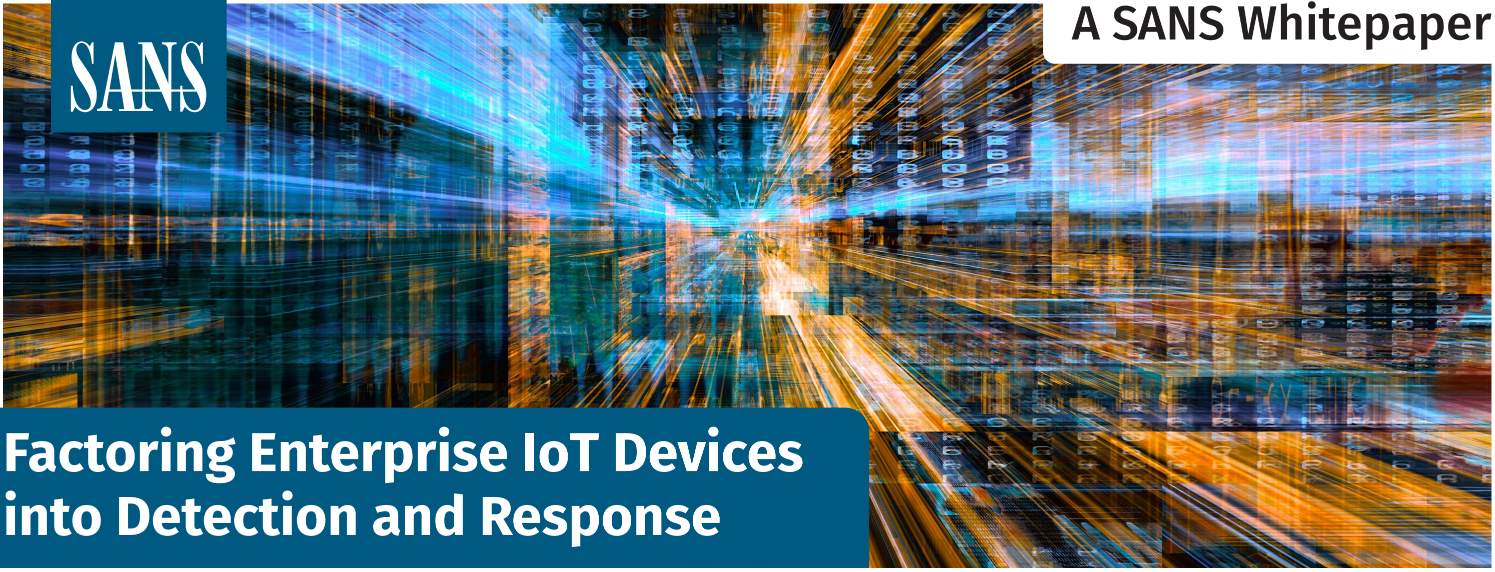
A SANS Whitepaper



Factoring Enterprise IoT Devices into Detection and Response

Written by **Matt Bromiley**

May 2020

Sponsored by:

ExtraHop

Let's start with a simple question: What's in your enterprise network? In previous years, that answer might have been relatively simple: clients and servers. But in today's networks, the answer is more complex. Clients and servers are still there, but these days there's likely a multitude of different types of devices: BYOD, mobile devices and a growing population of Internet-connected business resources. These enterprise IoT (eIoT) devices are shifting your attack surface—but are they shaping your detection and response procedures?

To clarify, by eIoT devices, this paper doesn't mean every employee who comes and plugs in a Raspberry Pi[1]—although this paper does examine such scenarios. Instead, think of the enterprise-owned devices that may power "new normal" business operations, such as smart TVs, badge scanners, projectors, whiteboards and printers, to name just a few. These smart devices are continually showing up in enterprise offices and connecting to your networks.

Organizations need to ask some specific questions in relation to enterprise IoT:

- Is our security team aware of every new IoT device that finds its way onto our enterprise network?
- Has the team assessed how a potentially unmanaged, nonstandard device increases security risk on our network?
- Has the information security team assessed how to detect and respond to suspicious traffic stemming from enterprise IoT devices?

Unfortunately, in many situations, the answer to these questions is a resounding "no."

[1] Raspberry Pi is a trademark of the Raspberry Pi Foundation.

This paper explores the growth of enterprise IoT devices inside corporate networks and how they change the shape of incident detection and response. The enterprise device landscape is dynamic; it's prudent for your information security team to track changes to understand the effects on your network.

As you work your way through this paper, consider the following:

- Are there any approved enterprise IoT devices in your enterprise?
- If so, are they factored into the security team's detection and response capabilities?
- Are there any unapproved/foreign enterprise IoT devices in your enterprise? Would you even know?

With the advent of the cloud, corporate networks are becoming more complex. There is a constant state of change with new types of devices installed daily. To keep pace, you will need an approach to threat detection and response that enables your team's full visibility so it can quickly adapt and include enterprise IoT devices in its response plans.

Enterprise IoT (eIoT) devices aren't always lightbulbs or employee-owned devices. Think of the enterprise devices in use today: printers, smart televisions, whiteboards, cameras, badge readers and so forth. These devices are sanctioned and purchased by the organization—but did anyone consult security while making this decision?

IoT in the enterprise is an issue that is of concern as a potential attack vector to gain entry into the network. If you haven't taken stock of the eIoT devices in your network, you might be surprised at just how many devices are already in place.

A Grown-up Problem

In researching the implications of this topic, it became clear that eIoT is a problem that's been around for many years. The acceleration of the number of IoT devices connecting to the corporate network means that we can't wait any longer to address this issue—making this a grown-up problem. Such devices are now part of normal business operations and assist in delivering services on a daily basis. Stop for a moment and think about the various eIoT devices in your organization. How many did you walk past on your most recent visit to the office?

The problem is compounded when you move beyond authorized eIoT devices. Unauthorized and/or third-party eIoT devices open up additional attack vectors that your information security team may not have visibility into, as shown in Figure 1.

Enterprise IoT devices found in many enterprises are already having an impact. A 2019 Ponemon Institute study[2] reported that between 2017 and 2019, there was an increase of 11% in data breaches specifically due to an IoT device; however, just as many organizations admitted they were not aware of every IoT device in their environment, so these numbers are likely higher. When asked about monitoring, just over 50% of respondents indicated they were monitoring their own IoT devices, but only a third admitted monitoring third-party IoT devices.

Unauthorized IoT Devices	• Installed by users with knowledge of the organization • Potentially connected to the same network used by employees • May be used to circumvent security controls • Likely default-configured or insecure
Third-Party IoT Devices	• Installed as a part of third-party service delivery • Very little visibility or knowledge to the security team • Likely default-configured or insecure • Lack of mechanism for support/updates

Figure 1. Security Considerations for Unauthorized and Third-Party IoT Devices

[2] www.businesswire.com/news/home/20190507005347/en/Ponemon%E2%80%99s-Annual-Study-Party-IoT-Risk-Companies

Organizations realize that modern business is reliant on third-party vendors, but they are not always aware of the risk this may pose. A vulnerable third-party application or device (such as eIoT) could be a potential entry point into your network or a vehicle for data exfiltration.

Enterprise IoT devices alone present multiple security issues, from easily hacked devices that are shipped with default or cleartext passwords, to the fact that most communications are not encrypted and go unmonitored on the network. The growth of eIoT devices further complicates matters when an organization is at risk from legacy and complex processes and trying to move to the cloud. As this paper examines in the next section, visibility and awareness are the required starting blocks for successful eIoT detection and response.

eIoT threats and gaps are already being realized in many organizations where monitoring is admittedly inadequate and risk programs do not include these security concerns.

Case Study: Houston, We Have an Unapproved Device

The business need for visibility and awareness was never more apparent than in mid-2018, when NASA's Jet Propulsion Lab (JPL) experienced a significant data breach directly attributed to an unauthorized IoT device. Let's break down this particular data breach, explore how IoT device handling went awry, and determine how NASA could have mitigated or prevented this particular breach.

The Cause

A 2019 audit report from NASA's Office of Inspector General (OIG)[3] revealed that in April 2018, NASA's Jet Propulsion Laboratory (JPL) suffered a data breach that resulted in approximately 500MB of data being exfiltrated from the environment. The 500MB included mission-critical data, including data directly related to the Mars Science Laboratory mission.

After an investigation, NASA determined that the cause of the data breach was an *unauthorized Raspberry Pi* attached to JPL's network. Not only was the Raspberry Pi unauthorized, but it was also left connected in an insecure state that allowed for relatively simple compromise.

The effects of this breach were compounded when the threat actor was able to easily move laterally from the Raspberry Pi into sensitive NASA networks. Two of JPL's three networks were accessed, and at least one account was taken over by a threat actor that allowed for access and data exfiltration.

Deep Impact

This particular breach, all from one tiny IoT device, rippled through the JPL, the whole NASA organization and several external parties. Interpretation of the audit report shows that impacts included the following:

- Two of JPL's three primary networks were accessed by the threat actor, with the data loss resulting in potential mission compromise.

[3] https://oig.nasa.gov/docs/IG-19-022.pdf

- Depending on mission status, exfiltrated data may have caused severe setbacks and/or R&D losses to NASA. Again, considering the timeline of some NASA projects, this data breach may have caused significant financial and/or taxpayer impact.
- As a result of the data breach, other groups within NASA disconnected from the JPL network. When a particular business unit is deemed untrustworthy, other subgroups would do well to disconnect; however, if these groups require communication for daily operations, the organization will feel this impact much more strongly.

While not necessarily a "typical" enterprise, NASA's breach illustrated that IoT devices—even those that are seemingly harmless—can provide ample opportunities for attackers to gain access into a network.

Moving Onward

The April 2018 JPL breach pointed out some obvious flaws within NASA networks. To learn from the mistakes of others, organizations of all shapes and sizes should be analyzing this case study. Let's examine some key security implementations that NASA should have used to mitigate this breach.

Network Segmentation

The unauthorized Raspberry Pi device was able to easily move laterally among multiple JPL networks due to a lack of segmentation. Let's be clear: A lack of network segmentation is not new nor has it anything to do with IoT devices; network segmentation is simply good practice. And, with the introduction of new IoT devices into a network, *revisiting segmentation policies would be prudent.*

Least Permissions

The threat actor used the compromised Raspberry Pi to pivot and move deeper into the JPL networks and to escalate privileges. Regardless of a lack of segmentation (discussed previously), users should not be allowed to connect unauthorized devices *and* their credentials should limit access to only the systems they need to do their particular job. *Enacting least privilege at all times means that compromised credentials cannot be used to escalate privileges and prevent access to sensitive data.*

Device Detection

One of the NASA OIG's chief complaints centers on the device being connected to the network in the first place, and we couldn't agree more. Given the sensitivity of the data on the network, all connected devices should require approval. When a new device is connected to the network, the IT and security teams should have immediate visibility into that device and understand its primary function on the network. For NASA, *requiring approval for connectivity to the network* is an excellent start, but the agency failed to monitor the network to detect the device and its communication with critical devices. Worse yet, the compromise remained on the network for nearly a year before finally being detected.

Any organization knows that the earlier you can catch malicious activity, the less severe it will be. The connection of the Raspberry Pi to the JPL network was the earliest possible point of detection, and one we focus on in subsequent sections.

There are many examples of organizations falling victim to unknown and/or unmanaged IoT devices on their networks. In some cases, the impact may have been an increase of bandwidth, as was seen in the 2016 DDoS attack that was launched by the Mirai botnet.[4] In others, the damage may be more significant. NASA's JPL breach saw significant systems accessed and data stolen; this ultimately resulted in other NASA units disconnecting from core gateways. Regardless of size or impact, the message is still the same: Improper network visibility, monitoring, detection and response will significantly impact the business.

Key Takeaways from NASA's JPL Raspberry Pi Breach

- Complete visibility of networked devices and an understanding of their function are required to monitor your network for unauthorized device connections.
- Segment your network to protect sensitive data and prevent privilege escalation.
- IoT devices can be vulnerabilities and easy entry points to the greater network.
- Network detection must be present to respond to ongoing threats and prevent them from remaining on the network.

Why Network Detection and Response

With an inevitable rise in eIoT devices, expanded threat vectors and multiple public cases of how eIoT breaches can impact an organization, how can security teams best prepare themselves to handle the changing landscape? As unique as eIoT devices are, they are ultimately just one more type of device on your network that requires visibility to detect, enabling you to respond to suspicious behavior.

Not Quite an Endpoint

Many enterprises have built up their security programs via agent-based endpoint visibility, which can be useful and provide excellent insight; however, eIoT devices are installed with either minimal or custom operating systems (if any at all). This makes it difficult, if not impossible, to install an endpoint on a system—assuming you own it in the first place! Remember, some eIoT devices are installed in corporate networks, but owned and/or managed by a third party.

Organizations should consider using data that flows over the network as the primary source of truth. If your organization is already utilizing network traffic for incident detection and response, then you're likely already seeing traffic for eIoT devices on your network. You can immediately begin to pivot off of this data to identify devices and the utility they serve on the network.

The volume of eIoT devices, combined with the fact that they are not designed for endpoint-specific monitoring, means you must turn to the common denominator: the network. The network serves as a way to not only identify, but also monitor, segment and detect compromised eIoT devices.

If your security team is not utilizing network traffic in your current incident detection and response approach, then you are likely missing a considerable portion of the environment. Although this paper focuses on eIoT, we encourage you to use eIoT as a discussion point to incorporate the monitoring of Layer 2 through Layer 7 data traversing the network into your current detection and response plan. Network data provides the basis for complete, up-to-date network device visibility in an organization for *all* devices, including eIoT.

[4] www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

eIoT Network Monitoring for Detection

Taking network-based approaches toward eIoT devices offers an organization multiple benefits, most of which also serve as overall detection benefits. This paper focuses on eIoT devices, but keep in mind when you start analyzing your organization's network traffic, you're opening up a new route for monitoring and detection that can provide faster identification of incidents.

Let's examine a few considerations and benefits, shown in Figure 2, regarding utilizing network monitoring for IoT security.

Notice how a network monitoring approach provides multiple simultaneous benefits. A security team can begin to discover, identify, segment and monitor eIoT devices with a few quick steps. Network monitoring for detection and response carries an intrinsic benefit for security teams as well—the same data they use to discover is used to monitor. Techniques used to discover and identify can easily be compounded into monitoring, allowing for easy recycling throughout the organization to continually discover new devices.

Discovery	• IoT devices, authorized or not, will often have specific signatures that make them stand out from other devices. • You may be able to rely on known access points or subnets to make discovery easier. • This is a good chance to inventory and document third-party IoT devices that may be utilizing your network. • Your team's knowledge of expected client/server behavior should help with finding needles in the haystacks.
Identification and Access	• Once you've discovered one or more IoT devices on the network, the next step is understanding their purpose. • What types of devices are they: whiteboard, refrigerator, smart TV, Raspberry Pi? • Are devices authorized or unauthorized? Does anything need to be unplugged? • Again, utilize access points and subnets to determine where devices are and what they have access to.
Segmentation	• With device discovery and identification completed, the next step is to confirm that IoT devices are truly segmented from the rest of the network. • Validate segmentation or move devices to segmented networks. • If a device violates segmentation and cannot be moved, consider implementing device-specific blocks. • Layers 2 and 3 will be critical to success here, again proving the network's value in assessing and managing IoT devices.
Monitoring	• With device discovery and identification completed, your security team can begin to build detections around what these devices should and shouldn't be doing. • Ensure that network visibility and alerting is extended to SIEM and monitoring platforms. • Categorize devices appropriately (e.g., if a device sits on a sensitive network, rank its criticality and build alerting accordingly).

Figure 2. Considerations and Benefits When Using Network Monitoring for IoT Devices

Doing More with Your Network Data

It's worth mentioning that much of what we've discussed thus far—writing detections, analyzing network traffic and/or finding eIoT devices inside your environment—may require some manual approaches from the team. Although such exercises have many benefits for the security team, some environments are so large or have so many devices that it would take a dedicated team longer than necessary to identify eIoT devices in the environment. For that reason, we recommend assessing solutions that will automate or perform much of the above for your security team.

Discovering and identifying eIoT devices within a network is only half the battle. Once your teams discover them, it's time to understand what access they have, who they can talk to and how they can impact the environment.

Security solutions that include a focus on eIoT offer another advantage in the form of historical device experience for insight into normal behaviors. These solutions can automate analytics to help build robust signatures and rules for detections. For example, many vendors will utilize machine learning and other advanced techniques to automatically comprehend the role(s) and privilege(s) of all devices, including eIoT, and assist in assessing and/or grouping them. This insight means that detection of unusual behavior or threats is provided in the context of the entire hybrid network.

IoT Incident Response

With an effective eIoT device identification and detection plan in place, your organization is well on its way to understanding your eIoT ecosystem, and your team has a good basis of intelligence for responding to an incident.

Changing the Game

There is no question that eIoT has created a new attack surface, and incident response (IR) plans don't necessarily change just because IoT devices are involved. In some situations, eIoT-based incidents may be fairly self-contained or device-limited; in others, the device can be used to pivot to the rest of the network. Consider, as was discussed previously, the Mirai botnet in 2016 that crippled several high-profile services with a massive DDoS attack. These attacks were certainly considerable, but they were easily mitigated by disabling internet access for infected devices—if, of course, you could identify them before the botnet spread. The data breach at NASA's JPL laboratory involved multiple systems and data exfiltration. While eIoT devices can add another layer of complexity to an incident—they don't change the fundamental nature of response.

If you are responding to an incident involving an eIoT device, you should still follow a solid IR process, layering in how eIoT impacts the incident. Figure 3 shows a model six-step IR process.

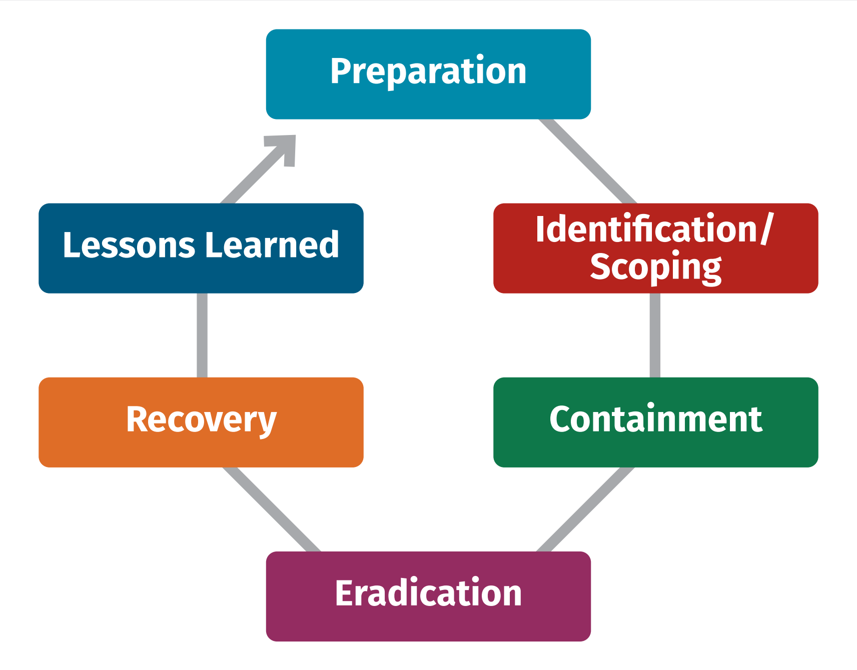


Figure 3. Six-Step Incident Response Process

The six-step IR process provides high-level guidance to help any organization through an incident while remaining flexible enough to adapt to the specific organization's makeup. Let's look at the six-step process with IoT in mind:

1. Preparation (prior to an incident)

The preparation step is both pre- and post-incident. In the pre-incident phase, you want to ensure that your organization has identified and profiled eIoT devices. This will make the subsequent steps significantly easier.

Key Questions:

- Have we identified/profiled our eIoT devices?
- Are we aware of how eIoT is used in our environment?

2. Identification (during an incident)

Incident identification involves identifying all systems impacted by a data breach. This is where network visibility and monitoring become crucial to success—and provide the key to the most important question of scope. Once you have network monitoring (think north-south AND east-west) wrapped around your eIoT devices, you can easily see whom they are talking to/receiving information from and what that communication might look like.

Key Questions:

- Is the eIoT device the entry vector, the vehicle or the target?
- How many other systems are involved?
- How can our eIoT network data be paired with other data in the environment to provide next steps for the response team?

3. Containment (during an incident)

The containment phase of an incident is exactly what it sounds like—implementing controls to contain the spread of infection and prevent the attacker from gaining any additional access or access to sensitive data. Again, consider network traffic the secret weapon here. Network blocks and/or firewall implementations are a quick way to contain an incident and limit it to a small number of systems.

Key Questions:

- Are there steps we can implement to prevent the spread of infection?
- How can we prevent the attacker from accessing more data without necessarily tipping them off?
- Do we contain or move right to eradication?

4. Eradication (during an incident)

Once the incident has been properly scoped and the organization is ready to remove the attacker from the environment, eradication is the swift step of performing all necessary activities to kick the attacker out once and for all. The key data points captured during Steps 2 and 3 should ensure that eradication is successful.

Key Questions:

- How quickly should we eradicate?
- How will this affect users/applications/systems/business processes?
- Are there other security vulnerabilities and/or entry vectors that we should close off to make sure our attacker doesn't return?

5. Recovery (post-incident, but still on high alert)

With the attacker out of the environment, the security team is still on high alert. It's time to begin assessing what happened, while keeping a close watch to ensure the attacker doesn't return and any containment/eradication steps are not reversed, either by a user or the attacker. Utilize the network monitoring and detection you've wrapped around your eIoT devices to assess these.

Key Questions:

- Is the attacker coming back in?
- Are users inadvertently re-opening entry vectors as a result of the remediation?

6. Lessons Learned (post-incident, alert is lowered)

By the time you've reached this stage, the organization needs to learn from what happened to prevent a similar event in the future. As a team, examine the key takeaways from the incident and ensure that preventative measures are implemented. If communication needs to be issued to the organization (such as "Don't plug in your Raspberry Pis!"), now is the time to do so.

Key Questions:

- How did this happen?
- How can we prevent it from happening again?
- Do we need to tune/enhance/implement any new detections?
- Do we need to communicate new policies to our users?

The IR process is cyclical, which means each incident should make the security team stronger. You may notice as you read through the process that eIoT devices didn't change the overall goal of getting the organization back to your baseline. You may also notice that at certain points, the process relied on other data points to add value to the IR process. If your eIoT devices are the only devices involved in a breach, they will be the primary source. But don't forget you likely have other telemetry in the environment you can use to measure the impact of an incident.

What Can Organizations Do Now?

This paper explored how the changing landscape of devices in an organization will impact its security posture. In particular, the growth of eIoT devices—approved by the business or not—increases the potential attack surface of the organization. As security teams are tasked with protecting the organization, these newer device types likely fall within their scope of defense, but outside the scope of visibility.

To help bridge this gap, this paper recommends turning toward network traffic as your best medium for profiling devices and defending against eIoT-based threats. Historically, your "north-south" traffic will provide visibility into environment egress and ingress, while "east-west" will show internal traffic whether on-premises or in the cloud. Both are crucial to a solid network security program. Furthermore, there's a strong chance that eIoT network traffic differs enough from the rest of your environment that it presents a chance for incident detection and response.

Want to get started right away? Begin by ensuring that you have visibility and access to internal network traffic and start thinking of ways to analyze and/or extract key data points from that traffic. This paper describes a few analysis tips. Turn those into action items.

Network evidence will also prove to be invaluable in the event a security team must respond to an IoT-involved incident. Network traffic will allow for rapid incident scoping, containment and eradication—but success depends on visibility and classification. The first step to success is ensuring that you have visibility into relevant traffic and that the right team members can classify and act upon relevant IoT traffic.

Despite the capabilities that network detection and response provide for IoT devices, success will be hard to find if your organization doesn't begin factoring IoT devices into its threat landscape. Remember, it's likely these devices are already in your network. Don't let your organization get caught off guard and need to deal with an incident for which you have very limited visibility.

About the Author

Matt Bromiley is a SANS digital forensics and incident response (IR) instructor, teaching FOR508 (Advanced Incident Response, Threat Hunting, and Digital Forensics) and FOR572 (Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response). He is also an IR consultant at a global incident response and forensic analysis company, combining his experience in digital forensics, log analytics, and IR and management. His skills include disk, database, memory, and network forensics; incident management; threat intelligence; and network security monitoring. Matt has worked with organizations of all shapes and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

ExtraHop

Rise Above the Noise.