



The Hacker-Proof Homefront

How your business can win the war on cybercrime



The war abroad



As the number of connected devices and digital platforms grows, cybercriminals are becoming increasingly sophisticated, causing more devastation than ever before.



\$6 trillion



will be lost to cybercrime damages worldwide by 2021.

The FBI's top 2 most wanted cybercriminals have collectively cost their victims

\$100+ million in damages.



Nearly **2 out of 3** U.S. adults who have personal social media profiles know their accounts have been hacked.

A strong foundation

A growing number of enterprises are already using Security Information and Event Management (SIEM) tools to protect their operations.

The SIEM market has shown a **\$1,390 million increase** from 2009 to 2017.

Source: IDC



Strengthening the homefront

Use the power of the SIEM platform to add more functionality that will evolve your organization into a Security Operations Center (SOC):



24/7 service desk

This can be integrated into the SIEM platform to provide a user portal, and to help drive security awareness across the organization.



Threat intelligence

Engage external threat intelligence services to provide the "wisdom of crowds," extending threat visibility beyond the horizon.



Incident response

A team that can respond to distress signals both virtually and physically will help protect your business from inevitable attempts at infiltration.



Hunt teams

Dedicated teams that use proactive intelligence to search for and eliminate threats early in the kill chain will help your organization shift from defense to offense.



Machine learning

Using machine learning tools to detect anomalous user behavior and rogue network traffic will give hunt teams a weapon from which cybercriminals will find it difficult to hide.



Co-managed SOC approach

The journey from SIEM to SOC is much more than a technology uplift — it requires advanced skills and optimization. With a co-managed SOC approach, you can use your own resources, as well as those of your managed security service provider, to execute a more aggressive and offensive program.



Gauging victory

Expect several advantages after adopting a SOC:



Improved threat management by reducing breach Time to Detect (TTD)



Optimization of available expertise by coordinating the security teams and consolidating the functions



Enhanced regulatory compliance for monitoring, auditing and reporting

Sources:

FBI. (2017). Most Wanted: Cyber Crimes Most Wanted.

Morgan, S. (2017, June 15). Top 5 Cybersecurity Facts, Figures and Statistics for 2017. CSO.

University of Phoenix. (2016, April 27). Nearly Two-Thirds of U.S. Adults With Social Media Accounts Say They Have Been Hacked.