CIPHER SUITE AND ENCRYPTION MONITORING – FINDINGS

KEY FINDINGS FOR CIPHER SUITE AND ENCRYPTION MONITORING

5,660 **insecure sessions**	• Sensitive information may be exposed to malicious actors, which can directly cause further data loss and security breaches.
64,000 **sessions**	• Sessions using RC4 encryption are considered insecure and expose your company to data theft.
1,900 **days**	• It has been 400 days since the oldest SSL certificate expired. This exposes the enterprise and customers to malicious cybercrime.
1,650 **Insecure sessions**	• Number of sessions observed using SSLv3, an insecure version vulnerable to man-in-the-middle attacks.

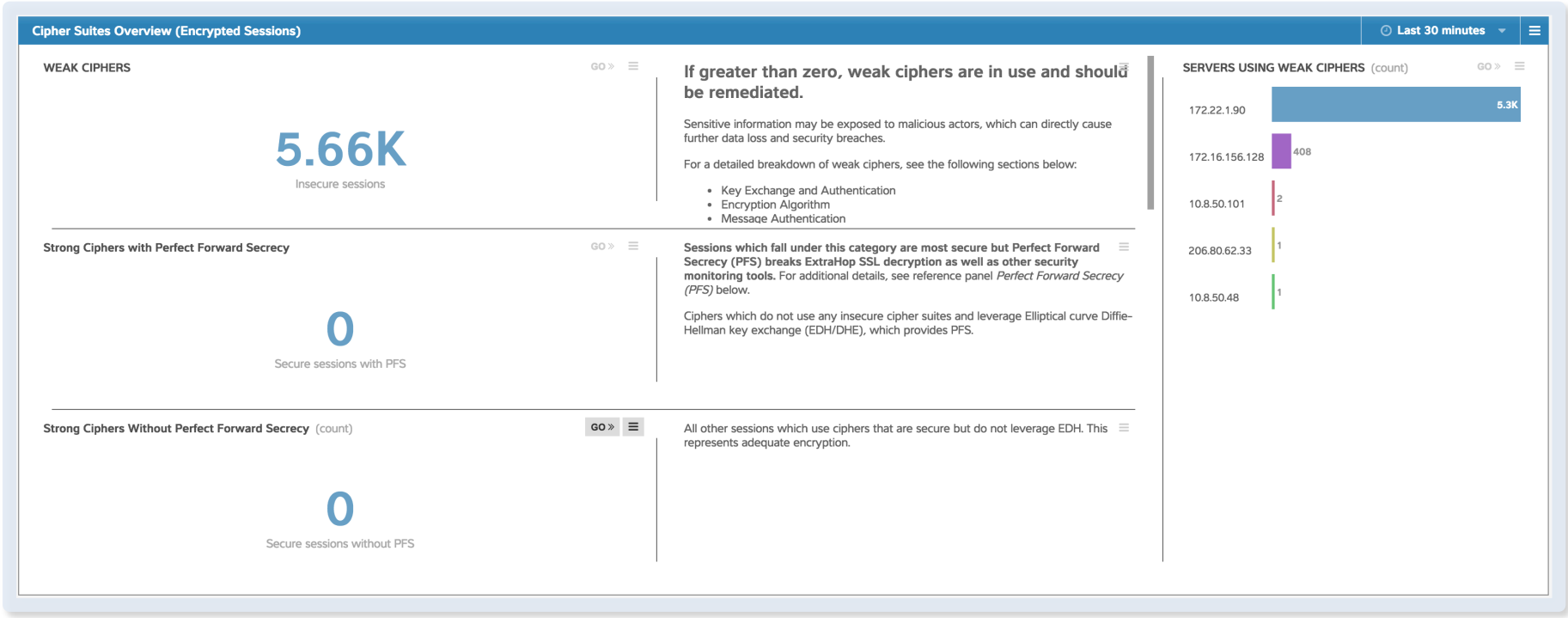
INDUSTRY FACTS

- A data breach cost U.S. companies an average of **$6.5M per incident** in 2014 – Ponemon Institute
- **Compliance with PCI DSS v3.1** requires phasing out SSL by June 2016 – Dara Security
- **Only 40% of HTTP servers support TLS or SSL** and present valid certificates – Redhat (scan of Alexa top 1M sites)
- **20% of servers are using broken cipher suites** making encrypted data vulnerable – Redhat
- RC4 is still used in **>18% of HTTPS servers** – Redhat

CIPHER SUITE AND ENCRYPTION MONITORING DASHBOARDS

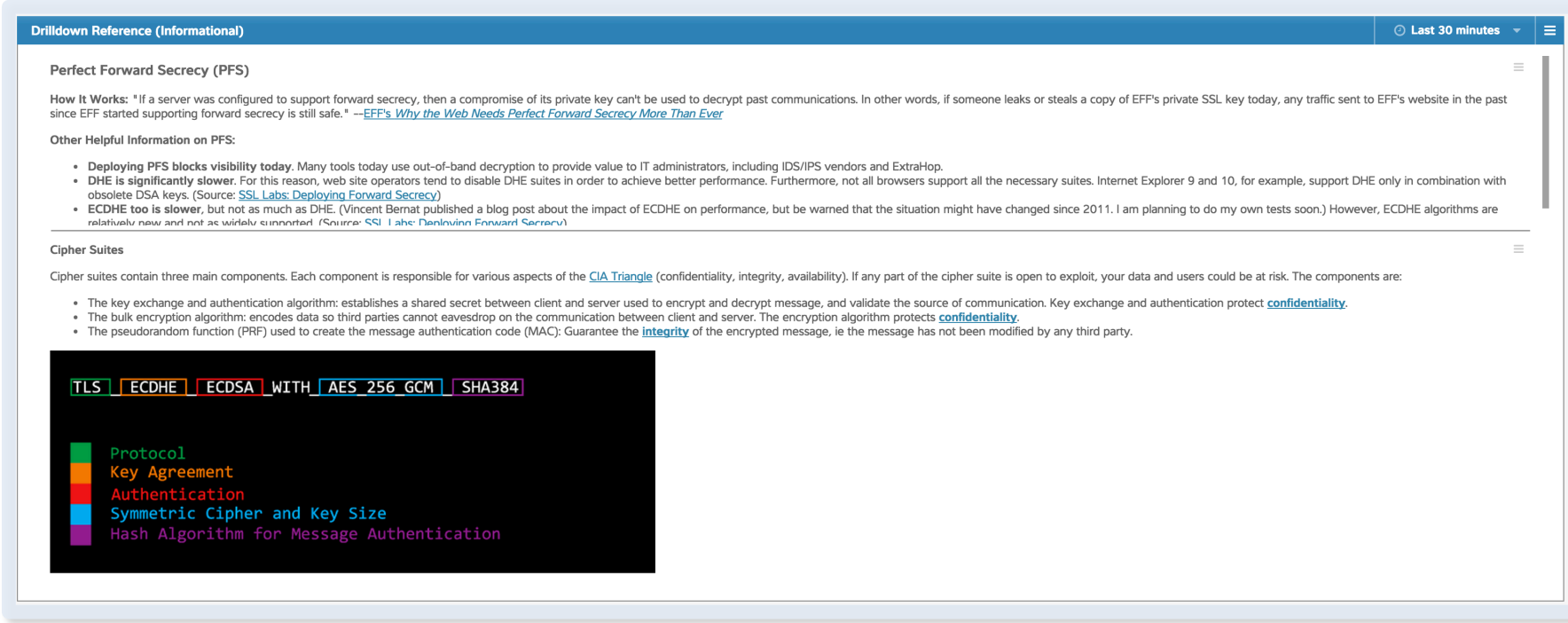
The ExtraHop platform performs continuous SSL envelope analysis to determine the ciphers used, the expiration dates of keys, and other critical metrics that must be monitored to ensure proper application functionality and security. The the Cipher Suite and Encryption dashboard shows observed behavior and activity during the project period and should be referenced by the InfoSec team.

The section of the the Cipher Suite and Encryption dashboard below provides a complete picture of the strength or weakness of ciphers on your network, and your weakest points that require immediate remediation.

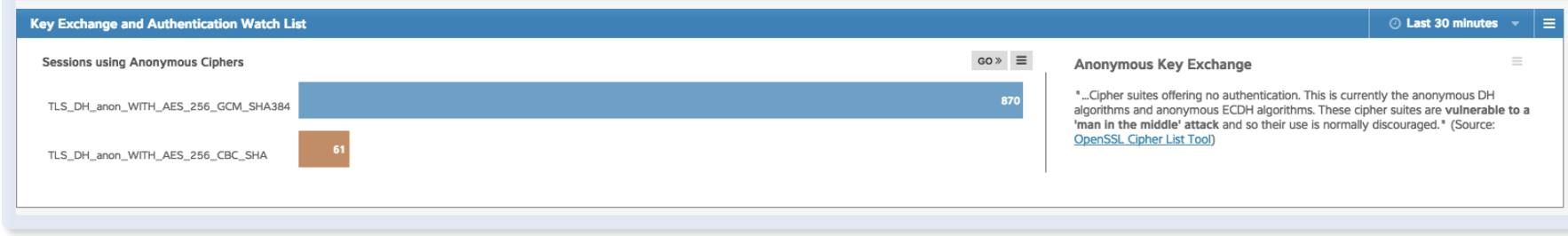


CIPHER SUITE AND ENCRYPTION MONITORING DASHBOARD

This dashboard section describes the latest issues in modern encryption, so you can be as secure as possible without hampering visibility.

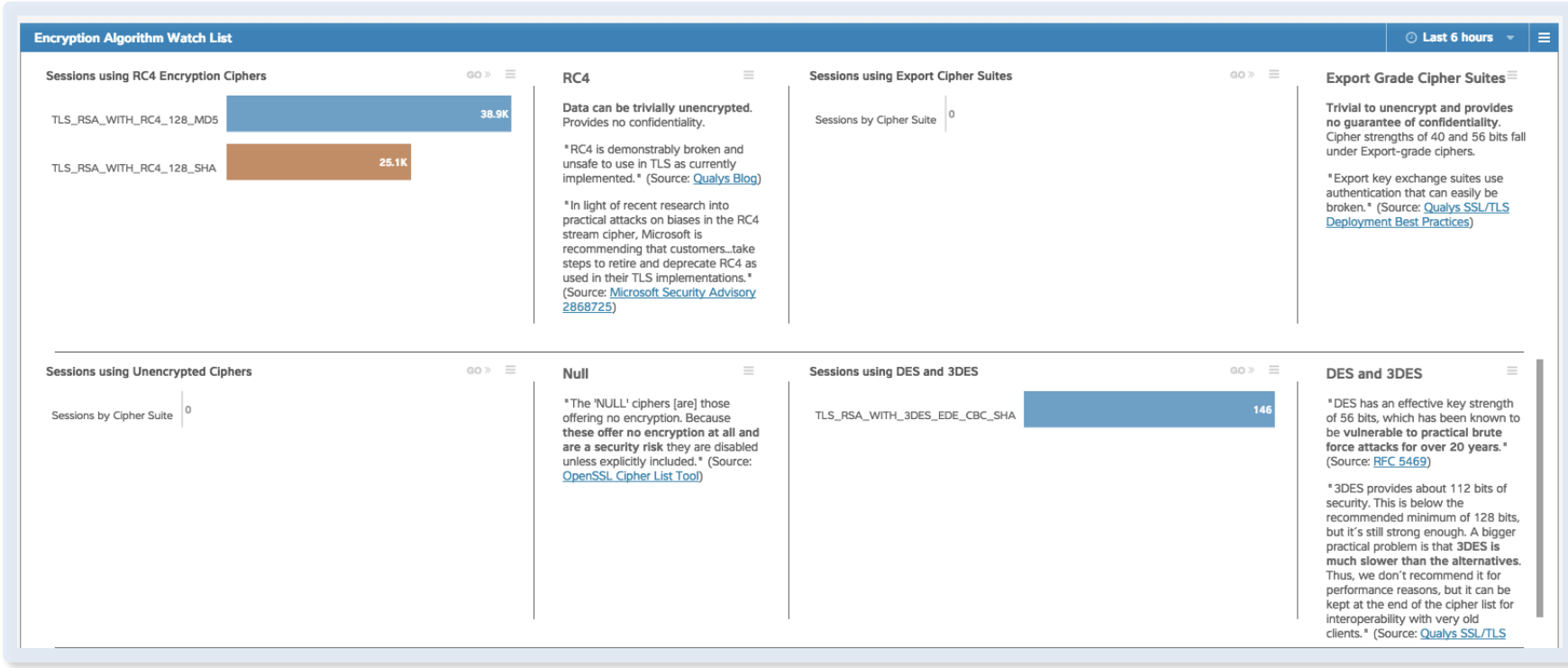


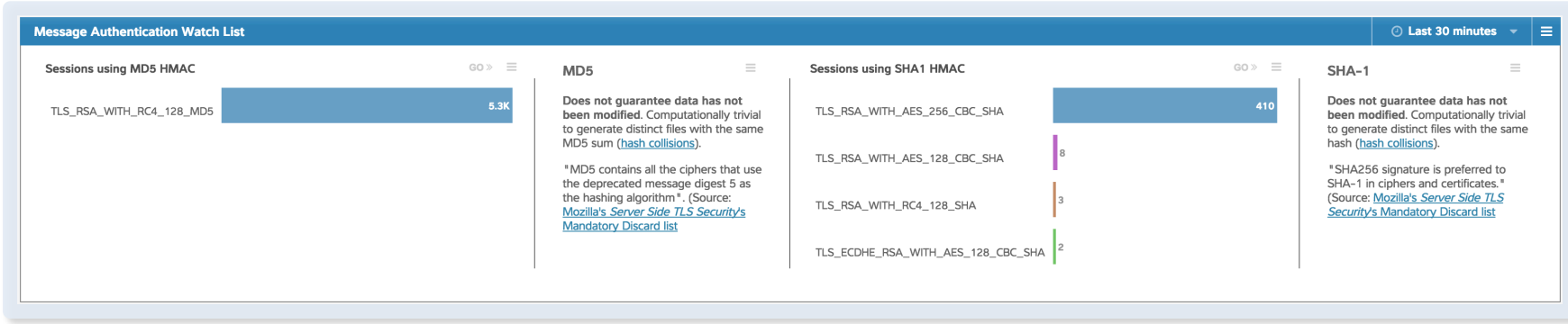
This section shows the number of anonymous ciphers in your system, which are vulnerable to hacking through man-in-the-middle attacks.



CIPHER SUITE AND ENCRYPTION MONITORING DASHBOARD

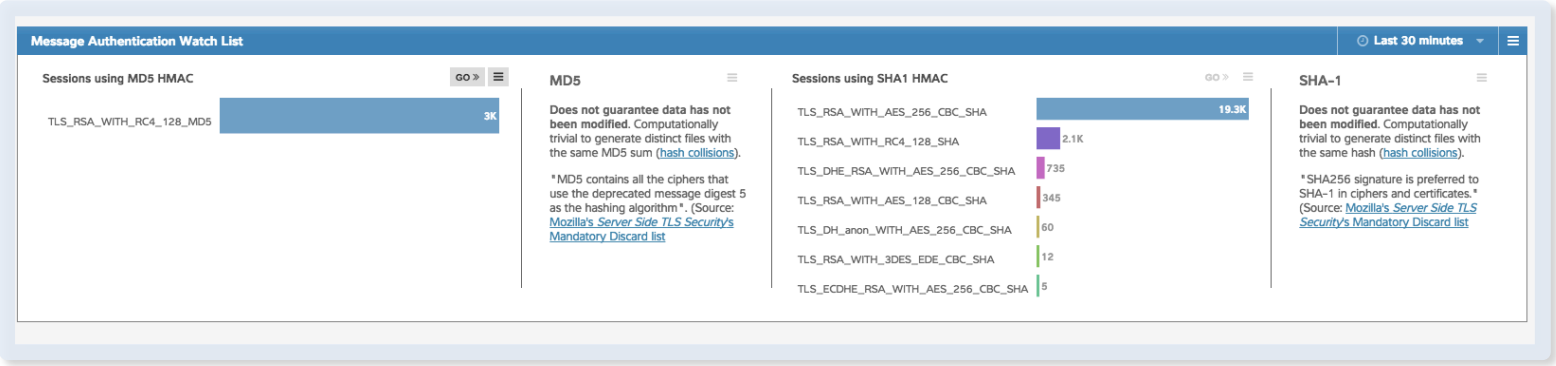
These dashboard areas show non-secure ciphers in your network. These should be tracked continuously and remediated immediately.



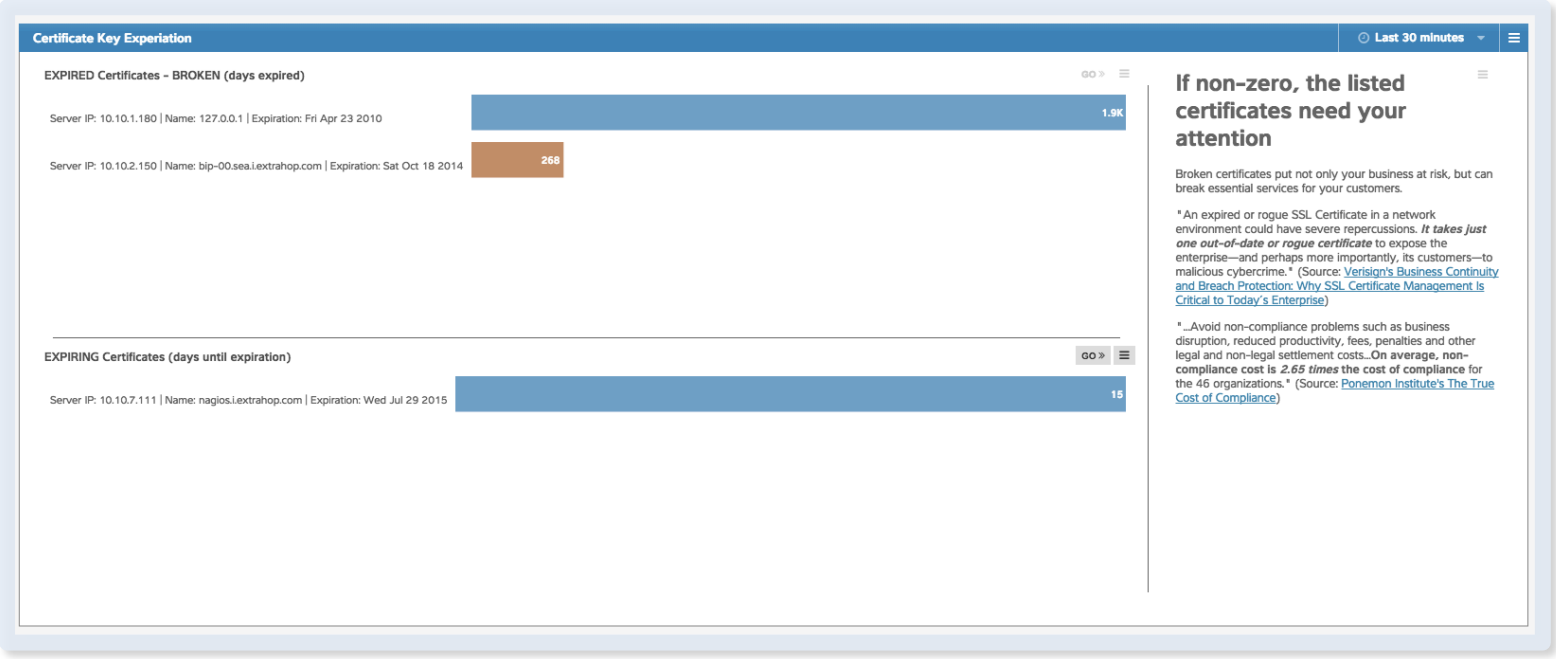


CIPHER SUITE AND ENCRYPTION MONITORING DASHBOARD

These fields show sessions on your network using the non-secure MD5 and SHA-1 ciphers. These must be removed to assure data security.

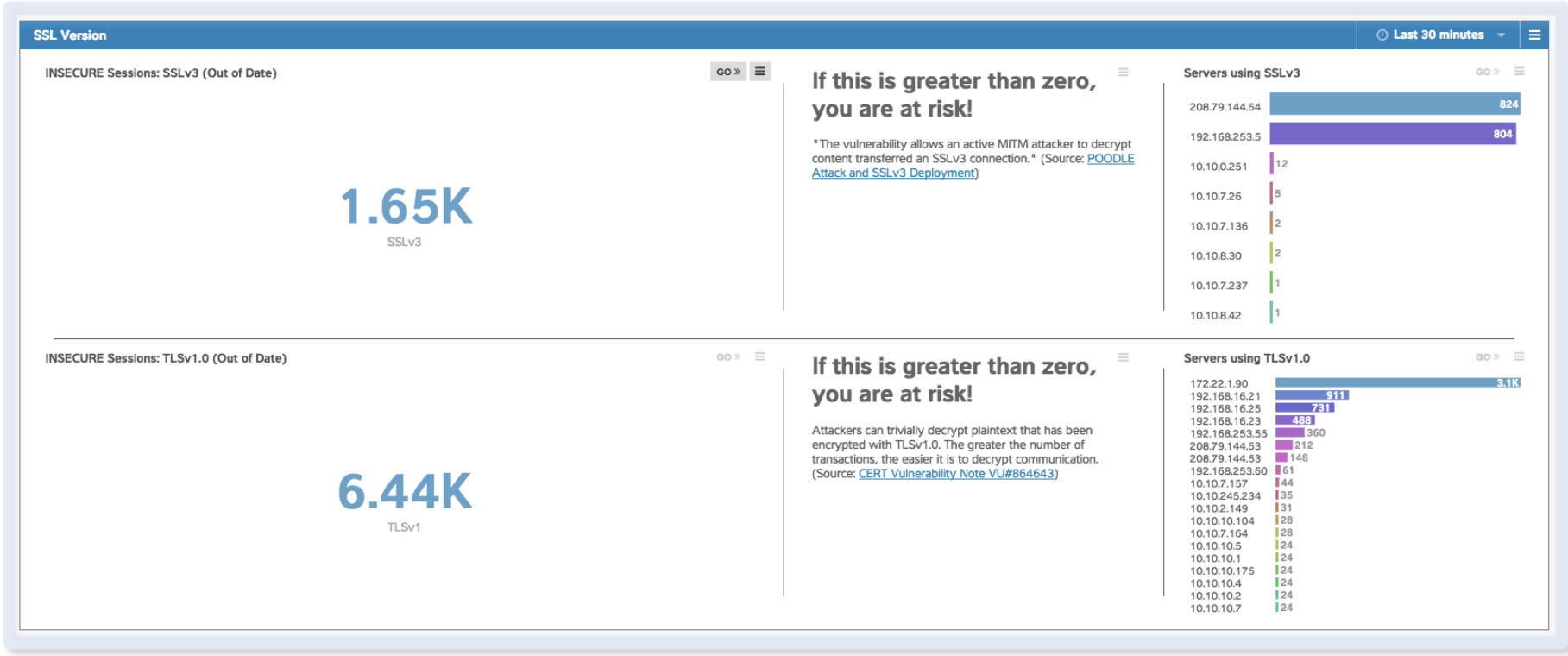


Here you see the number of expired or soon-to-expire SSL certificates on your network. Expired certs need immediate remediation.



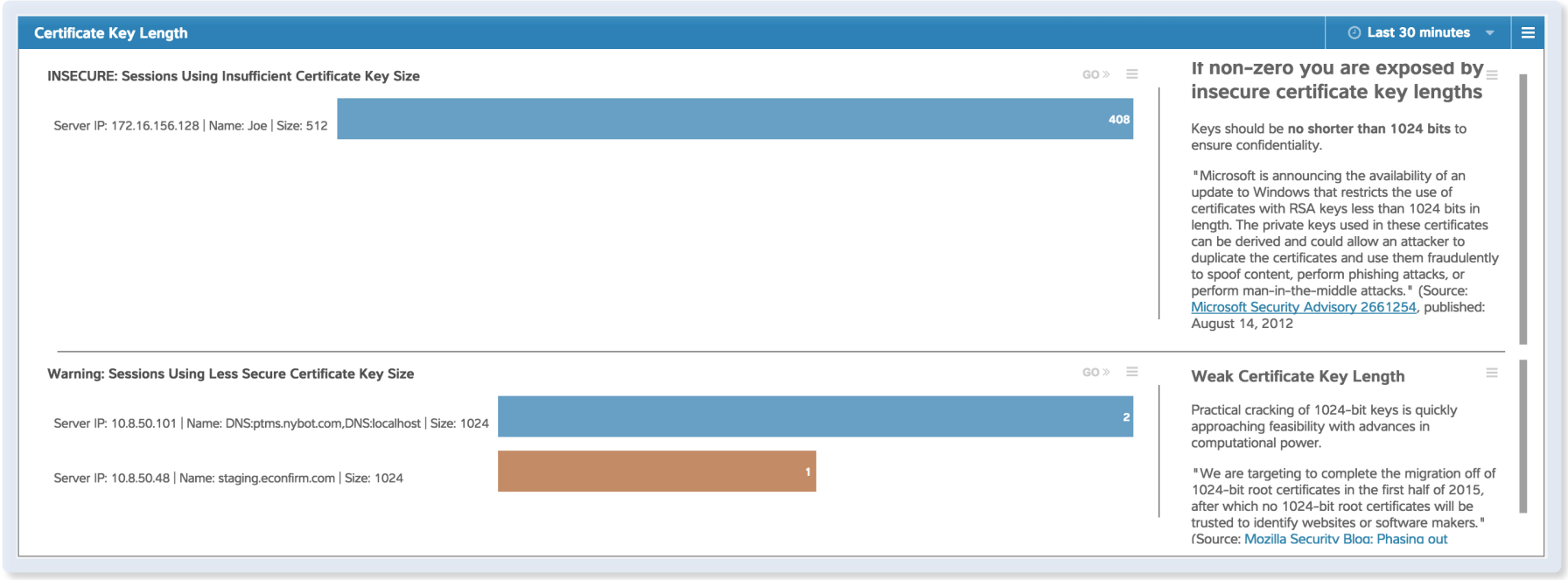
CIPHER SUITE AND ENCRYPTION MONITORING DASHBOARD

This section of the Cipher Suite and Encryption dashboard shows the number of sessions on your network using outdated and vulnerable SSL or TLS connections, which require immediate remediation.



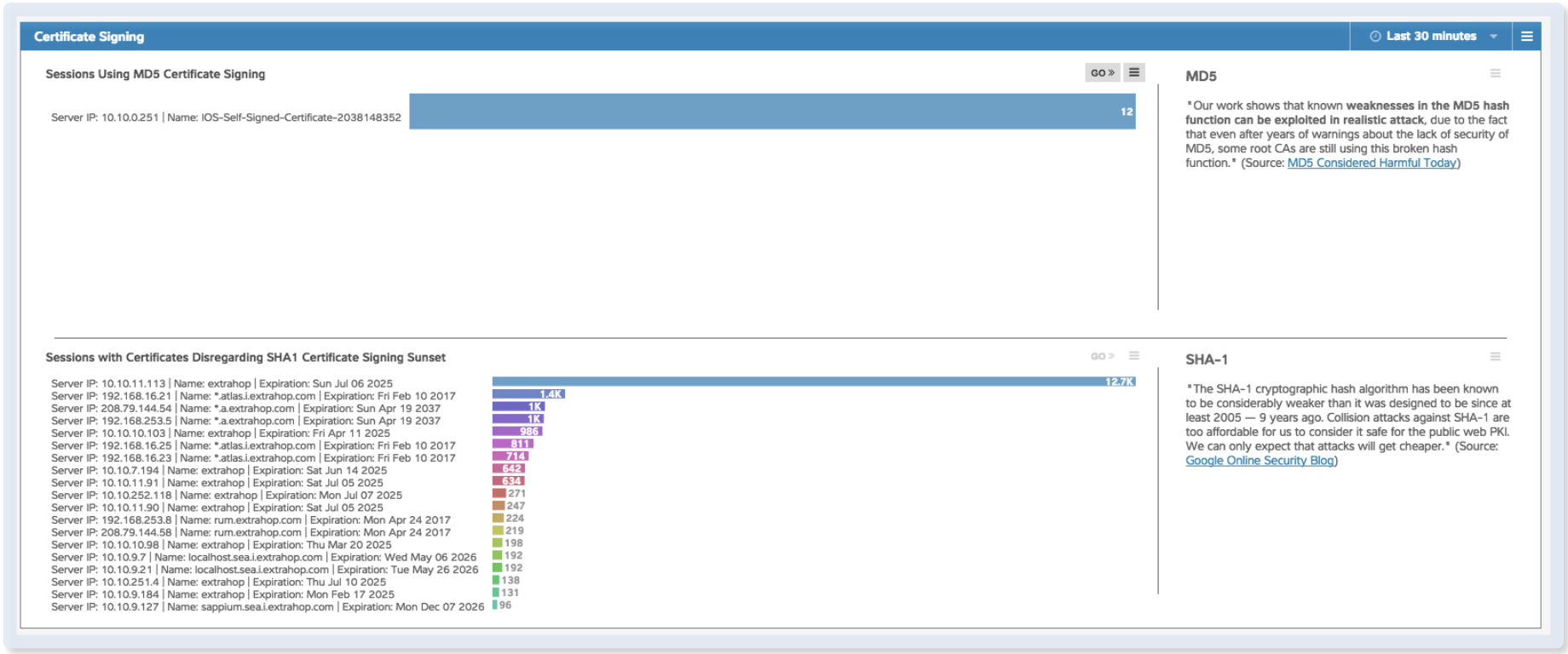
CIPHER SUITE AND ENCRYPTION MONITORING DASHBOARD

Here you see the number of sessions using weak security keys. Using weak security keys leaves your data at risk.



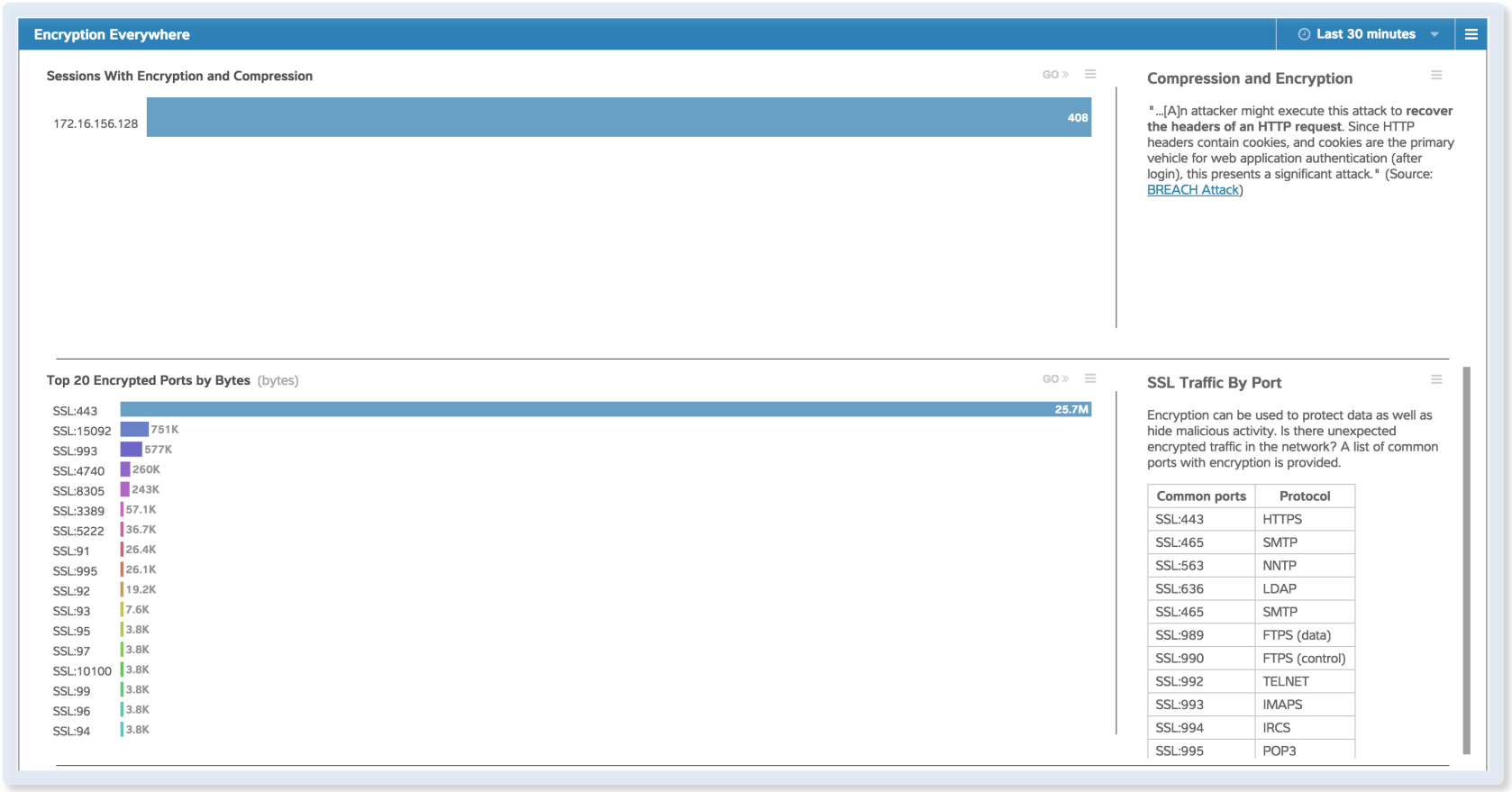
CIPHER SUITE AND ENCRYPTION MONITORING DASHBOARD

MD5 and SHA1 are vulnerable, broken hash functions that are still widely in use. This section of the Cipher Suite and Encryption dashboard shows instances of them on your network, meaning your data is insecure.



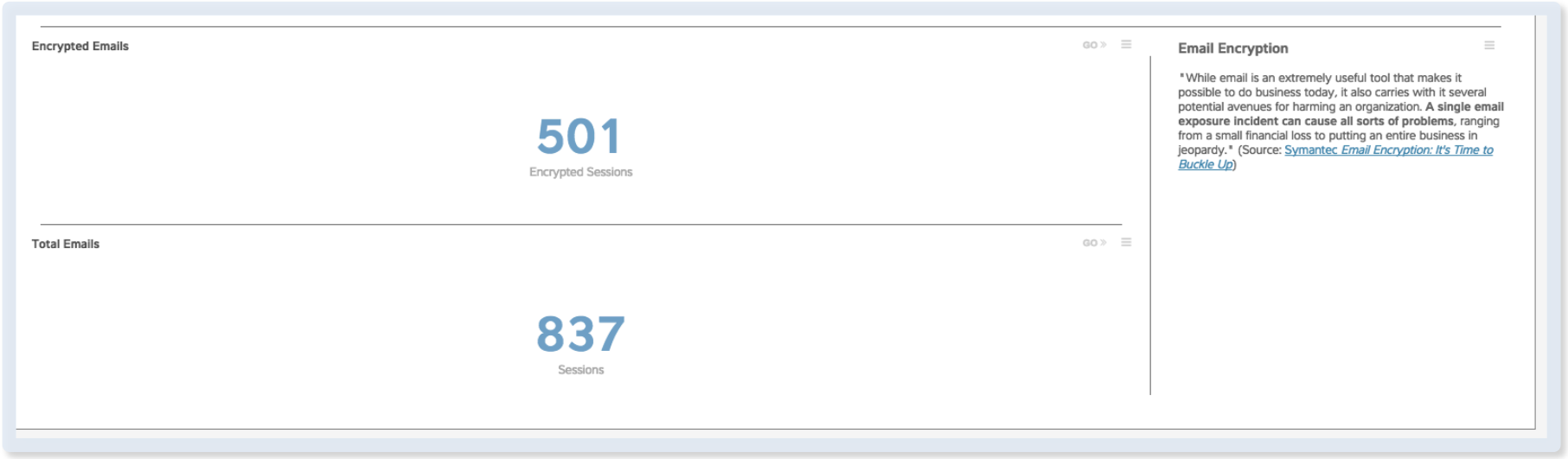
CIPHER SUITE AND ENCRYPTION MONITORING DASHBOARD

This section of the Cipher Suite and Encryption dashboard shows where encryption is present on your network. This view provides you with a continuous audit of encryption use, which is necessary when proving compliance with certain industry and privacy regulations.



CIPHER SUITE AND ENCRYPTION MONITORING DASHBOARD

This section of the Cipher Suite and Encryption dashboard shows how many emails going across your network are encrypted. Unencrypted email is a security risk, especially if you handle sensitive information. Encrypting all email is a vital step toward data security.



CIPHER SUITE AND ENCRYPTION MONITORING DASHBOARD

This part of the Cipher Suite and Encryption dashboard calls out multi-server and wildcard certificates that increase your vulnerability to "man-in-the-middle" attacks. Another surprising vulnerability comes in the form of certificates with long validity periods. This dashboard shows how long you have until certificates expire, so you know exactly when to refresh them.