

| THREAT HUNTING



The Threat Hunting service, offered by VinCSS, is a proactive approach to hunt for and identify signs of intrusion or exploitation within an organization. This service helps organizations and businesses discover ongoing or previously undetected cyberattacks hidden within their infrastructure.





PROACTIVELY HUNT FOR THREATS

The service actively hunts for and analyzes indicators to detect sophisticated cyberattacks that may be lurking within organizations.



ENHANCE MONITORING SYSTEMS

The Threat Hunting service assists organizations in thoroughly reviewing their existing network security monitoring solutions and systems.

01

ENVIRONMENTAL ASSESSMENT

VinCSS collaborates with organizations to understand and clarify their IT environments, gathering necessary information to deploy the service.

02

CHECKLIST DEVELOPMENT

After obtaining insights into the client's IT environment, business context, and related information, VinCSS develops technical checklists to identify potential threats and indicators to hunt and recognize them.

03

CONDUCT HUNTING

Using the checklists created, VinCSS conducts hunting operations and searches for signs of intrusion.

04

ANALYSIS AND EVALUATION

For each completed checklist, VinCSS analyzes and strings together the information gathered to identify threats or enhance the checklists for deeper review.

05

REPORTING RESULTS

VinCSS reports the threat hunting results and provides solutions for remediation.

The Threat Hunting service helps organizations detect sophisticated and concealed threats within their IT environments to promptly mitigate and address them. As a result, this service assists businesses in minimizing damage caused by targeted and advanced cyberattacks, enabling them to timely identify complex security issues within their network monitoring systems and, consequently, enhancing their overall security posture.





DETECTING SOPHISTICATED AND CONCEALED THREATS WITHIN THE ORGANIZATION

VinCSS helps organizations promptly detect and mitigate hidden, sophisticated threats that may never be discovered by traditional security solutions.



PROVIDING COMPREHENSIVE INFORMATION ABOUT ONGOING AND PAST ATTACKS WITHIN THE ORGANIZATION

Through threat hunting campaigns, businesses gain a holistic view of the tactics, techniques, and procedures employed by threats that have targeted or are currently targeting the organization.



ENHANCING SECURITY SYSTEMS AND NETWORK MONITORING

Threat hunting activities assist organizations in timely identifying and addressing vulnerabilities in their security systems and network monitoring infrastructure, ensuring readiness against sophisticated targeted attacks.



EXPERIENCED TEAM

VinCSS boasts an experienced team of experts and engineers who have acquired numerous reputable cybersecurity certifications such as SANS and EC-Council. The team continuously hones their skills in various industries within a leading diversified corporation in Vietnam, including Automotive, Healthcare, Retail, Real Estate, Mobile device manufacturing, Technology, and Education.



EXTENSIVE CYBERSECURITY KNOWLEDGE REPOSITORY

Thanks to its diverse customer base spanning multiple sectors, including high-tech industries like Automotive, VinCSS has the opportunity to encounter and confront a wide range of cybersecurity threats daily. This experience enables VinCSS to build a vast repository of cybersecurity knowledge, which greatly supports its cybersecurity services. The repository includes tailored indicators of compromise (IoCs) specific to different threats and industries.

THANK YOU!

- Floor 20A, Vincom Center Dong Khoi Building,
No 45A Ly Tu Trong Street, Ben Nghe Ward, Dist. 1, HCMC, Vietnam.
- Email: sales@vincss.net • Website: www.vincss.net

