

MANAGED ENDPOINT DETECTION & RESPONSE

FOR SMBs, SMEs & MSPs



DETECTING AND RESPONDING TO THREATS

The increasing number of data breaches and successful ransomware attacks have concerned IT and business leaders across the globe. With all the technology and expertise at hand, why do companies continue to fall victim to cybercrime? Whilst defences can always be augmented, many organisations are simply overwhelmed by the volume and sophistication of attacks. Other organisations cannot afford the technology and deep expertise required to detect and respond to threats.

Another ongoing problem lies in staffing – organisations make significant investments in cybersecurity technologies only to find they do not have the time and/or skills required to adequately operate the technology to detect and respond to threats. Even the most sophisticated protection, detection and response technologies require human oversight. To bridge this gap, organisations often purchase Managed Endpoint Detection & Response (MEDR) services.

CONTINUOUS CYBERSECURITY OVERSIGHT

Utilising a best-in-class technology platform, First Response can provide a fully-managed or co-managed endpoint detection & response service.

Knowing First Response is continuously monitoring your environment and extending the capabilities of your team provides tremendous relief in the uncertain world of cybersecurity. As a client, First Response provides you with a broad range of proactive and ad-hoc services to ensure you're always protected and any questions or concerns you may have are addressed.

Following are examples of how First Response's team assists clients detect, investigate and respond to threats, as well as continually inform clients of important security-related updates and provide on-demand expert advice and assistance.

DETECTION

24x7 Monitoring, Analysis and Proactive Outreach

The First Response team, continuously monitors your environment – every hour of every day throughout the year. The team manages events, alerts, customer inquiries and incidents. The team also provides alert analysis and correlation to other alerted events.

The team will proactively contact you when certain alerts or events are detected along with details on the actions that have been taken. This type of outreach falls into three general categories each requiring different response actions.

Internal Activities

Includes a summary of the alerted event(s) and a description of their flow whilst implementing Whitelisting or Exclusion profiles.

Suspicious Activities

Includes a summary of the alerted event(s) and a description of their flow whilst working with your team to analyse the event.

Malicious Activities

Includes a summary of the alerted event(s) and a description of their flow whilst implementing steps for remediation and analysis. In specific “Critical risk” and “High Risk” severity incidents, a First Response analyst will contact you to make sure you’re aware of the incident.

Connectivity & Availability Monitoring

The First Response team cooperates with your internal team to ensure continuous protection and server usability. This includes monitoring abnormal PCQ sizes of any protected environment to help evaluate the environment's activity load. In case connectivity is lost, First Response will immediately reach out to remediate any connection disruptions.

Dear team,

We are sending this email to inform you that it appears that there is no network communication between one or more of you EPS agents and our Virtual Private Cloud.

Please follow this checklist to make sure that they system is working properly and please reply with answers to all of the tests.

It is important to maintain connectivity in order to provide you with the maximum protection possible.

Implementing New Detection Mechanisms

The First Response team is continually researching and analysing new attack techniques to develop and implement protection and detection mechanisms in the platform.

Proactive Threat Intelligence and Hunting

The First Response team continually searches for new emerging threats in order to implement IOCs and patterns into the platform. These proactive actions enable the platform to collect, analyse and alert for events while giving forensic details to the risk level.



✓ SC-SOC

To: ● All team

Subject: High Risk – PowerShell Malicious Command – Main Server

We have detected **Emotet** activity on this host.

The following command has been launched:

New Ransomware Variations

Ransomware variants are analysed by First Response analysts for specific identifiers which are implemented into the platform detection mechanisms.



✓ SC-SOC

To: ● All team

Subject: Data Breach

I have acquired part 01 of the **** data breach lake, from the official site of the ***** ransomware operators.

After downloading the archive (11GB) – I have validated the files and they are indeed related to *****.

The documents have the ****logo and worker names are signed on them.

Please forward the attached photos to the client, and lets schedule a session to present our findings.

Sample email to new client during incident response engagement

SSDeep Implementation

The platform detects file hashes (SSDEEP) which are highly similar to file hashes that are flagged in our threat intelligence database as malicious. This alert is used to detect new variants of known malware.

Netwalker Meta_Data	
MD5	993b79fjkj39803hjks0347jdskkuryh393498jhf
SHA-1	6fd3947sdja2340daj340-90klfskg0oljppoerh937343434
SHA-256	6fd3947sdj hjks0347jdskkuryh
Vhash	0940566513f4098345907z lz
Authentihash	hjks0347jdskkuryh40983452340daj3 ldfskg0oljppoerh937sdfsd
Imphash	sd ldfskg0oljppoerh9373434
SSDEEP	1536:NQVICPQEIORKSRKLJhe82POuerlknbtTYkl;sdj kf93khlkdsfg3KJH UIEWR340
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	94.00 KB (96256 bytes)

Example of SSDEEP hash included with NetWalker metadata

Memory Patterns

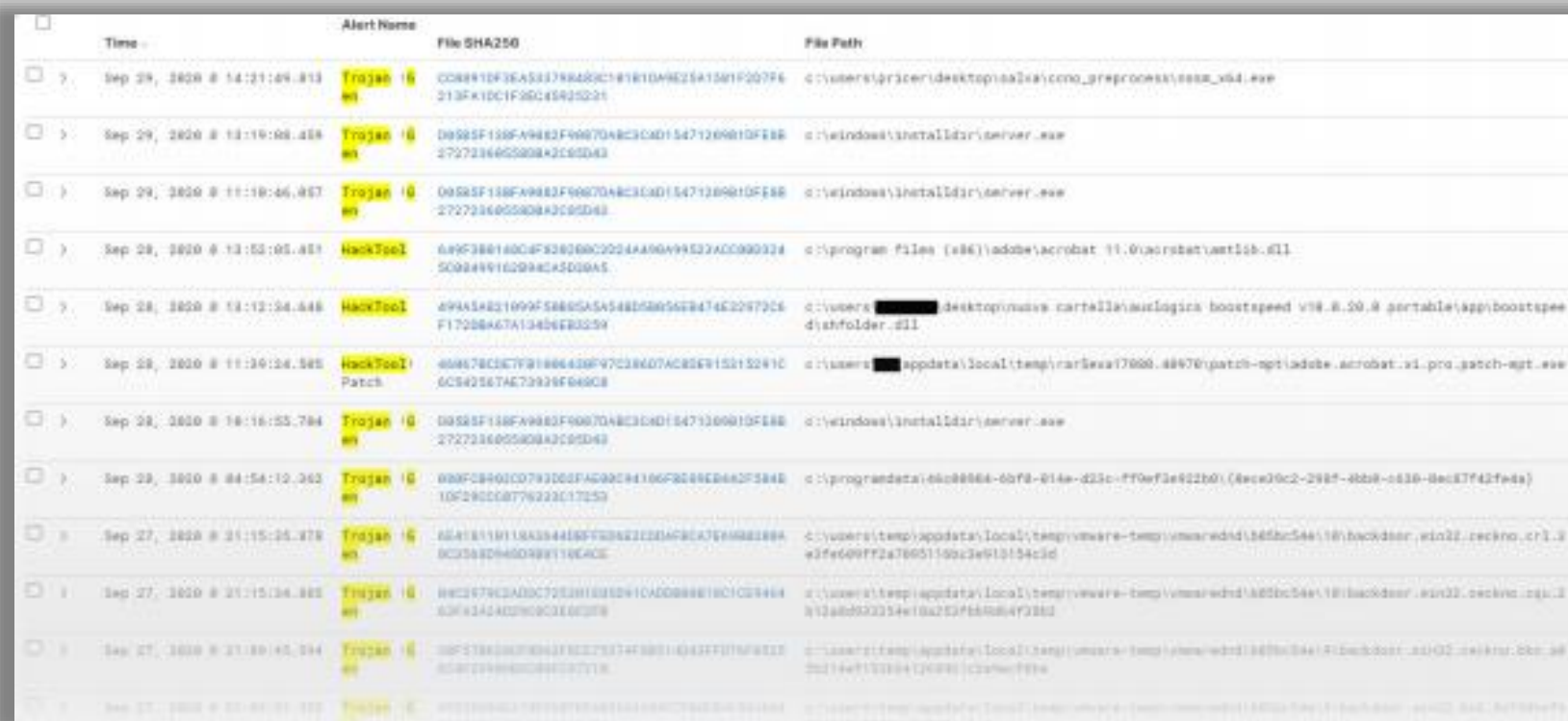
The platform can detect a ransomware process by analysing, identifying and matching malicious memory patterns.

Alert Notification	
Action	Blocked
Severity	Critical
Category	Memory Pattern – Ransomware (Netwalker)
File	C:\window\syswow64\explorer.exe
Description	This file contains malicious code

Example of memory pattern matching alert notification

File Classification

Files seen by the platform are classified per file type, including numerous values indicated in the console for forensic purposes. Any files classified as malicious also create a trigger with the incident mechanism, which opens an event in the console, showing the details of the incident (Hostname, SHA256, and more).

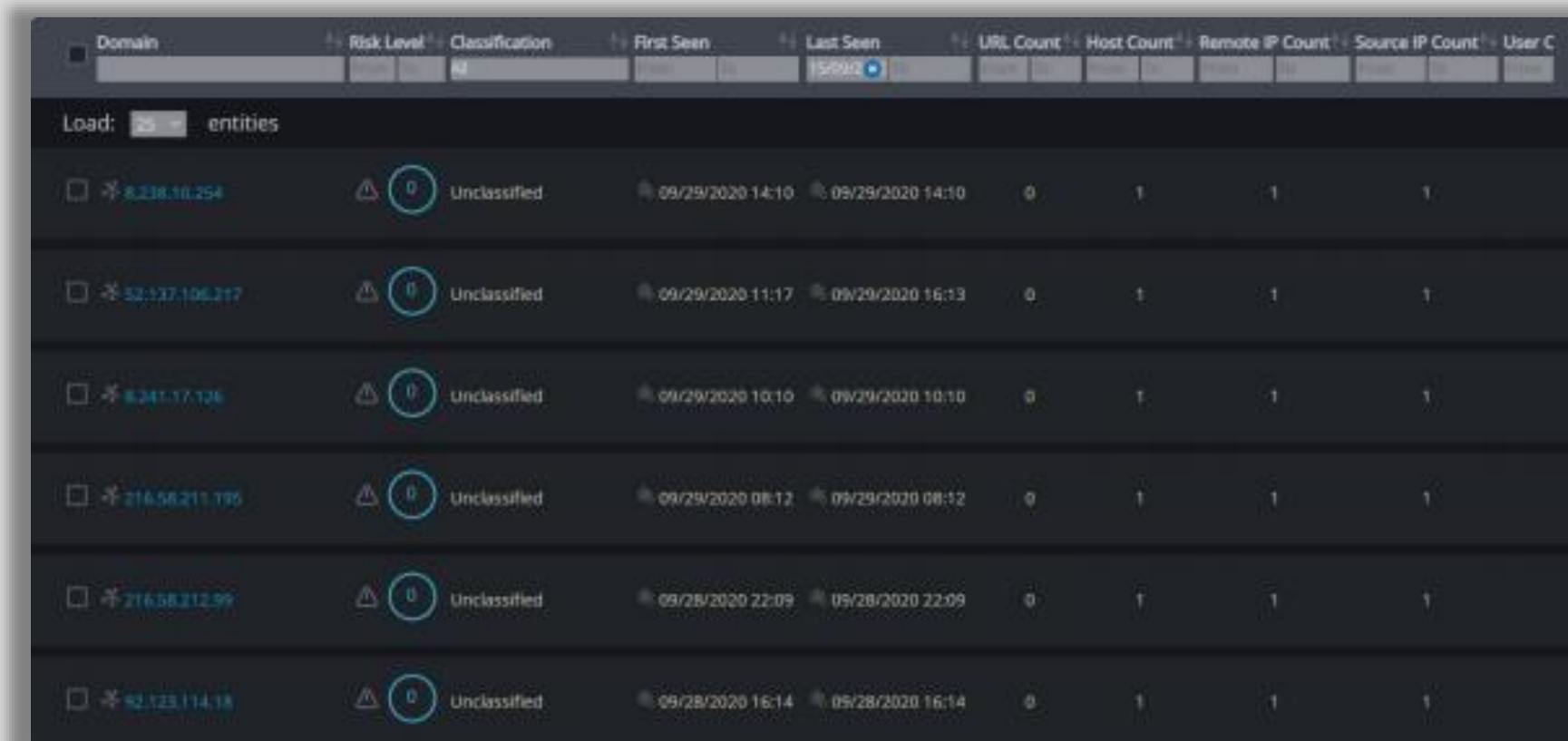


Time	Alert Name	File SHA256	File Path
Sep 29, 2020 @ 14:21:09.813	Trojan en	008810F3E533786483C181810A9E25A1361F207F6 213F81DC1F30C45925221	c:\userstgr3ceridektop\sa\sa\cno_greprocess\sesa_vd4.exe
Sep 29, 2020 @ 13:19:08.458	Trojan en	D892F138F4982F6670A8C3CAD15471269810F188 2727360580843C95D43	c:\windows\installer\server.exe
Sep 29, 2020 @ 11:19:46.867	Trojan en	0082F138F4982F6670A8C3CAD15471269810F188 2727360580843C95D43	c:\windows\installer\server.exe
Sep 29, 2020 @ 13:52:05.851	HackTool	649F3881A0C4F838309C2024A90A99523A0C900324 508499162994045D08A5	c:\program files (x86)\adobe\acrobat 11.0\acrobat\actlib.dll
Sep 28, 2020 @ 13:12:34.448	HackTool	49A54821099F58805A54548D5865628474C22972C6 F17088A67A1348683259	c:\users\██████████\desktop\masa cartalla\auologica boostspeed v18.8.50.8 portable\app\boostspee distfolder.dll
Sep 28, 2020 @ 11:30:34.585	HackTool Patch	468678C3E7F91886438F97C38607AC825F15215241C 6C84567AE7993F84908	c:\users\██████████\appdata\local\temp\rar5wa17660.48476\patch-opt\adobe.acrobat.xl.pro_patch-opt.exe
Sep 28, 2020 @ 18:16:55.784	Trojan en	D892F138F4982F6670A8C3CAD15471269810F188 2727360580843C95D43	c:\windows\installer\server.exe
Sep 28, 2020 @ 04:54:12.362	Trojan en	090F0901C0793D0FAC90C84166F3046C862F384E 10F280C08776233C17253	c:\programdata\eko8886-6b78-814e-d33c-ff0e73e922b0\{8eca9c2-298f-4bb8-c838-8ec3742fe4e}
Sep 27, 2020 @ 21:15:25.378	Trojan en	65418119119A354483F73622323MFC8A76A88288A 6C3582D4480489118C40C	c:\users\temp\appdata\local\temp\vmware-temp\vmware\rd1365bc54e18\backdoor_win32.ockno.cr1.3 e3fe69ff2a7865159c3e913154c3d
Sep 27, 2020 @ 21:15:34.882	Trojan en	88C2F79C3A0C72331183E291CADD888818C1C0944 63F43428D960C8E807718	c:\users\temp\appdata\local\temp\vmware-temp\vmware\rd1365bc54e18\backdoor_win32.ockno.cr1.3 9138852354e18a253f8a8b4738d
Sep 27, 2020 @ 21:10:45.044	Trojan en	38F23808078042F82275374F38514342F079F822F 638F299860C080037718	c:\users\temp\appdata\local\temp\vmware-temp\vmware\rd1365bc54e18\backdoor_win32.ockno.cr1.3 2d14e1f13284126381c2a8e1f8e
Sep 27, 2020 @ 22:01:01.022	Trojan en	47C23994217892F84653488C7942348154484 63F43428D960C8E807718	c:\users\temp\appdata\local\temp\vmware-temp\vmware\rd1365bc54e18\backdoor_win32.ockno.cr1.3 9138852354e18a253f8a8b4738d

Example of malicious file classification

Network IOC Classification

Network IOCs seen by the platform are classified by risk type, including numerous values indicated in the console for forensic purposes. Any network IOCs classified as malicious also create a trigger with the incident mechanism, which opens an event in the console, showing the details of the incident (Hostname, domain, and more).



The screenshot displays a console interface for network IOC classification. At the top, there are several columns for sorting: Domain, Risk Level, Classification, First Seen, Last Seen, URL Count, Host Count, Remote IP Count, Source IP Count, and User C. Below the sorting options, the console shows a list of entities. The first row indicates 'Load: 25 entities'. The table below lists six IP addresses, each with a checkbox, a risk level indicator (a triangle with a '0' in a circle), a classification of 'Unclassified', and various counts for URLs, hosts, remote IPs, and source IPs. The 'Last Seen' column shows timestamps for each entry.

Domain	Risk Level	Classification	First Seen	Last Seen	URL Count	Host Count	Remote IP Count	Source IP Count	User C
<input type="checkbox"/> 8.238.10.254	0	Unclassified	09/29/2020 14:10	09/29/2020 14:10	0	1	1	1	
<input type="checkbox"/> 32.137.106.217	0	Unclassified	09/29/2020 11:17	09/29/2020 16:13	0	1	1	1	
<input type="checkbox"/> 8.241.17.126	0	Unclassified	09/29/2020 10:10	09/29/2020 10:10	0	1	1	1	
<input type="checkbox"/> 216.58.211.195	0	Unclassified	09/29/2020 08:12	09/29/2020 08:12	0	1	1	1	
<input type="checkbox"/> 216.58.212.99	0	Unclassified	09/28/2020 22:09	09/28/2020 22:09	0	1	1	1	
<input type="checkbox"/> 92.123.114.18	0	Unclassified	09/28/2020 16:14	09/28/2020 16:14	0	1	1	1	

Example of malicious network details

INVESTIGATION

File, Network, Host & User Analysis

First Response will conduct ad-hoc analysis for any suspicious activity, files or processes. Working with your team to validate and triage potential threats within the environment.

Attack Investigation

Deep-dive into validated attack bits and bytes to gain the full understanding of scope and impact, providing you with updated IOCs and attack reports.

RESPONSE

Whilst the platform includes automated remediation actions, we can always work with you to create more complex, custom orchestration and response actions across the environment.

Full Remediation

Conclusion of investigative attacks entails concrete detail on which endpoints, files, users and network traffic has been remediated.

RESEARCH REPORTS

The First Response team shares regular updates and reports to keep you informed of new attack and protection techniques.

Attack Investigation

Deep-dive into validated attack bits and bytes to gain the full understanding of scope and impact, providing you with updated IOCs and attack reports.

CONCLUSION

An effective cybersecurity strategy requires a combination of technology along with human oversight and expertise. The First Response team ensures the technology platform is deployed, configured and optimised correctly, whilst continuously monitoring your environment, proactively remediating and responding to security incidents.

Whether your organisation lacks security expertise, or the necessary time and staff to implement a full 24/7 monitoring service - First Response can help bolster your team and expertise in the ongoing fight against cybercrime.

<https://first-response.co.uk/>

ABOUT FIRST RESPONSE

Established in 2013, First Response is a cybersecurity, digital forensics, and incident response company. Working with SMBs, SMEs & MSPs to protect their organisations and accelerate cybersecurity maturity. This is through outcome-focused consultancy and services incl. managed cybersecurity services (endpoint, network, mobile & cloud), and secure infrastructure design.

Our technical specialists comprise respected security and investigative professionals from a diverse set of backgrounds, including police cyber-crime units, the security services & enterprise network specialists.

We are headquartered in London with offices in Manchester and Rome, from where we assist our clients around the world. We also help organisations navigate the complex issues surrounding systems breaches, server compromises and data loss. Working with a wide variety of clients including banks, law firms, energy & manufacturing companies and public sector bodies.

Contact

Email: info@first-response.co.uk

Tel: +44(0) 20 7193 4905

Web: <https://first-response.co.uk/>

| first
response