CYREN

Cyren Incident Response Service (CIRS)

Use Cyren's expert services to give your Office 365 users and admins peace of mind

For security teams who are swamped with cyber alerts and struggling to investigate and resolve threats, Cyren Incident Response Service (CIRS) is ready to step in and shoulder that burden for you. With CIRS consultants constantly on the lookout for suspicious emails, mailbox anomalies, and cyber trends, you can assure fast and effective response to malicious attacks that threaten your Office 365 users and your business.

Even evasive phishing attacks that are always changing their stripes and trying new methods are no match for our team of CIRS experts. Typically, by the time before your IT team is free to look at a suspect email, CIRS will have already investigated and resolved the incident and initiated the proper response. Moreover, we leverage our experience with myriad cyberattacks across numerous organizations and industries to help you understand the big picture of attack vectors threatening your business, while making sure that reported incidents are taken care of immediately and security breaches can be prevented.

How does Cyren do it? In a word, expertise.

Expertise Expedites Response

CIRS is a 24/7 managed service for users of Cyren Inbox Security. Our threat response experts are laser-focused on investigation, analysis and resolution of the threat incidents reported by your Office 365 mailbox users, as well as investigation of suspicious low-confidence incidents detected by the CIS system.

We leverage our unsurpassed threat visibility and Cyren's purpose-built toolset to take the burden off your IT staff and provide peace of mind regarding Office 365 security. Our global security cloud processes 25 billion email and web security transactions every day; identifies 9 new threats and blocks over 3,000 known threats each second. Cyren garners experience and expertise with every incident we investigate and resolve. We've seen it all, and then some. While we leverage global visibility and crowdsourced intelligence to the advantage of every Cyren Inbox Security user worldwide, CIRS security analysts are dedicated to responding to the reported incidents from your organization and resolving them quickly.

Is the Threat Real?

When a Cyren Inbox Security user clicks the red PhishScan button to report a suspect email, it can fall into one of three categories:

- Phishing threat detected by CIS, but shouldn't be
- Phishing threat not detected by CIS, but should be
- Nuisance email (not a security threat per se, but unwanted or nuisance emails)

Each threat report is immediately investigated and verified by CIRS experts to determine if the reported threat is real or not. Validated threats may trigger an automatic rescan and remediation of all mailboxes to eradicate a phishing attack for example. When a reported threat is not valid, the incident is immediately resolved and closed.

CYREN INBOX SECURITY

Cyren Inbox Security is an Inbox Detection and Response (IDR) solution that allows organizations to establish a critical layer of email security at the inbox and strengthen overall security posture.

INCIDENT RESPONSE SERVICE

With Cyren Incident Response Service, our expert security analysts become an integral part of your Office 365 security team. The managed service operates round-the-clock, 24/7, as Cyren security experts stand ready to verify and respond to suspect emails, every time an employee clicks the Cyren's red PhishScan button.

EXPERT THREAT ANALYSIS

It pays to have an expert pair of eyes watching out for your security. Cyren Incident Response analysts bring a wealth of cybersecurity expertise and know-how that cannot be matched by automated, machine-learning investigation.

CIRS HELPS YOU:

- Relieve the SOC team from time-consuming and stressful threat investigation and response
- Bring cyber expertise and resources to your SOC through Cyren managed services
- Reduce alert backlog and fatigue
- Assure employees receive a timely response to their PhishScan reports
- Detect changing evasion tactics as attackers pivot and try new techniques
- Assure every threat is handled and none fall through the cracks

25B
Security Transactions Daily

1.3B
Users Protected

300M
Threats Blocked Daily

Make Every Case Open-and-Shut

Every day, Cyren Incident Response Service (CIRS) analysts investigate and remediate numerous incidents, like these:

PHISHING ON SHAREPOINT

- Employee clicks PhishScan on suspect email.
- CIRS verified phishing that was using URL accessed from a file open in company SharePoint.
- Phishing URL manually blocked. Subsequent attacks detected upon arrival and remediated automatically.

BEVERAGE BRAND GETS PHISHED

- CIRS identifies phishing attack in a specific user account
- The attack is verified within 4 mins and offending URL is blocked in the specific user account and 22 others.
- 8 subsequent attacks detected upon arrival and remediated automatically.
- Global manufacturer; 10,000+ employees.

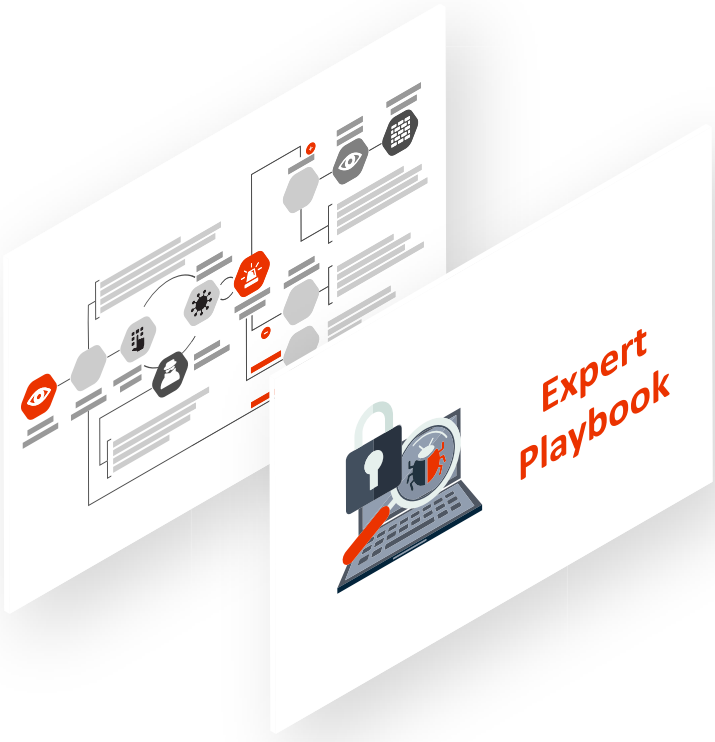
UNIVERSITY GETS SCAMMED

- University user requests PhishScan on email with suspect body and sender.
- CIRS identifies marketing scam sent repeatedly to all university employees. Not a phishing threat, but a nuisance scam.
- Sender blacklisted while IOCs are fed back into CIS AI detection engine
- 450+ accounts remediated. Subsequent scam emails (new sender address) detected on arrival and remediated automatically.

COMPROMISED ACCOUNT

- Employees receive strange email from “Microsoft Outlook HelpDesk” with a malicious URL
- Cyren Inbox Security detects phishing and puts a warning banner on the email
- CIRS identifies attack sent from legitimate user account that is compromised
- CIRS notifies customer security team about compromised account.

Cyren Expert Playbooks Automate and Accelerate Incident Response



CIRS playbooks orchestrate and automate the investigation and response to every type of phishing threat your Office 365 users encounter:

1. Analyze the cyber incident to uncover the scope of the attack
2. Identify and report potentially compromised data and its impact
3. Establish requirement(s) for a full forensic investigation
4. Develop a remediation plan based on the scope and details of the cyber incident
5. Remediate and report case closed
6. Send post incident report to admin