

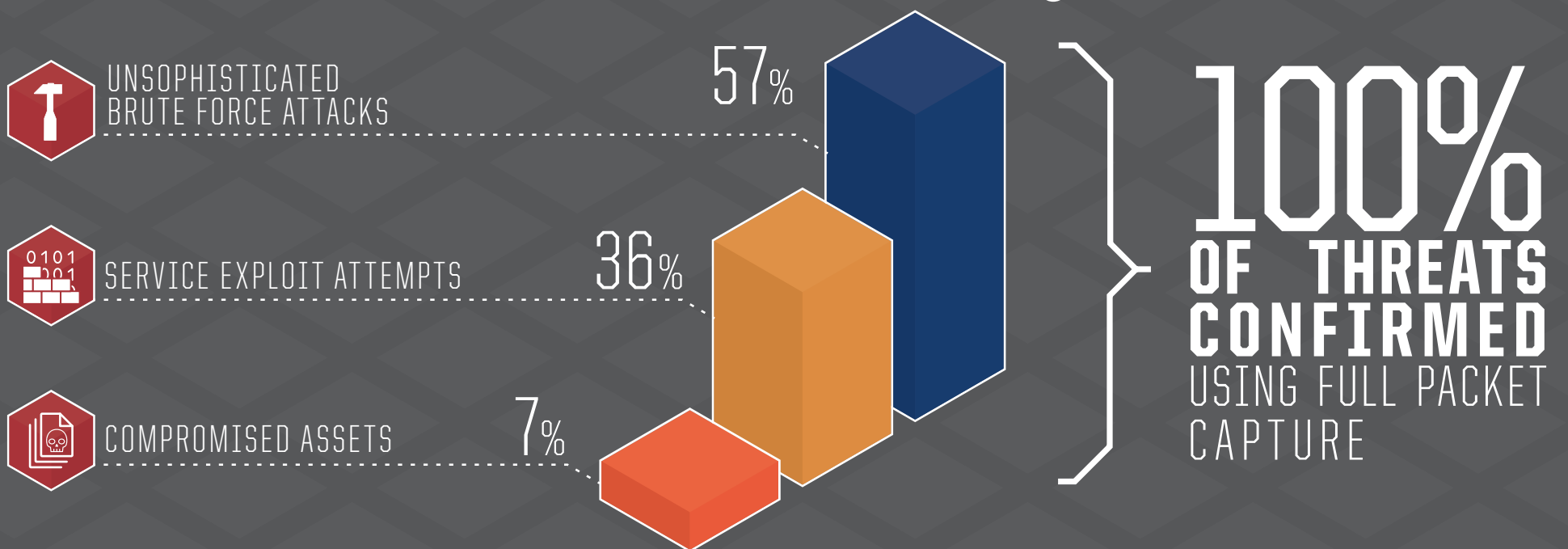
# A VIEW FROM THE SOC

## INCIDENT BREAKDOWN

01/01/2014 - 01/01/2016

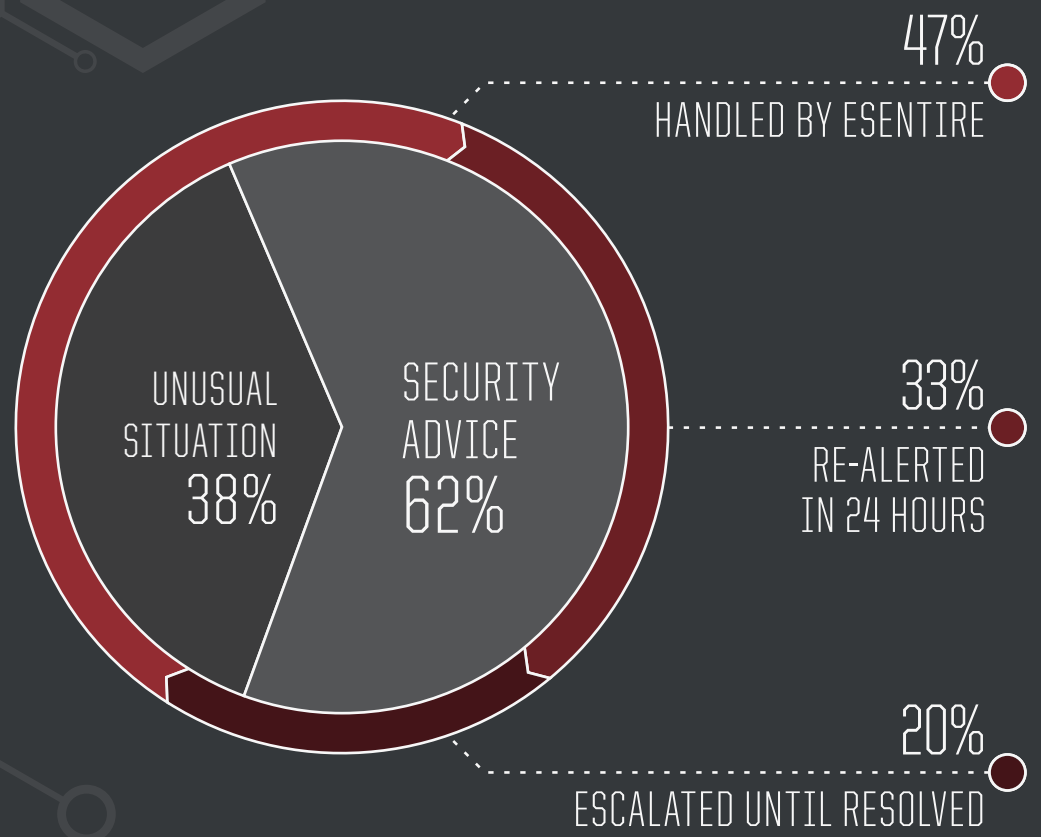
The eSentire Security Operations Center (SOC) recently commissioned a study of its own data to correlate and profile threat vectors and trends impacting mid-sized enterprise. This analysis represents all threats actioned by SOC analysts from January 2014 to January 2016.

### ATTACKS DETECTED & RESPONDED TO PER SENSOR



### INCIDENTS HIGHLIGHT THE GAP THAT EXISTS BETWEEN THE FIREWALL AND THE ENDPOINT

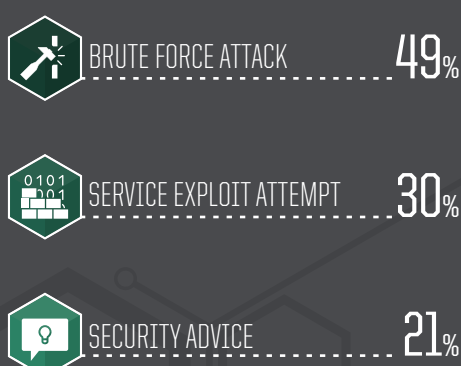
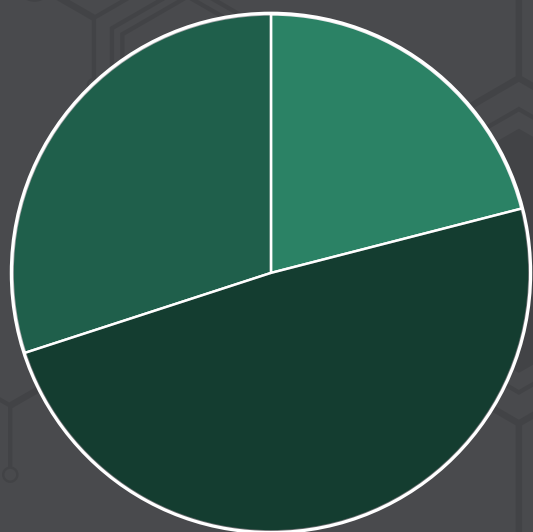
Unlike traditional Managed Security Service (MSS) providers, client communication is the core of our business. The SOC asks questions and provides valuable advice; about a quarter of all incidents opened in the SOC either provide generic recommendations on how to implement better security hygiene (i.e. removing an attack vector the SOC saw that isn't being exploited today, but could be), or to track situations considered to be unusual (i.e. possible attack vectors flagged where the SOC is unsure if an incident constitutes malicious activity or is acceptable to the client) and can't be explained without client feedback.



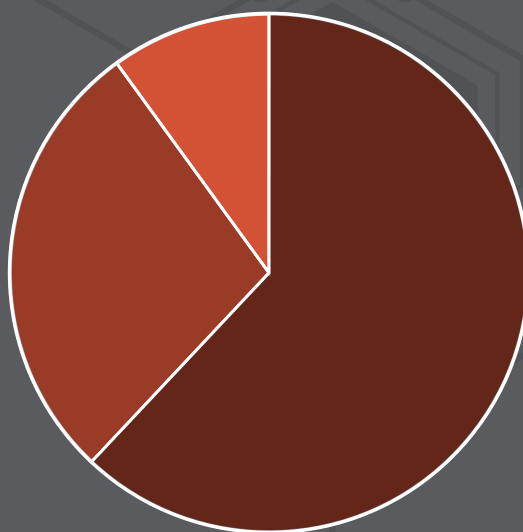
## INDUSTRY BREAKDOWN

Top 3 threats impacting segments.

### FINANCE



### LEGAL



### HEALTHCARE

