Skillmine
Technology • Consulting • Services

CASE STUDY OF

SECURITY OPERATION CENTER

A major Indian fashion e-commerce company

India's largest e-commerce store for fashion and lifestyle products, they aim at providing a hassle free and enjoyable shopping experience to shoppers across the country with the widest range of brands and products on its portal.

Business Challenge

- The company was experiencing internal breaches and external cyberattacks.
- Cyber security management was obsolete.
- Threat detection and incident response was missing.
- The company experienced multiple log-in failures.
- Anti-virus and malware protection were not up to the mark.
- Patching for majority of the machines were out of date.
- Most spyware threats went undetected.
- User accounts were locked out and malfunctioning.

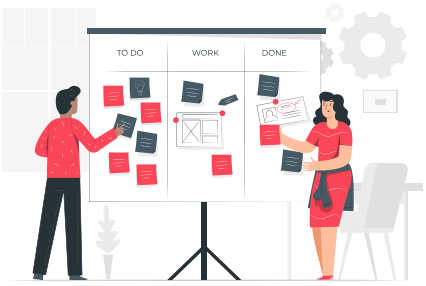
Skillmine Solution

- Undertook a comprehensive study and assessment of the current environment to design and implement a security command center (SOC) for the company.
- Guided & Planned- Defined objectives and requirements that govern the design and use of SIEM.
- Defined, designed, and implemented servers, software, log collectors etc comprising the SIEM system architecture.
- Designed, integrated, and implemented components needed to generate alerts and visibility.
- Defined and managed processes that needed to ensure ongoing support, management and tuning of SIEM.
- Established measurement, reporting and communication capabilities to demonstrate changing state on Security.
- We created a structure for the basics of IT security like patching and login failures and end point.

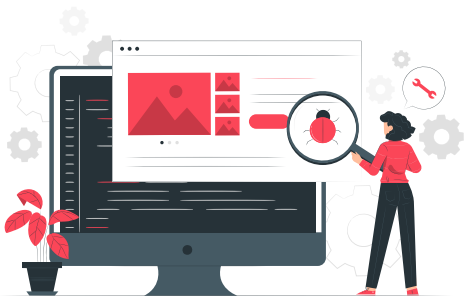
Solution

- Detected threats, vulnerabilities, and malware at the earliest stage.
- Provided advanced technical skills to mitigate security threats.
- Our experts monitor the frequently changing threat scenario and analyze cross-platform threats to offer a wide range of IT security.
- We continuously Improve & Enhance the solution capabilities based on new requirements and gain operational efficiencies.

Execution



- Brought the best practices of security managementto the company, this included educating the distributed IT teams the basics about the management of security.
- We started reporting the number of login failure and the causes, this led to creating a user awareness program of security for the company's application users.
- We tightened the active directory group policies and the self-change password management, so that the login failures could be minimized.
- There was an onsite 24x7 team of Skillmine security experts who would react quickly to threats.

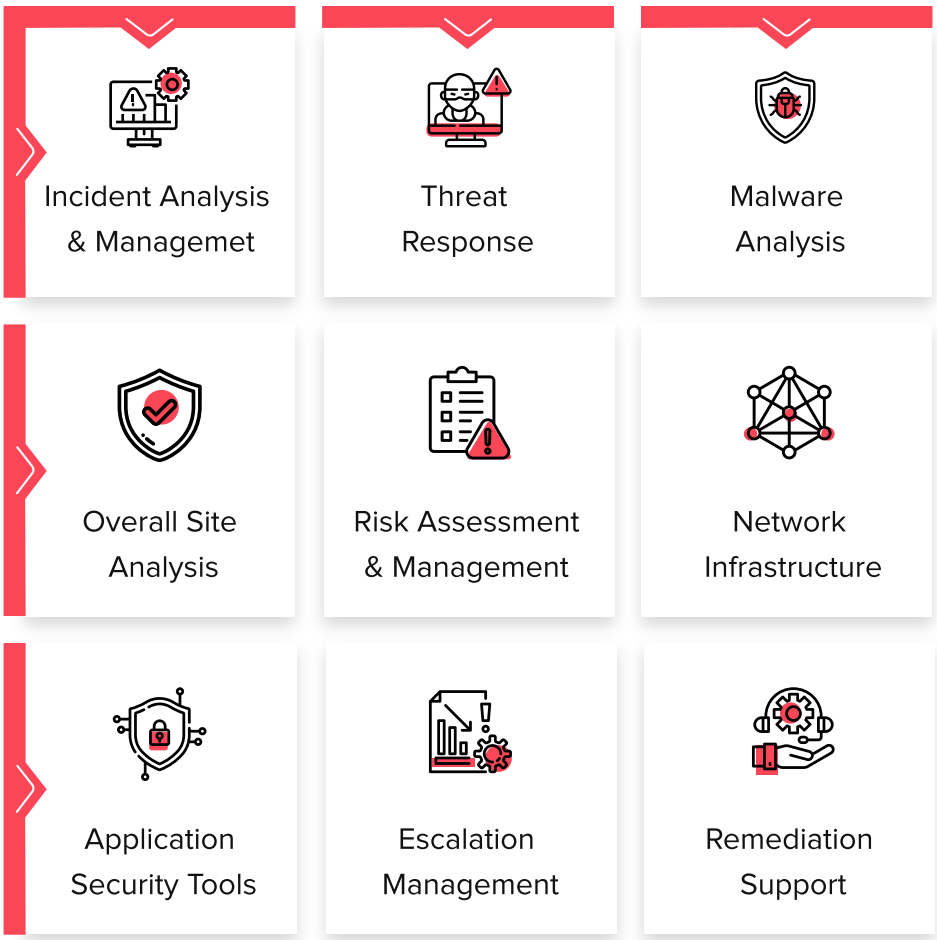


- We were included in the change control board of the company, to cover the security related aspects of change management.
- Every security malware was treated as a major incident, whereby the IT administrative team dealt with the security issues regardless of the time of day. This helped bring more sensitivity towards security awareness and taking security controls more seriously when any new systems were installed of changed.

Data Points

- The overall security environment was made stable and secure over a period of six months.
- The login failures were reduced by 97%.
- Patching was up to date within 3 months across the organization.
- The anti-virus compliance went up by more than 85% in the week+1 scenario and 100% in the month +1 scenario.
- The number of malwares reduced from almost 100 per month and to less than 7 a month.

Capability & Competency



For more information
Contact: info@skill-mine.com
Visit us: skill-mine.com

Skillmine
Technology • Consulting • Services
India | KSA | UK | USA

Stay connected