prospects a quick, easy and free insight into their security posture. It helps you build credibility, establish yourself as a trusted advisor and create a strong business case to choose Fortinet solutions to mitigate threats.

CTAP takes advantage of FortiGuard services, independent 3rd party testing (Virus Bulletin, AV Comparatives, and NSS Labs) and validation of superior security intelligence and protection effectiveness.

Why CTAP? What's in it for me?

- Demonstrate security expertise and establish yourself as a trusted advisor
- Accelerate prospect's decision to buy when threats are uncovered
- Gain a foothold into accounts (bridges the "demonstrate value" to "purchase" gap)
- Quickly prove FortiOS/FortiGuard value specific to customer environment
- Establish Fortinet Security Fabric as something tangible, not just a vision
- Overcome common objections related to PoC difficulties (time, cost, manpower, etc.)
- Standardize your sales processes and manage the end-to-end sales cycle

What are the Benefits to my customer?

Your customer's network is a complex set of interactions between applications, users and content at risk from sophisticated threats such as APTs, botnets and advanced malware. To manage the complexities and block the threats requires greater visibility and performance than traditional network firewalls can provide.

The Cyber Threat Assessment Program offers a FortiGate network security platform deployed as internal segmentation firewall (ISFW) or next generation firewall (NGFW) to provide your customer with an unprecedented insight into security and threat prevention, user productivity and network utilization without compromising performance or adding latency.

Most importantly, the Cyber Threat Assessment Report will translate this information into recommended actions your customer can take to mitigate security and threat concerns, improve user productivity and optimize network utilization with FortiGate's granular control over applications, users and content.

What happens during a CTAP?

- Duration to run a CTAP typically takes 3-7 business days.
- Assessment report available within 2 days after receiving log files.
- Report output is in PDF format.
- Report can be branded with Partner Logo.

We advise that the CTAP report is presented back to your prospect to maximise the use of time spent running it, this also gives you another chance to get in front of them and present real value by giving them real time insight into their network activity.

Report Differentiators

Here are some of the key differentiators when it comes to our assessments versus other security vendors:

- **Performance section**

We have an entire report section dedicated to network utilization/performance. Obviously, that's great for us since 1. performance plays to our strengths and 2. it will force prospects getting assessments from competitors to ask about missing sections.

- **At risk hosts chart**

We can utilize client reputation to determine the trustworthiness of individual hosts. Competitive programs do not provide similar insight.

- **FortiGuard**

We inherit all of the content security advantages of FortiGuard. This includes our 3,300+ application sensors (less than 2,000 for most competitors), 8,100+ IPS signatures, etc.

- **Deployment flexibility**

We allow streaming logs directly to a remote logging server OR uploading them to the portal. In addition, we support two deployment modes: sniffer and inline.

- **Use of FortiAnalyzer**

We use a FortiAnalyzer on the backend (eat our own dog food, so to speak). Most competitors use a separate tool entirely (and this is a great way to upsell a FortiAnalyzer unit!).

- **Sandboxing included**

There is no need to run firewall and sandbox reports separately. CTAPs can include sandboxing by choosing a checkbox, which demonstrates our Security Fabric in action.

How do I arrange a CTAP?

CTAP can be arranged through your Exclusive Networks account manager, we would identify the size of the required unit based on the network throughput. We have a number of units available from our loan pool, so please give us a call to discuss your requirements and we'll let you know which unit would be most appropriate.

A loan agreement would then be signed by the Partner, the End user & the Exclusive Networks Fortinet Team, delivery dates will then be set.

Installation

It is recommended that the first two CTAP installation are carried out in conjunction with a Qualified Exclusive Networks Engineer, the first installation would see the CTAP installed and set up by the Exclusive Networks Engineer with the Partner Engineer shadowing, the second installation would see the partner engineer installing the CTAP with the Exclusive Networks Engineer overseeing the installation, following the successful deployments the partner engineer is then free to undertake installation of CTAP evaluations.

The Exclusive Networks engineering time is not chargeable however there is a set of prerequisites that must be adhered to before the Engineer attends site:

- Span port configured to capture traffic to be sent to the FortiGate
- Management IP address, mask, gateway for the FortiGate with internet access

This will ensure smooth installation of the CTAP unit on customer site.

CTAP Report Generation

The CTAP report is received 2-3 days after the log data is received by Fortinet, the PDF Report is then emailed to the Partner to present back to the prospect.

What happens to the CTAP unit when the CTAP is complete?

The unit is packaged up (in the original box) and returned to Exclusive Networks:

Exclusive Networks
Alresford House
Mill Lane
Alton
Hampshire
GU34 2QJ

Example CTAP Reports

NGFW Assessment Report

Prepared For: **Indiana College**
Prepared By: **John Doe**
Report Date: **May 5, 2021**

Executive Summary

We aggregated the findings from our NGFW assessment to help you understand the overall security posture of your network. The highlights are listed below. We also provided remediation recommendations. Please refer to the Remediation section of the report for more details.

Security

- 11,126 Applications Analyzed
- 13 Malware and Botnets Detected
- 17 Top Risk Applications Detected

Productivity

- 330 SaaS Applications Detected
- 5 Top Priority Applications
- 5 Total Score for Peer Applications

Utilization

- 40.5m Bytes of Bandwidth Used
- 12.5 Mbps of Log Data
- 58.0% of Traffic is Critical

Security

Top Application Vulnerability Exploits Detected

Rank	App Name	CVSS	Severity	Count
1	Adobe Flash Player (All Plugins)	7.5	Critical	2,054
2	Microsoft Word (All Versions)	6.5	High	1,105
3	Microsoft Excel (All Versions)	6.5	High	1,105
4	Microsoft PowerPoint (All Versions)	6.5	High	1,105
5	Microsoft Outlook (All Versions)	6.5	High	1,105

Top Malware, Botnets and Spyware/Adware Detected

Rank	Malware Name	Type	Count	Severity
1	HEUR/HKJ.L	Malware	1	Critical
2	HEUR/HKJ.L	Malware	1	Critical
3	HEUR/HKJ.L	Malware	1	Critical

Cover Page

Executive Summary

Security: Applications / Devices / Threats

Productivity

Quick Stats:

- 330 SaaS Applications Detected
- 5 of 5 SaaS Applications Detected
- Score by Peer Applications Detected
- Score by Peer Applications Detected
- Score by Peer Applications Detected

Cloud Usage (SaaS)

Top 10 SaaS Applications:

Rank	App Name	Usage
1	Microsoft Office 365	12.5 MB
2	Google Workspace	8.5 MB
3	Zoom	5.5 MB

Cloud Usage (IaaS)

Top 10 IaaS Applications:

Rank	App Name	Usage
1	Amazon Web Services	15.5 MB
2	Microsoft Azure	10.5 MB
3	Google Cloud Platform	7.5 MB

Utilization

Quick Stats:

- 40.5m Bytes of Bandwidth Used
- 90.0% of Traffic is Critical
- 12.5 Mbps of Log Data
- 58.0% of Traffic is Critical

Average Bandwidth by Hour

Top Bandwidth Consuming Sources/Destinations:

Source/Destination	Bandwidth
www.google.com	15.5 MB
www.microsoft.com	10.5 MB
www.amazon.com	7.5 MB

Productivity: Cloud Usage / Applications / Websites

Utilization: Bandwidth / Log Width / Usage

Recommendations

- 1. Quarantine Botnet Hosts**
If you identify any botnet hosts in your network, you should immediately quarantine any infected hosts to prevent the infection from spreading and to protect your network.
- 2. Augment Your Email Security to Protect Against Known Malware**
Known malware is a significant threat to your organization's security. You should augment your email security to protect against known malware.
- 3. Add Sandboxing Technology to Detect Unknown Malware**
The best way to protect your organization from unknown malware is to use sandboxing technology to detect and isolate any suspicious activity.
- 4. Improve Malicious URL Detection and Training**
Malicious URLs are a significant threat to your organization's security. You should improve your malicious URL detection and training to protect your organization.
- 5. Educate and Protect Users from Phishing Attempts**
Phishing is a significant threat to your organization's security. You should educate your users and implement measures to protect them from phishing attempts.
- 6. Audit High Risk Hosts for Attack Susceptibility**
Some hosts in your network are at a high risk of being attacked. You should audit these hosts for attack susceptibility and implement measures to protect them.
- 7. Enforce Corporate Use Policies on Peer to Peer Applications**
Peer to peer applications can be a significant threat to your organization's security. You should enforce corporate use policies on these applications.

Recommendations

You can download CTAP sample reports from the Fortinet Partner Portal

<https://partnerportal.fortinet.com/prm/English/c/CTAP-Methodology>