NETWORK WAREHOUSE

Azure Sentinel

Maple Networks

NEXT-GEN HYBRID SIEM

www.networkwarehouse.co.uk

Contents

Security Challenges

1.0 Security Challenges

One of the key challenges in any SOC is dealing with the vast number of alerts that get generated. Every server, endpoint, network device and anything else in scope, constantly generates events. The role of the SOC is to try and differentiate which are security events, and then determine whether any of those are security incidents that are relevant and merit investigation.

Traditionally this has been tackled by feeding everything into a SIEM platform and throwing people at the problem. With attacks growing in volume and sophistication, this no longer works and increasingly means real and relevant security incidents are getting missed, while organisations are paying over the odds to have someone watching the screens 24/7.

1.1 Resource Shortage

In a recent survey carried out by The Enterprise Strategy Group, 75% of respondents agreed that the cyber security skills shortage has negatively impacted their security operations practices. The same survey highlights that 70% of recruiters find it difficult to hire qualified cyber security staff, and in many cases, particularly at a junior level, these staff often move on quickly after a year or two into higher paying positions. With this in mind, the logical step for many organisations is to outsource their Security Operations function to an MSSP, such as Maple Networks.

1.2 On-prem SIEM

On-premises Security Incident and Event Management (SIEM) platforms are often burdensome to maintain. For instance, implementing updates or OS patches typically falls to internal teams, and often means log collections interruption and means the Security Team cannot access the SIEM platform during those outages. On-premises SIEM solutions often suffer from various performance and interoperability issues, depending on the vendor.

Solution – High Level Overview

2.0 Solution – High Level Overview

Maple Networks have a wealth of experience with cyber security across various industries. Our team are no strangers to building Security Operations services, and we endeavour to build the best possible next-generation solution for our customers, integrating into their existing cyber security investments.

2.1 Azure Sentinel

At Maple Networks, we are driven by cloud technologies and automation. Across all our services, we strive to remove the repetitive tasks that are a burden to organisations. For this reason, we decided to leverage Azure Sentinel as the foundation to our Next-Gen Hybrid SIEM platform.

2.1.1 Hybrid SIEM

With Azure Sentinel being a cloud native SIEM, it has many advantages over its on-prem counterparts. For instance, updates and patching are the responsibility of the vendor – meaning they are rolled out automatically and this is one less burden on customers in-house teams. As the SIEM is in the cloud, so are the logs. Storage costs rise and fall with usage – no more having to account for 3-5 years' worth of logs for on-prem storage. Azure allows the customer to define retention periods on a per data type, so logs do not need to be stored for any longer than they have to. Current and Forecast costs can be viewed any time in the Azure portal.

2.1.2 Security Orchestration, Automation & Response

With automation being an important part of our business, investing and developing into a SOAR platform was a priority. This has enabled us to drive the efficiency of our Security Operation team, and as a result driving down the Mean Time to Response and Remediation for our customers. Utilising the Playbooks in Sentinel (based on Azure Logic Apps), this has allowed us to automate alert enrichment and conduct one-click remediation tasks. This helps prevent 'alert fatigue' that plagues so many SOC Analysts, whilst ensuring uniform ticketing and documentation across all alerts.

2.1.3 Machine Learning-based Detection

ML-based detection is built upon three pillars: Fusion, Built-In, and Bring Your Own ML (BYOML).

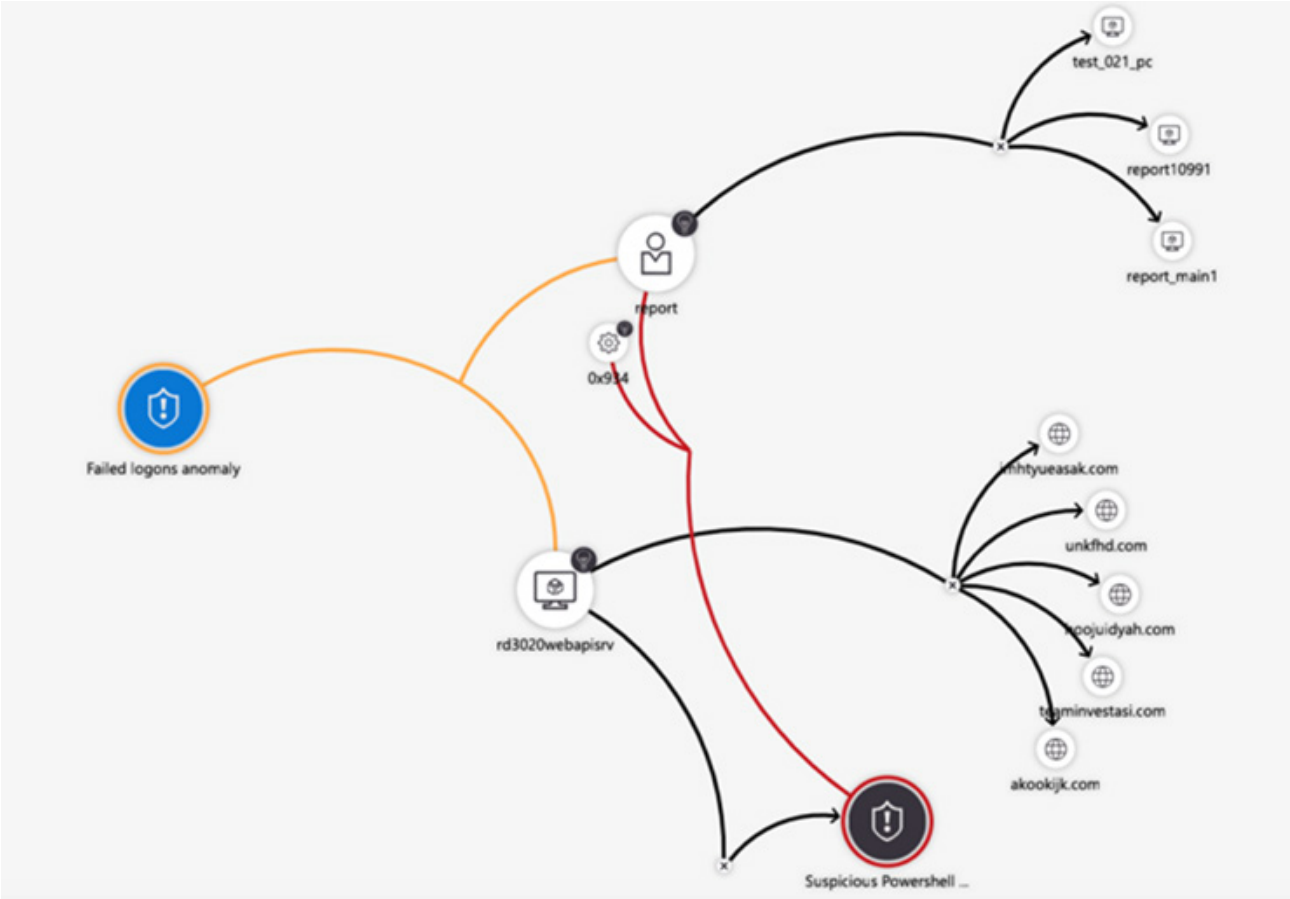
With Fusion alert detection rules, machine learning is utilised to identify multiple related Low and Medium alerts, that on their own may not appear to be a risk and correlate them into one single High alert. Utilising Machine Learning in this way drastically reduces false positive rates.

Built-in Machine Learning builds a baseline of normal activity within the environment and can alert when there is activity identified out-with baseline. This type of ML is used in behaviour analytics, for instance if a user credential is active from an IP Address in London, then 20 minutes later it is used to login from China, this can be defined as 'impossible travel'.

With most aspects of Azure Sentinel, flexibility is key and the ability to create our own machine learning analytics rules via BYOML is no different. Maple Networks can work with our customers to develop these, as and when the use case arises.

2.1.4 AI-enable Investigation

When malicious activity is identified on the estate, it is of paramount importance to understand the scope of the attack as well as its impact. Azure Sentinel's AI-enabled Investigation rapidly speeds up this process and provides a graphical interface and timeline to support the analyst in their investigation.



2.1.5 Key Service Integrations

It is key to us to be able to quickly integrate into various commonly used services and platforms via API. With over 40 native Data Connectors, and the ability to create custom connectors, we can connect into many of our customers services and platforms, both on-prem and in the cloud with just a few clicks. With these connectors the operability is endless, for example, we can create custom alerts rules based on the specific technologies used and utilise Playbooks to block a malicious IP Address on a Palo Alto firewall following a security alert. Whereby there is no native connector, as a rule of thumb, where remote logging via Syslog or CEF is supported – we can ingest the data.

As Azure Sentinel supports both Syslog and CEF data, this allows us to monitor any applications that also supports Syslog or CEF as remote logging. With this, it opens the possibility of Application Layer monitoring. Whether it is an Insider Threat/Disgruntled Employee, or compromised user credentials, it is good to have the experienced eyes of the Maple Networks Security Operations monitoring the business-critical applications that keep our customers in production. Similarly, due to the Syslog/CEF logging, we are also able to monitor third-party security tools, such as Vectra, through Sentinel.

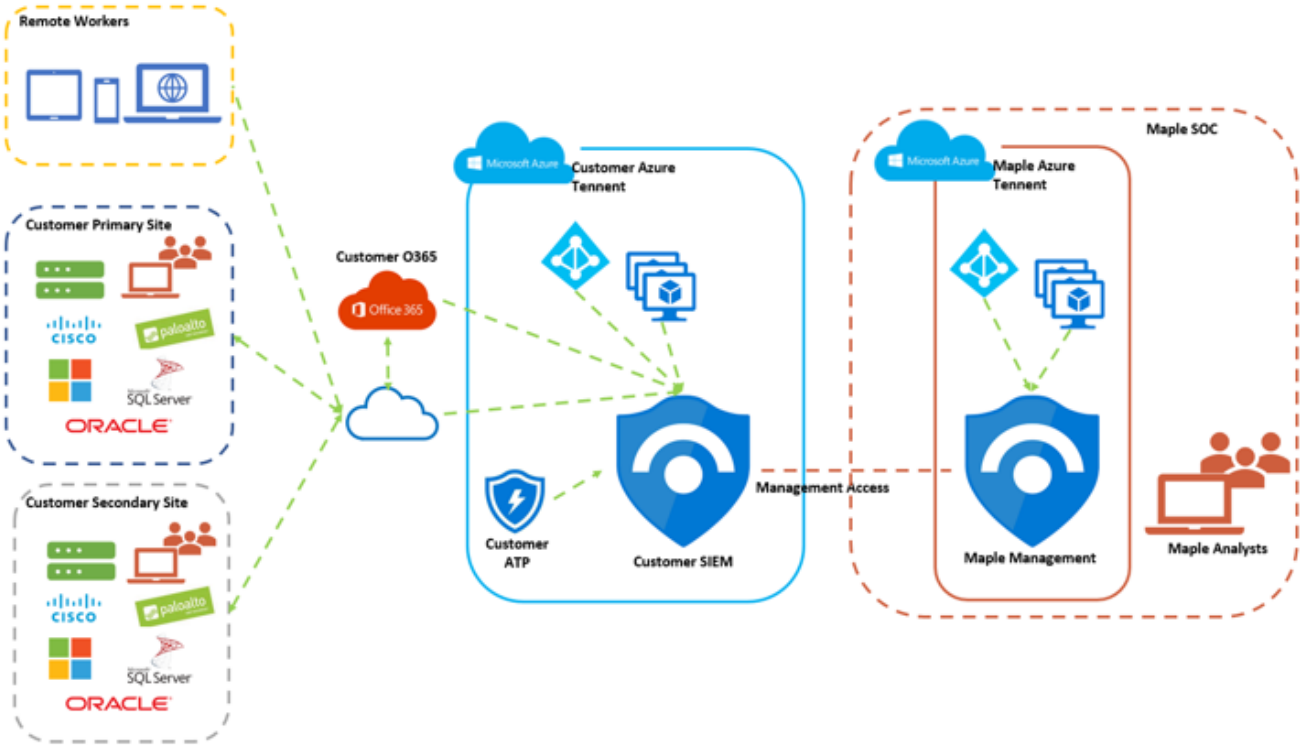
Solution Design

3.0 Solution Design

At Maple Networks, we believe flexibility and transparency is key in all services and products we offer. By design, all our toolsets are not only simple to on-board, but to dismantle – should the customer wish to bring the service in-house.

3.1 Decoupled Service

With Azure Sentinel, the Workspace is located within the customers Azure Tenancy. The platform, including all logs, remain in the ownership of the customer. This design keeps the control of the platform with the customer. Maple Networks only require access to the Sentinel piece within Azure, and this is done via Azure Lighthouse. This access is provided on the principle of least privilege.



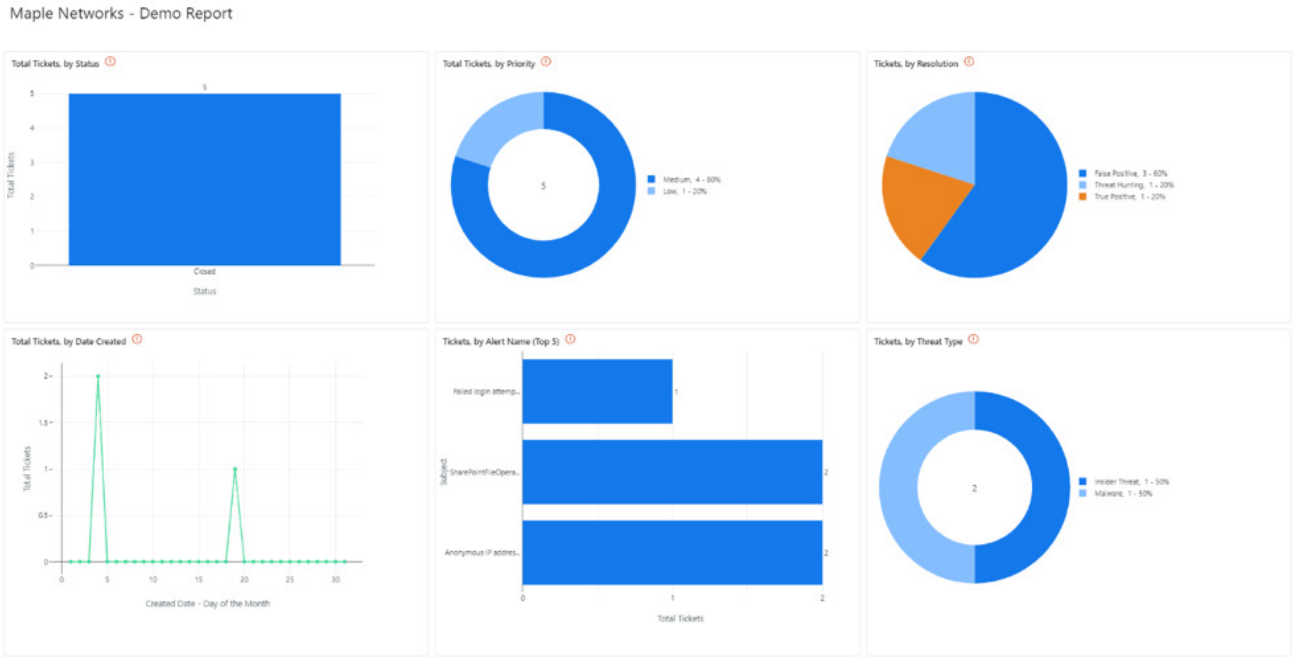
3.2 Rapid Onboarding

We are an incredibly automation-focused organisation. As our SIEM Service is based on Azure, we have developed Azure Resource Management (ARM) template's that allow us to create a Log Analytics Workspace and enable Sentinel within just a couple of minutes. For any on-prem Windows devices, we require an Agent to be installed. For non-Windows devices or applications, we can collect these logs via Syslog/CEF. We strive to have the Workspace created, the core "crown jewels" onboarded, Syslog/CEF collector deployed and threat intelligence feeds streaming into the Workspace within just a few days.

3.3 Customer Ticketing Portal

As Azure Sentinel is fully integrable with our ticketing platform, all Medium and High alerts are ticketed automatically. Furthermore, a portal is set up for each customer allowing their Information Security teams to go in and review all tickets that have been created at any time – meaning they do not have to wait for our regular automated reports. This approach allows both Maple and customer Information

Security teams to work collaboratively when responding to security incidents and performing remediation tasks.



3.4 Intuitive Dashboards

With the Workbooks in Azure Sentinel, it allows our customers to visualise and get the most out of their data – not just from a security perspective. These workbooks run based on the API Connectors and are specific to the data source, which is great to determine Office 365 usage, for example. We also have Workbooks that help our customers keep track of the health of their Workspace, as well as cost and being able to visualise "noisy" devices on the estate.

3.5 Proof of Concept

Maple Networks are a flexible organisation and we fully understand that it is good to see how a new technology would operate within their environment. For this, we are always happy to offer a Proof of Concept. This typically involves a small subset of the "crown jewels" so we can demonstrate how efficiently we implement perimeter, identity, and application protection, as well as how the Maple Security Operations Team act as an extension to your internal Information Security Team.

Professional Services

4.0 Professional Services

With the flexibility of Azure Sentinel, it allows Maple Networks to offer a variety of services on top of the value to ensure that our customers are getting the most for their money, and full use of the toolset that they are investing in.

4.1 Single-click Threat Hunting

With over 80 out of the box queries, threat hunting activity can be carried out with a single click, identifying potentially malicious activity across an array of threats that may have slipped through the net. This type of hunting is carried out daily by the Maple Security Operations Team. Custom Queries are provided by Maple Networks as standard to best detect various threats such as BlueKeep Exploitation or Emotet malware execution.

4.2 Intelligence-driven Threat Hunting

Maple Networks utilise the best-in-class threat intelligence providers to help identify what threats are facing which industry, and the Technique's, Tactics and Procedures (TTPs) in which the threats are being carried out. Notebooks allow us to hunt for specific threats based on the actionable intelligence for the organisations industry. In addition to this, Microsoft also released their own Notebook to hunt for Covid-19 related threats which Maple Networks have been utilising in recent months.

4.3 Industry Specific Threat Intelligence

Maple Networks has a vast bank of Threat Intelligence feeds, pulling in over 1 million unique and active Indicators of Compromise (IoC's) on a daily basis. We strive to implement the most appropriate and relevant feeds to our customers on an individual basis that is most relevant to their industry and threat landscape as well as tracking common widespread malware groups such as Emotet/Heodo and Dridex that target many organisations and industries indiscriminately.

To capitalise on the benefits of the threat intelligence we provide, we can tie into various data connections to alert to potential threats or areas of compromise. For instance, mapping our Threat Intelligence IoC's to Office Activity can alert the Maple SOC to potential phishing campaigns or malware delivery. Mapping to DNS Activity can bring attention to connections to potential C2 domains or IPs. Utilising our threat intelligence in this way can provide an extra layer of defence and visibility into what is going on within your network.

4.4 Flexible Coverage

We understand that every company is different and has different needs and requirements. In-house Security Operations Centre's are very expensive and come with its own challenges. With Maple Networks, we offer a very flexible service to fit round our customers current investments and resources. For this reason, we offer:

- 24/7 coverage
- Out of hours coverage only

Like the Flexible Coverage above, we are flexibly in approach to Incident Response and Remediation. We look to fit in with the customers current process(es) when it comes to Remediation. Some customers have the resource and the staff already on-call to carry out these tasks, other customers do not, which is why we offer the below escalation and remediation options to all our customers:

- Initial "first line" alert triage with escalation to customer Information Security Team
- First and Second Line support with remediation i.e. blocking a compromised account in Azure AD

Common remediation tasks are built into the SOAR Playbooks, such as blocking an IP address on a firewall or disabling a compromised Azure AD user account. This functionality allows for one-click remediation, meaning it is carried out having to login to additional services but most importantly, containing the threat within just a couple of seconds.

Business Benefits

5.0 Business Benefits

Combining the key factors of the Hybrid SIEM, how Maple Networks design and implement the solution, as well as the Professional Services that we offer on top of the platform as standard, we are confident in that we can provide our customers with the following benefits to their organisation:

- 24/7 coverage, and the assurance that the network is being monitored round-the-clock
- Maintaining current investments
- Protection of valuable data, such as IP or PII
- A cost-effective price model, helping the customer budget accordingly
- Reduction in cyber security risk
- Data sovereignty – all data is stored under the customer ownership
- A proactive, not reactive, approach to security

Commercial Summary

6.0 Commercial Summary

With Azure Sentinel come's a straightforward pricing model, the customer owns their Azure Tenancy in which their logs reside, so the customer pays the bill to Microsoft for the log storage and Sentinel costs. The customer can keep track of all costs and forecasts in the Azure Portal. Secondly, there is the bill from Maple Networks for the service in which we run on Sentinel – no hidden costs, no jargon.

FAQ's

Q. Do we have access to Sentinel?

A. Yes, Sentinel is within the customer tenancy.

Q. How quick is deployment?

A. We aim to have the "crown jewels" logging within a few days

Q. Can we ingest our other security toolsets into Sentinel?

A. Yes, as a rule of thumb, anything that supports remote logging via Syslog/CEF we can ingest from

Q. Can you monitor our critical applications?

A. Yes, as above – anything that supports remote logging via Syslog/CEF we can ingest from – even application logs

Q. How much does log storage in Azure cost?

A. We recommend accounting for 2GB, per device, per month. At time of writing, in the UK South region 1GB = £2.147 per month

Q. How much does log retention cost? And for how long can I retain logs?

A. Logs on Sentinel-enabled workspaces are free for 90 days. Logs can be stored for as long as two years. If longer is required, they can be pushed to long-term storage

Q. Can I ingest logs from my existing cloud provider?

A. Yes, we can ingest from Azure, AWS and GCP

NETWORK WAREHOUSE

85 Great Portland St
London
W1W 7LT

t. +44 (0) 203 733 2345
e. support@networkwarehouse.co.uk

www.networkwarehouse.co.uk

Azure Sentinel

Maple Networks