THREAT INTELLIGENCE PRIMER

OCT 2024

VULNERABILITY MANAGEMENT PRIMER

TABLE OF CONTENTS

INTRODUCTION

In a world where cyber threats evolve at breakneck speed, staying ahead requires more than just strong defences—it demands intelligence. Organisations today face a staggering volume of threat data, often scattered across disconnected systems, making it difficult to detect and understand potential risks in real time. Sophisticated adversaries,rising attack volumes, and limited resources further complicate the picture. Threat Intelligence transforms raw data into actionable insights, empowering security teams to make informed, proactive decisions to protect critical assets and reduce risk.

CYBER THREAT INTELLIGENCE

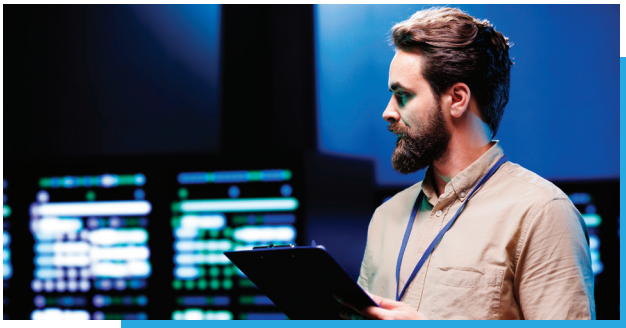
Threat intelligence is knowledge that allows organisations to prevent or mitigate those attacks. Rooted in data, threat intelligence provides context — like who is attacking an organisation, what their motivation and capabilities are, and what indicators of compromise in organisation's systems to look for — that helps security teams make informed decisions.

"Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets. This intelligence can be used to inform decisions regarding the subject's response to that menace or hazard." — Gartner

THREAT INTELLIGENCE CHALLENGES

Some organisations try to incorporate threat data feeds into their network, but don't know what to do with all that extra data, adding to the burden of analysts who may not have the tools to decide what to prioritise and what to ignore.

A proper cyber threat intelligence strategy can address each of these issues. Some of the things to consider while building a cyber threat intelligence strategy are:



- Threat intelligence should be actionable, timely, provide context, and be able to be understood by the people in charge of making decisions.
- Solution that uses machine learning to automate data collection and processing.
- Orchestration capabilities to integrate threat intelligence data with your existing solutions.
- Blueprint to take in unstructured data from disparate sources, and then connect the dots by providing context on indicators of compromise (IoCs) and the tactics, techniques, and procedures (TTPs) of threat actors
- Capability to automate response actions.

Organisations leveraging Threat Intelligence within their security operations and response actions, observe a number of benefits.

Topline Metrics

Overall more efficient IT security teams
32%

3-year ROI
284%

To payback
4 Months

Security Operational Efficiencies

Less Staff time spent compiling security reports
34%

Early identification of threats
10x

Faster resolution of security threats
63%

Risk Reduction

22%
More security threats identified before impact

86%
Reduction in unplanned downtime

$1M
Potential penalties/fines per breach avoided

THREAT INTELLIGENCE AND CYBER FOOTPRINT

To achieve end-to-end visibility of your entire cyber footprint, the threat intelligence solution should be able to automatically collect, analyse, correlate and present enriched threat data across a variety of categories that could impact the business. The data could range from botnets and command & control servers to targeted malware variants; from tracking stolen credit cards and confidential credentials to rogue mobile apps, and hacktivist activities and phishing campaigns aligned against your organisation. Some of the questions to consider are:

- Who is targeting your organisation, and from where?
- Do you know what your presence is on the dark web?
- How has your corporate network been compromised?
- Who is impersonating your brand or VIPs?
- Has sensitive information been leaked out?
- Have credentials been compromised, are they being used to commit fraud?
- Do you know what your compliance liabilities are if you're breached?

THREAT CONTEXT

Data that provides security teams with continuously updated and intuitive information around threat actors, campaigns, IOCs, malware, attack patterns, tools, signatures and CVEs. Instance access to the data so analysts can rapidly gather enriched, contextualised information before, during and after an attack.

DARK WEB

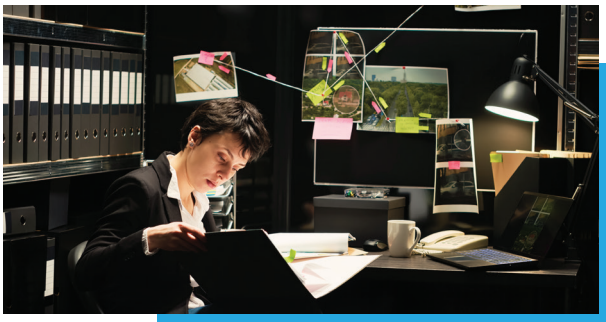
Data that boosts your awareness of what's going on in the underground, observe malicious activities targeting your organisation

CREDENTIALS

Actionable intelligence around leaked, stolen and sold user credentials. Solution should have capability to locate them in real-time on the open, deep and dark web, along with information about relevant malware used to steal the information.

DATA LEAKAGE

Discover if your organisation's sensitive documents and source code have been leaked on the internet, deep web or P2P networks, intentionally or not, such as with shared internal documents with poorly secured file sharing providers.



CREDIT CARDS

Ability to dig deep enough and you can find all sorts of credit card data online. This type of data can dramatically reduce losses from theft and fraud of credit cards.

MALWARE

Detects malware seeking to steal sensitive information or commit fraud. Proactively hunts down targeted malware and ‘Man in the Brower’ attacks, aimed specifically at your organisation.

HACKTIVISM

Monitor global hacktivism activity on social networks and the open and dark web that can affect your infrastructure. Using an advanced early warning system and active geolocator, you should be able generate targeted threat intelligence to shield against potential manually. Ability to detect applications claiming affiliation to your organisation or using company assets without authorization to protect your brand and reputation.

SOCIAL MEDIA

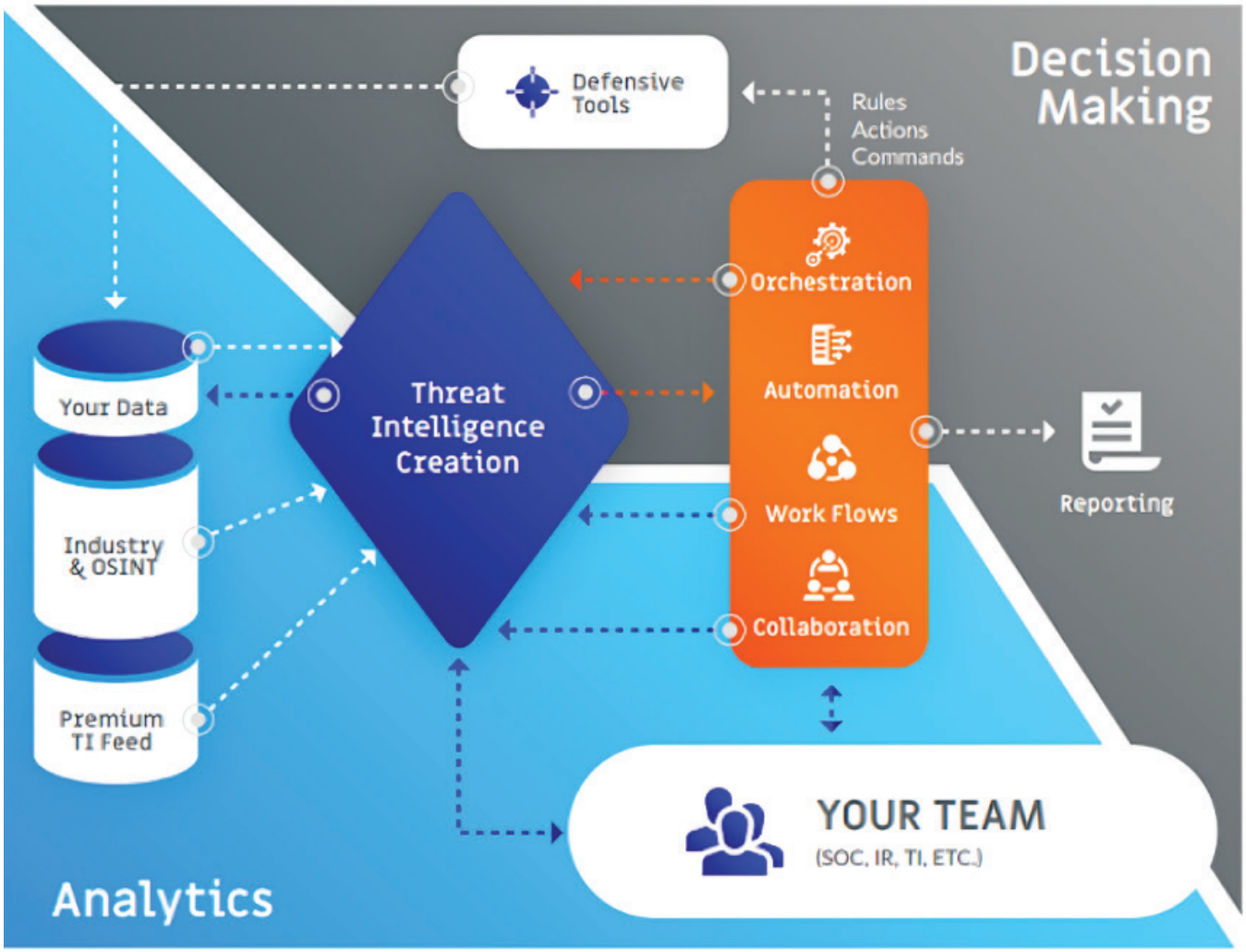
Monitor your organisation’s digital footprint on social networks and search engines. Find websites not authorised to use your brands, logos, assets claiming partnership affiliation assets and more, so you can take proactive steps to shut them down.

DOMAIN PROTECTION

Fraudulent domains are a risk to your organisation and your end customers, with the goal of stealing information or damaging your brand. Combat phishing and cyber squatting by proactively detecting attacks and taking countermeasures.

AUTOMATED THREAT INTELLIGENCE WITH SOAR

SOAR solutions derive several key benefits when connected to automated threat intelligence.



DETECT THREATS EARLIER

Real-time alerts on active and emerging threats drive proactive defense efforts by identifying threats earlier and providing insight into risk sources, relevance, context, and severity. When threat intelligence feed is given into your SOAR solutions, you can be even more proactive in identifying and mitigating threats.

INCREASE SECURITY TEAM EFFICIENCY

Direct access to source material gives IT security teams the context needed to act fast when making remediation decisions — and the confidence that they are taking the right path. This confidence extends to determining how best to proceed with containment, mitigation, and ongoing protection efforts. Integration with a SOAR solution would similarly increase efficiency.

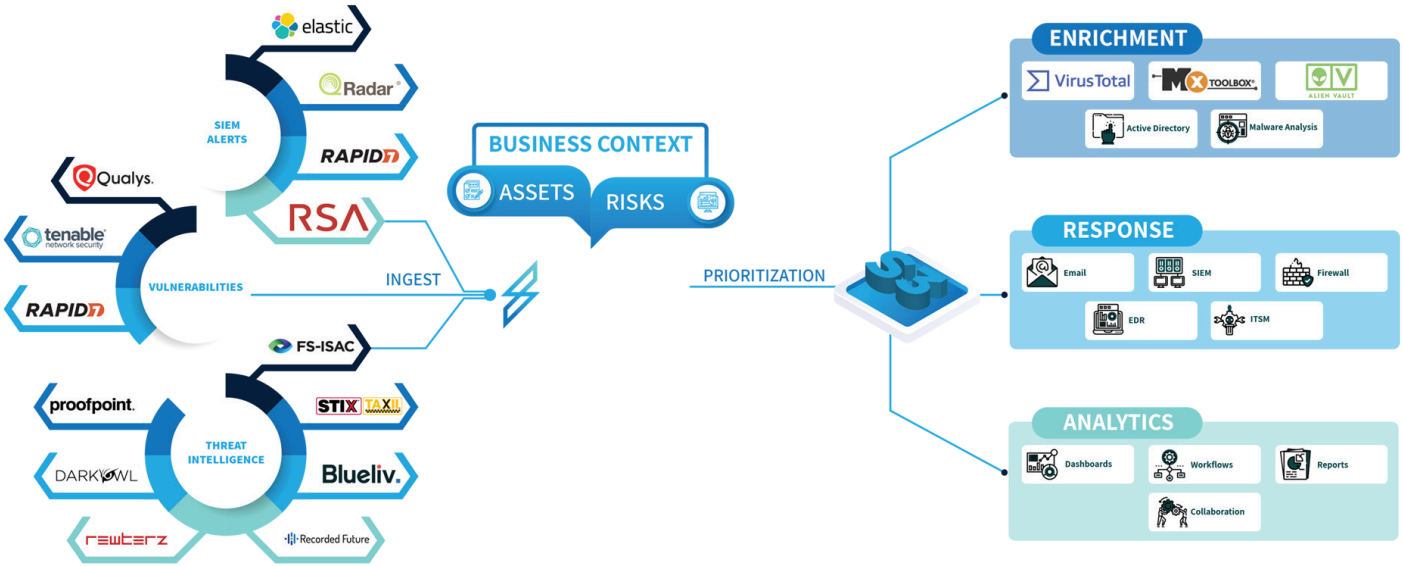
RESOLVE INCIDENTS FASTER

Access to contextualised intelligence replaces manual research that can drain IT resources. SOAR solutions, combined with the right threat intelligence, can resolve incidents faster by reducing research time and improving security team efficiencies. Many IT security teams have improved threat resolution times by 63% after integrating Recorded Future into their workflows — and incident response times would only drop further when incorporating threat intelligence into a SOAR solution.

SIRP – RISK-BASED SOAR PLATFORM

SIRP is a Risk-based Security Orchestration, Automation and Response (SOAR) platform that fuses essential cybersecurity information to enable a unified cyber response. Through a single integrated platform, it drives security visibility, so decisions can be better prioritised and response time is dramatically reduced. With SIRP, the entire cybersecurity function works as a single, cohesive unit.

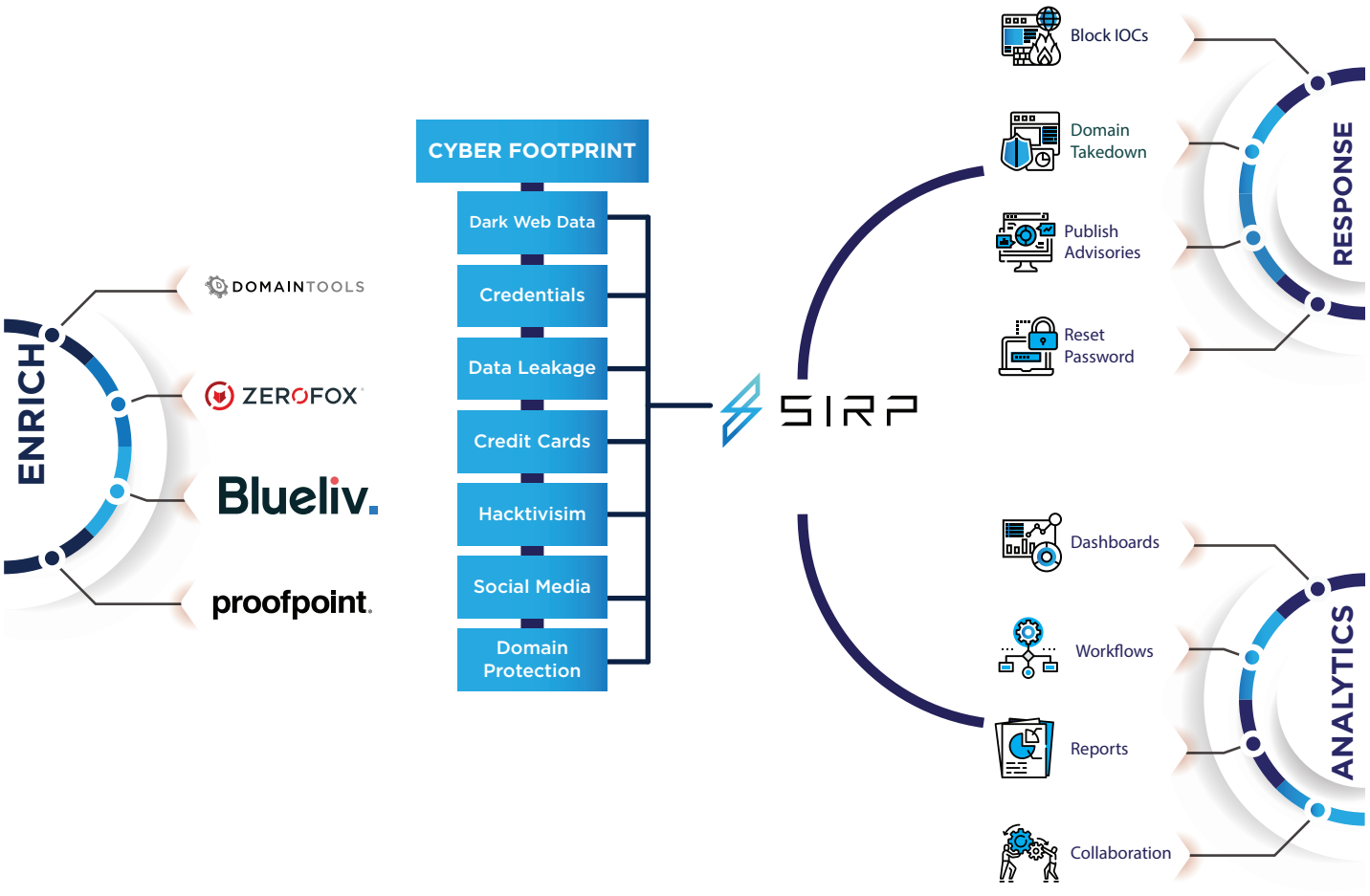
SIRP provides a more dynamic, complete view of incidents, threat intelligence, vulnerabilities, and risks in one place, so you can prioritise and make better decisions faster and respond more effectively. It combines security orchestration, playbook automation and case management capabilities to integrate your team, processes and tools together. SIRP makes security data instantly actionable, provides valuable intelligence and context, and enables adaptive response to complex cyber threats and vulnerabilities.



SIRP provides security teams with instant access to four powerful modules: Incident Management, Threat Intelligence, Vulnerability Management and Risk Management. SIRP Security Score (S3) module makes security data instantly actionable by fusing information from these modules and assessing the risk to the organisation. S3 uses machine learning algorithms to assess security data relevancy and calculate security score. S3 enables organisations to prioritise risks, make better decisions faster and respond more effectively.

SIRP's modular architecture supports more than 200+ applications with coverage of 1000+ APIs, enabling security teams to connect and coordinate complex work-flows across different teams and tools. Powerful abstraction allows security teams to focus on what they want to accomplish, while the platform translates that into tool-specific actions.

SIRP helps organisations implement an intelligence-driven defense by focusing on addressing the fragmentation problem across information, people, technology, and process.



INFORMATION

For relevant information to be refined into usable intelligence, it must be available to be correlated, enriched, and contextualised. You must remove the silos segmenting relevant data by creating a common source of record for it.

SIRP does this by aggregating internal and external information so that it can be refined into intelligence usable for informing decisions. Internally sourced information, details of an IR investigation, notable events from the SOC, or even curated intelligence from an in-house team is often the most valuable part of the feedback loop SIRP enables.

PEOPLE

Like data, the various functional teams within your security organisation (IR, SOC, Intel, Risk, Executives, etc.) also need the silos taken down from around them. They need access to relevant information from other teams, and intel sharing communities outside your organisation. seamlessly together with a dynamic workflow. SIRP facilitates this by allowing teams to provide tips and tasks to each other, create and funnel intelligence to relevant functional organisations, and create reports for executive decision makers based on threats to the organisation.

TECHNOLOGY

Most organisations today have a very heterogeneous and disconnected set of point defensive technologies. For most, coordinating action across them means coordinating tickets between IT and various facts of the security team. SIRP enables organisations to coordinate intelligence-driven action and automation across our ever-growing library of applications and integrations.

PROCESS

Once you have removed the silos between information, people, and technology, SIRP enables you to streamline your processes with playbooks that leverage both internal and external intelligence to inform action for your teams and your technology as well as learn from past experiences.

THREAT INTELLIGENCE VENDORS INTEGRATION

CRITS · DEVO · DNSlytics · DOMAINTOOLS · Internet Storm Center · E Hacking News

elastic · eset · CROWDSTRIKE · FARSIGHT SECURITY · DATADOG · DARKOWL

cuckoo · cybereason · cyberscoop · CYBER TRIAGE · CYLANCE · Cymmetria

CYMON.IO · CYPHORT Advanced Malware Defense · CYWARE · Fidelis Cybersecurity · FIREEYE · Forcepoint

IBM Radar · imperva · ipinfo.io · ipstack · JsonWHOIS · JUNIPER NETWORKS