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.

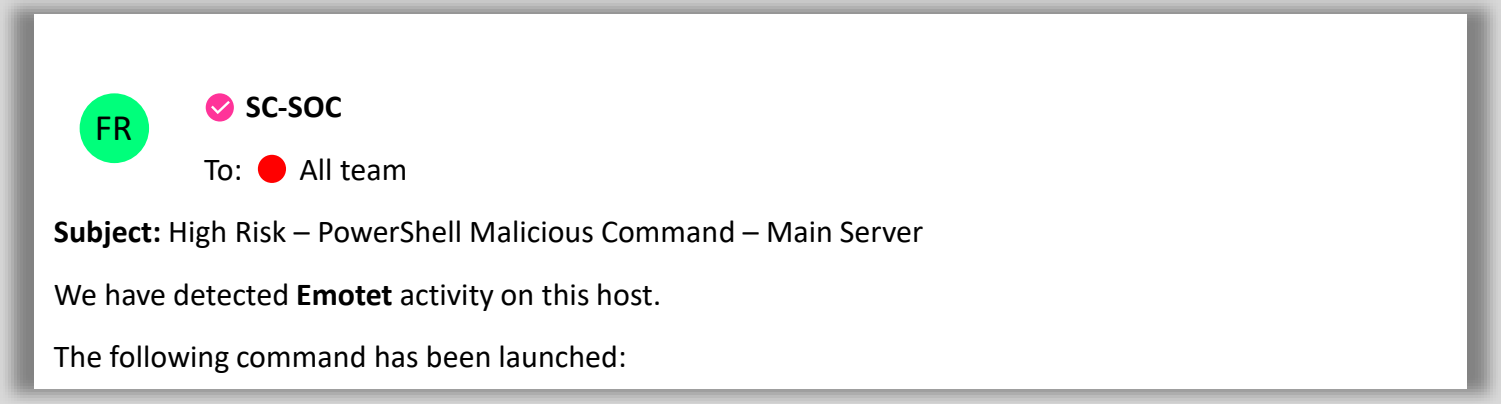
It is important to maintain connectivity in order to provide you with the maximum protection possible.

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.



New Ransomware Variations

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

FR

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	6fd3947sdja2340daj340-90kldfskg0oljppoerh937343434
SHA-256	6fd3947sdj hjks0347jdskkuryh
Vhash	0940566513f4098345907z!z
Authentihash	hjks0347jdskkuryh40983452340daj3 ldfskg0oljppoerh937sdfsd
Imphash	sd ldfskg0oljppoerh9373434
SSDEEP	1536:NQVICPQEIORKSRKLJhe82POuerlknbtTYkl;sdjkf93khlkdsfg3KJH 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

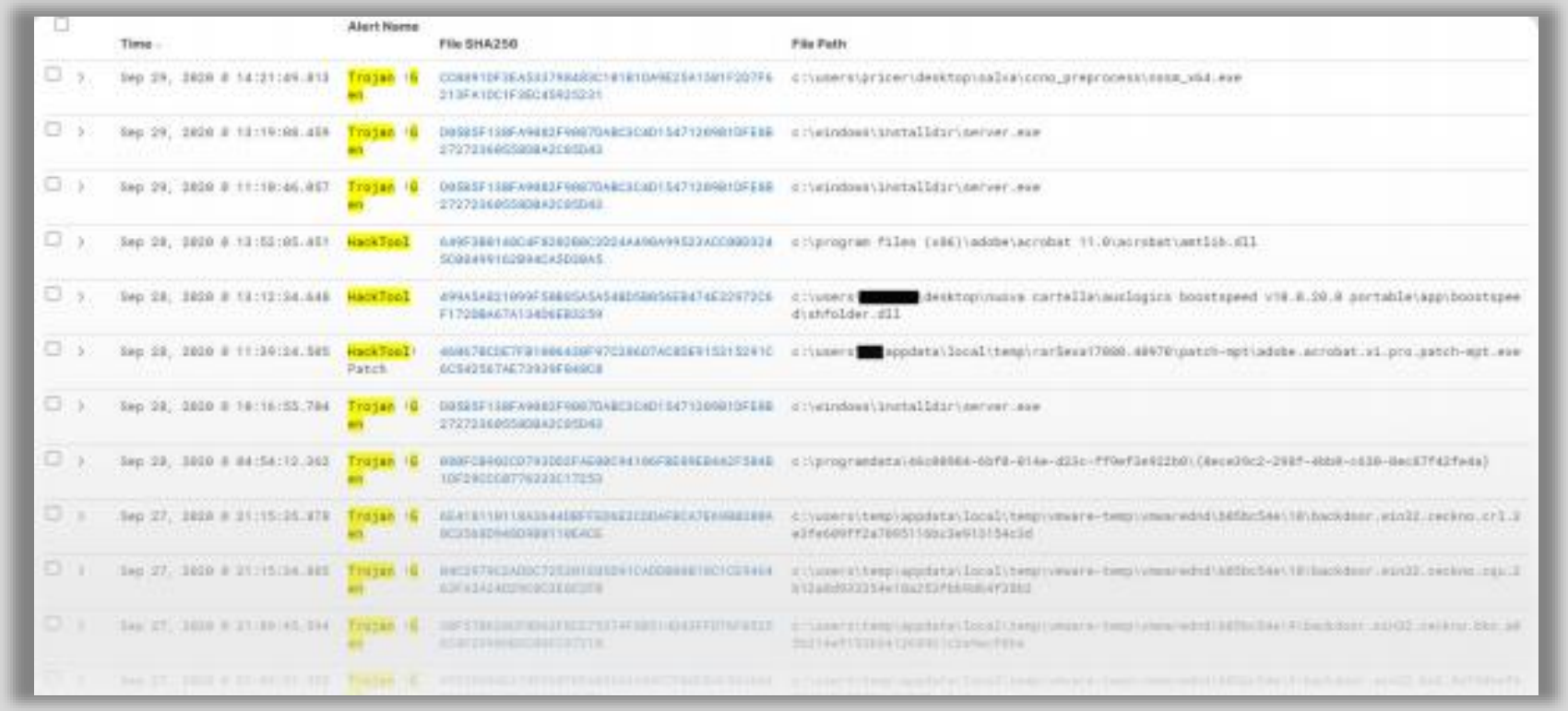
The platform can detect a ransomware process by analysing, identifying and matching malicious memory patterns.

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

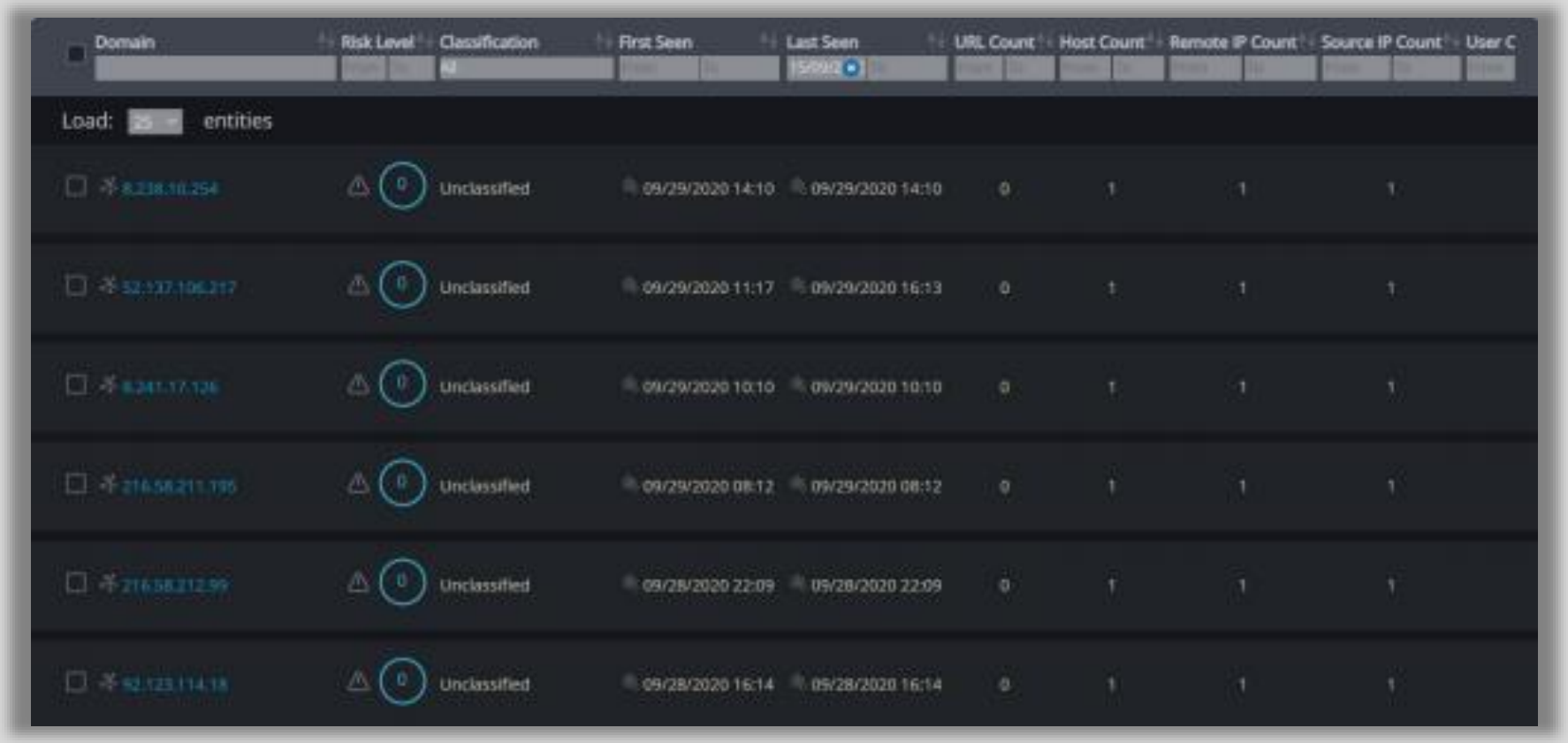
Files seen by the platform are classified per file type, including numerous values indicated in the console for forensic purposes. Any files classified as malicious also create a trigger with the incident mechanism, which opens an event in the console, showing the details of the incident (Hostname, SHA256,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



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).



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