NetOps and SecOps Collaborate to Identify & Remediate Vulnerabilities

Headline-grabbing cyberthreats exploded over the last 18 months that have paralyzed businesses, hospitals, and education districts. Many of these organizations have acquired cybersecurity solutions to help prevent future breaches. Another critical tactic has been to evaluate their environment to remove and stay ahead of potential vulnerabilities enterprise-wide.

A global services organization had recently implemented NETSCOUT's nGeniusONE Service Assurance solution, a packet-based network and application monitoring solution for performance management of their IT environment. The selection of nGeniusONE with InfiniStreamNG (ISNG) appliances was made by a cross-functional IT team that included leadership from infrastructure, network engineering, network operations, and security operations. Real-time monitoring, in-depth packet analysis, support out-of-the-box for more than 1,000 protocols and applications, alerting, troubleshooting, forensics, and packet decode capabilities all played a role in selecting nGeniusONE for this project.

The IT team, due to focus on several digital transformation projects at the time, also selected NETSCOUT's Visibility as a Service (VaaS) proactive 24 x7 x 365 managed service support to gain immediate value from the new service assurance solution while freeing up their corporate IT team to focus on the strategic cloud and application migrations in process to meet business goals.

Risk

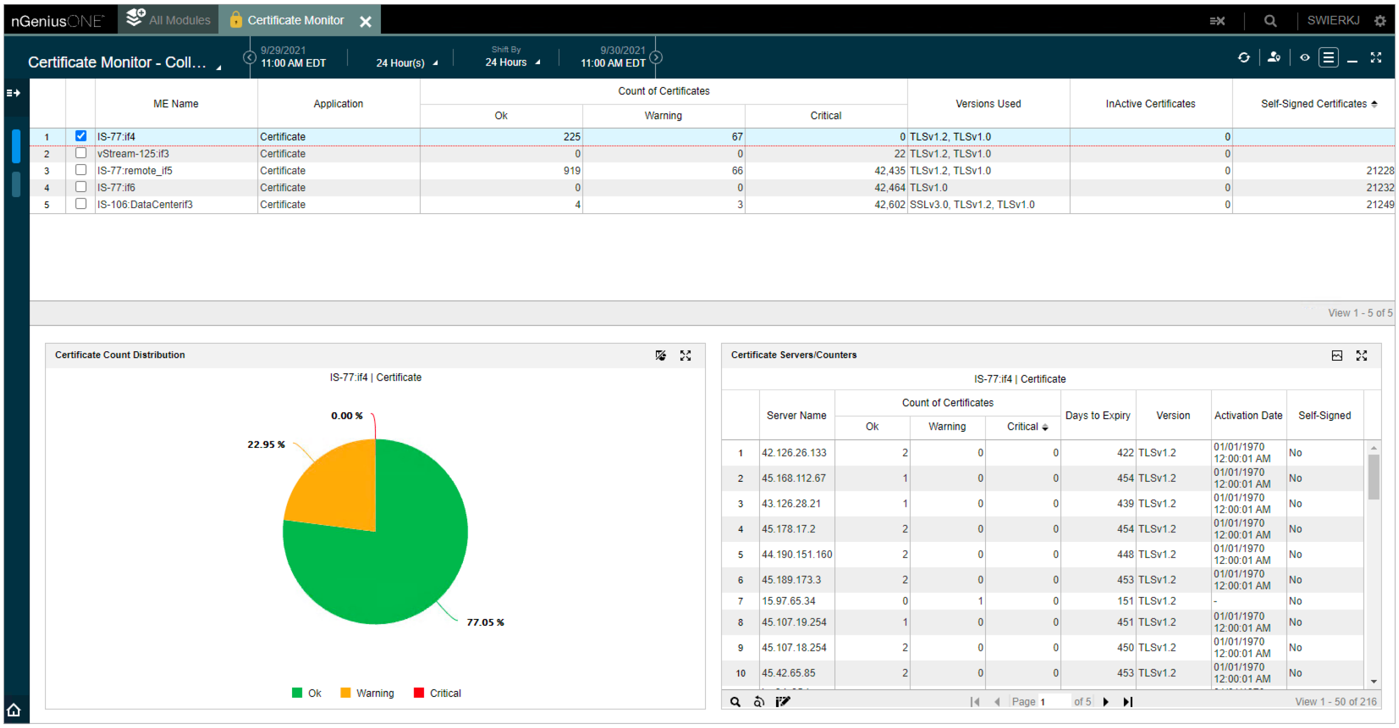
Becoming more proactive by reducing security risks and vulnerabilities throughout their global network was one of the goals the IT team shared with the NETSCOUT® Visibility as a Service experts in their initial planning meeting. Specifically, the NetOps and SecOps team communicated their concerns for maintaining updated Secure Socket Layer (SSL) / Transport Layer Security (TLS) certificates, reducing the use of weak ciphers, and identifying and remediating vulnerabilities that could be taken advantage of by malware and ransomware software.

Impact

Expired SSL certificates make both clients and websites vulnerable, which can result in unplanned outages, expose an opening to hackers who can enter the network, or create risks to users for man-in-the-middle attacks, all of which should be avoided by ensuring certificates are up to date. Keeping track of all the certificates and their expiration can be challenging, particularly for an IT organization responsible for the networks of recently acquired companies, where details may not be easily obtained.

Lower levels of encryption from weak cipher suites are more vulnerable to sophisticated hackers. The cipher suites themselves used for enabling secure network connections through TLS and SSL have developed over the years to provide greater levels of strength based on algorithms and protocols used. Identifying weak ciphers in the network and upgrading to more advanced ciphers ensure organizations have a greater level of protection.

Historically, hackers have found vulnerabilities in certain network protocols that have allowed them to wreak havoc with malware and ransomware attacks. Server Message Block (SMB) v1, legitimately used for printer services, file sharing, and network computer communications, had vulnerabilities that enabled hackers to create the highly disruptive WannaCry and NotPetya malware attacks. It is recommended that this be disabled throughout corporate environments to avoid these expensive disruptions from occurring.



		ME Name	Application	Count of Certificates			Versions Used	InActive Certificates	Self-Signed Certificates
				Ok	Warning	Critical			
1	☑	IS-77:if4	Certificate	225	67	0	TLSv1.2, TLSv1.0	0	
2	□	vStream-125:if3	Certificate	0	0	22	TLSv1.2, TLSv1.0	0	
3	□	IS-77:remote_if5	Certificate	919	66	42,435	TLSv1.2, TLSv1.0	0	21228
4	□	IS-77:if6	Certificate	0	0	42,464	TLSv1.0	0	21232
5	□	IS-106:DataCenterif3	Certificate	4	3	42,602	SSLv3.0, TLSv1.2, TLSv1.0	0	21249

	Server Name	Count of Certificates			Days to Expiry	Version	Activation Date	Self-Signed
		Ok	Warning	Critical				
1	42.126.26.133	2	0	0	422	TLSv1.2	01/01/1970 12:00:01 AM	No
2	45.168.112.67	1	0	0	454	TLSv1.2	01/01/1970 12:00:01 AM	No
3	43.126.28.21	1	0	0	439	TLSv1.2	01/01/1970 12:00:01 AM	No
4	45.178.17.2	2	0	0	454	TLSv1.2	01/01/1970 12:00:01 AM	No
5	44.190.151.160	2	0	0	448	TLSv1.2	01/01/1970 12:00:01 AM	No
6	45.189.173.3	2	0	0	453	TLSv1.2	01/01/1970 12:00:01 AM	No
7	15.97.65.34	0	1	0	151	TLSv1.2	-	No
8	45.107.19.254	1	0	0	451	TLSv1.2	01/01/1970 12:00:01 AM	No
9	45.107.18.254	2	0	0	450	TLSv1.2	01/01/1970 12:00:01 AM	No
10	45.42.65.85	2	0	0	453	TLSv1.2	01/01/1970 12:00:01 AM	No

Figure 1: The Certificate Monitor view in nGeniusONE revealed details regarding SSL certificates that were approaching their expiration dates. The Security Operations team was able to proactively update the certificates and avoid an expiration.

Analysis and Identification

Based on the input from the NetOps and SecOps at the service company, the VaaS team resourced their best-practices procedures in configuring nGeniusONE® and ISNG appliances to analyze several specific protocols, configured a couple of workspaces for contextual analysis, and based on the findings, provided recommendations for remediating the problems discovered.

Expiration Analysis of SSL Certificates – Proactive analysis of SSL certificates to identify expired or soon-to -expire certificates enabled the team to update the certificates in time to avoid unnecessary vulnerabilities. The Certificate Monitor feature in nGeniusONE provides visibility into the number of certificates in use, with special callouts for certificates approaching expiration, the versions of each certificate used on the server, and identification of expired certificates. In the case of this service organization, the analysis indicated that nearly half of the certificates monitored in one location (Figure 1) were approaching expiration. In another location, they revealed several expired certificates.

TLS Cipher Suite Analysis – The VaaS team configured monitoring of SSL protocol with analysis providing details of the different ciphers in use in their network. As seen in Figure 2, the details revealed that some ciphers in use were older and weaker than the levels approved by the service company's IT organization, e.g., Au_RSA. As several acquisitions had been completed recently for the company, ensuring all the devices were using secure ciphers was a priority and the details provided by the VaaS team helped close that gap to secure the service company's devices and environment quicker.

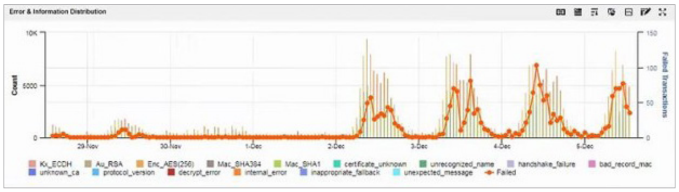
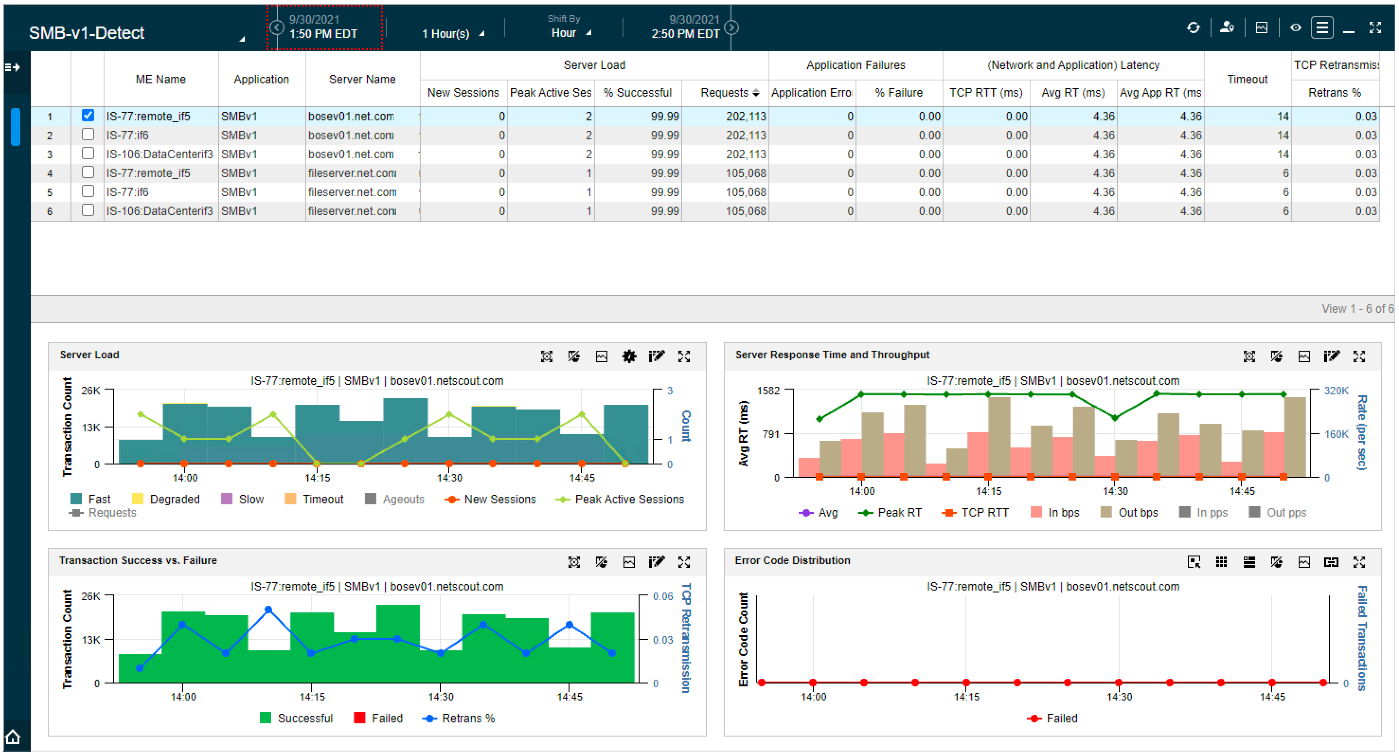


Figure 2: SSL monitoring in nGeniusONE provided analysis of the actual ciphers in use to ensure only strong, secure ciphers were implemented enterprise-wide. The Security Operations team was able to upgrade the weak Au_RSA to a stronger cipher approved for the service company network.

SMB v1 Vulnerability – The VaaS team configured the service company's nGeniusONE to identify and monitor the SMB v1 protocol, specifically to determine if it was running in the network at all. Companies have widely disabled SMB v1 network-wide due to its vulnerabilities, which noted WannaCry and NotPetya malware attacks have taken advantage of in the past. As seen in Figure 3, this turned out to be critically important, as they did in fact discover SMB v1 scattered in a few locations, which the IT team quickly disabled with the details from nGeniusONE.



SMB-v1-Detect 9/30/2021 1:50 PM EDT 1 Hour(s) Shift By Hour 9/30/2021 2:50 PM EDT

		ME Name	Application	Server Name	Server Load				Application Failures		(Network and Application) Latency			Timeout	TCP Retransmis
					New Sessions	Peak Active Ses	% Successful	Requests	Application Erro	% Failure	TCP RTT (ms)	Avg RT (ms)	Avg App RT (ms		Retrans %
1	☑	IS-77:remote_if5	SMBv1	bosev01.net.com	0	2	99.99	202,113	0	0.00	0.00	4.36	4.36	14	0.03
2	☐	IS-77:if6	SMBv1	bosev01.net.com	0	2	99.99	202,113	0	0.00	0.00	4.36	4.36	14	0.03
3	☐	IS-106:DataCenterif3	SMBv1	bosev01.net.com	0	2	99.99	202,113	0	0.00	0.00	4.36	4.36	14	0.03
4	☐	IS-77:remote_if5	SMBv1	fileserver.net.com	0	1	99.99	105,068	0	0.00	0.00	4.36	4.36	6	0.03
5	☐	IS-77:if6	SMBv1	fileserver.net.com	0	1	99.99	105,068	0	0.00	0.00	4.36	4.36	6	0.03
6	☐	IS-106:DataCenterif3	SMBv1	fileserver.net.com	0	1	99.99	105,068	0	0.00	0.00	4.36	4.36	6	0.03

View 1 - 6 of 6

Figure 3: nGeniusONE was configured to monitor SMB v1, which was discovered in a few locations and was quickly disabled.

Restoration

The visibility provided by the ISNG appliances and analysis by nGeniusONE revealed to the NetOps and SecOps teams several security vulnerabilities, including expired and soon-to-expire SSL certificates, weak ciphers, and malware vulnerabilities, which were all quickly addressed based on the details provided by the NETSCOUT Visibility as a Service experts. The IT team was able to update the SSL certificates and get ahead of the soon-to-expire certificates. The weak ciphers were all upgraded, and they disabled the SMB v1 protocol network-wide, including in the newly acquired divisions, all of which has made the users, devices, and corporate network much more secure.

Summary

Given the criticality of becoming more proactive and the need to reduce security risks and vulnerabilities throughout their global network, the combined efforts of the NETSCOUT Visibility as a Service experts and the service company's NetOps and SecOps team have successfully addressed three potential areas of concern in their early engagement. Not only have they updated their SSL / TLS certificates, they also have a process now to stay ahead of future expirations, well in advance of issues emerging. Further, the removal of weak ciphers and SMB v1 from the current enterprise, with periodic audits by the VaaS team using nGeniusONE, will continue to protect the organization from avoidable vulnerabilities.

With members of both teams able to analyze the same network and application traffic details, communications were more informed, visibility to potential security risks was improved, mean time to knowledge and resolution (MTTK/MTTR) was faster, and helped IT achieved higher operational efficiencies. The service company also reaped the benefits of a more cost-effective approach to gaining packet level visibility with a single source of truth from the NETSCOUT solution. The NetOps and SecOps teams will continue to protect the organization from avoidable vulnerabilities.

NETSCOUT.

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us