OU Intelligence

Advanced cyber intelligence service

30 Poltavskaya St, P2,, Nizhny Novgorod, 603089, Russia

octounit.ru/en

info@octounit.ru

2026

About us

A team of experts engineering adaptive cybersecurity defence technologies

Our mission

01

To act proactively and ensure cyber-immunity for our clients

Our team

02

We are cybersecurity professionals with 10+ years of experience in major international corporations. Our core competencies include SecOps, Threat Intelligence (TI), Incident Response (IR), Red Teaming, and DevOps

Our Approach

03

Our solutions are built upon extensive experience with existing market products and the development of proprietary platforms

300
Pentest projects delivered

5000
Monthly threats analyzed

100+
Sources under continuous monitoring, including Dark & Deep Web

~100
Monthly incidents registered

95+
Engagements delivered

15
min response time for OU Intelligence services

25+
Industries successfully covered

Customer industries

Banking | SIS | Telecommunications | Insurance | IT | Healthcare

Services provided

Security assessment

- Web services
- Mobile applications
- Infrastructure
- Source code

Secure Software Development

- End-to-End Implementation
- Strategy development
- Vulnerability Management process design
- SAST implementation

Attack Simulation

- External Pentesting
- Phishing

SOC Consulting

- L1 & L2 as a Service
- SOC evolution strategy
- Process auditing
- Custom detection rule development

Our products

OU Intelligence

Threat Intelligence

Security assessment and continuous security monitoring service

Comprehensive end-to-end application security analysis

OU ASOC

Secure Development

Legacy Threat Intelligence Services

ASM

Attack Surface Management

Assessment and monitoring of the attack surface, identification of basic threats and misconfigurations in digital assets

- IP Address
- Domain
- Mobile application
- Open network port
- Authentication form
- Email address
- Employee resumes, etc.

DRP

Digital Risk Protection

Early warning of cyberattack preparation, fraud, information leaks, and Darknet mentions

- Cashback fraud
- Database sales
- Service requests
- DDoS attack
- Employee correspondence leaks
- Illegal provision of services on behalf of the Customer, etc.

CPT

Continuous Penetration Testing

Automated vulnerability infrastructure scanning

- Lack of security updates
- Weak accounts
- Insecure configuration
- Vulnerability in the code
- 1Day / 0Day vulnerabilities

Legacy Threat Intelligence Services

ASM

Attack Surface Management

Assessment and monitoring of the attack surface, identification of [illegible] misconfigurations in digital assets

- IP Address
- Domain
- Mobile application
- Open network port
- Authentication form
- Email address
- Employee resumes, etc.

DRP

Digital Risk Protection

Early warning [illegible] separate [illegible] and Da[illegible]

- Cashback fraud
- Database sales
- Service requests
- DDoS attack
- Employee correspondence leaks
- Illegal provision of services on behalf of the Customer, etc.

CPT

Continuous Penetration [illegible]

[illegible] ability [illegible] scanning

- Lack of security updates
- Weak accounts
- Insecure configuration
- Vulnerability in the code
- 1Day / 0Day vulnerabilities

What if we combine several products in one solution?

OU Intelligence

CONSISTS OF

3

COMPLEMENTARY MODULES

ASM

Digital Asset* Discovery

Continuous monitoring of digital assets related to the company or brand, using various analytical methods, including data enrichment through DRP, to maintain accuracy and relevance of information about digital footprint and reputation

Monitoring of Digital Asset Changes

Situational awareness with all the latest changes regarding your digital assets, enabling quick responses to any changes and effective management of your brand's reputation and presence in the digital space

Digital Asset Management

Efficient asset lifecycle, including the ability to manually add data, enrich information with context, as well as prioritize and categorize assets to optimize monitoring and analysis processes, enabling more accurate and faster decision-making

* Digital assets – domains, subdomains, associated domains, SSL certificates, websites, IPs, ports, DNS records, technologies, mobile applications, social media accounts, perimeter devices, cloud services, login forms, etc

DRP

Leaks of source code fragments

Detection of source code leaks in open repositories, Pastebin-style services, and other sources

Detection of phishing resources

Detection of phishing domains and monitoring of suspicious web assets

Leaks of accounts and client databases

Monitoring for compromised credentials of employee accounts, protecting sensitive information, and customer data

Detection of fake mobile applications

Ensuring the security of your B2B clients and partners from malicious and counterfeit mobile applications

Monitoring of mentions of C-level executives

Detection of negative mentions and monitoring of information about top executives (C-Level)

Blocking fraudulent resources

Initiating requests to block fraudulent and suspicious websites

Monitoring of social media and news

Detection of disinformation and negative publications/news, as well as fake accounts. Search for original sources

Mentions in the Dark & Deep Web

Detection of mentions (preparation for attacks) or leaks of confidential data in the darknet, deep web, and hacker communities

CPT

Vulnerability assessment

Identification of vulnerabilities related to network resources, web applications, SSL/TLS, mobile applications, third-party libraries, mail servers, DNS, and other components

Detection of misconfiguration

Identification of errors related to networks, web applications, SSL/TLS, mobile applications, third-party libraries, mail servers, DNS, and other components

Automated penetration testing

Application of methods and approaches used by hackers to attempt unauthorized access to infrastructure

On-demand penetration testing

Option for regular requests to conduct manual penetration testing

OU Intelligence can be useful

01
CISO

02
AntiFraud Team

03
Security Infrastructure Team

04
Incident Response Team

05
Vulnerability Management Team

Customer Industries

- Critical Infrastructure and Government Sector
- Financial Sector and E-commerce
- Healthcare Sector
- Information Technology and Digital Economy
- Manufacturing and Logistics
- Retail and Consumer Services

Email/Messenger

We send alerts to a specified email or the preferred messenger

Deliverables

We prepare a package of documents based on the service delivery results

SIEM/SOAR/ Ticketing

We can configure alert delivery to a designated SIEM collector or a specified API endpoint

Custom Integration

We will develop an integration tailored to your needs

What do you get in the end?

Delivery Methods	
1	Direct Delivery
2	Integrator
3	White Label

Implementation Results

+40%

VISIBILITY
of real attack surface

Early

ALERTS
on attacks and suspicious activities

89

INSIDERS
identified during piloting phases

Report

CUSTOMIZATION
for the customer

100K+

ASSETS
with scalability

5K+

LEAKS
identified before attackers and regulators

324

ATTACKS
were prevented due to early warnings about their preparation

Our advantages

Unified solution

This synergistic, all-in-one platform seamlessly integrates External Attack Surface Management (EASM), Digital Risk Protection (DRP), and Continuous Penetration Testing (CPT) into a singular, cohesive operational framework

Customer adaptability

Customizable modules, reports, integrations, role-based model, asset management by companies and projects

Integration Features

Presence of RESTful API and GraphQL for integration with SIEM, IRP, SOAR, and enterprise systems, as well as the ability to send notifications via email/messengers

Flexibility and Scalability

Thanks to its proprietary platform and core, the service adapts to the specifics of any business and holding structure

Expert team

24/7 support and provision of recommendations from OU Expert Team

Try Our Service – It's Easy!

01 Fill out the form below or email us at info@octounit.ru

02 We'll demonstrate our service and answer your questions

03 Fill out a short questionnaire about your company/brand

04 Enjoy a free 1-4 week pilot to test our solution

05 We will provide a cost calculation tailored to your requirements

info@octounit.ru
octounit.ru/en

Contact Us

We look forward to providing further information regarding our company, products and services.