What is that?

This is a glossary of commonly-used terms.

Active	A device is “Active” if it’s responded to traffic we’ve sent to it or if we’ve heard about the device Indirectly (via SNMP for example).
Active Discovery	Scanning where a Collector’s Scanner places traffic on the network destined for a targeted address and listens for the responses from that address (or hops along the way in the case of Path)
Alias	For credentials (like SNMP or WMI) an alias is just the name we associate with that credential for reporting purposes. It allows us to say “secret1” in a report instead of putting the actual and presumably sensitive credentials into a report.
Collector	A collection of associated Scanners within a Zone that share a single Scanning Interface.
Commanded Packet Rate	A Scout’s network interface can be given a Commanded Packet Rate. This is the rate of scanning traffic (in packets per second) that Spectre will not exceed (at least over intervals of greater than 1 second). Depending on the targeted address space, we may not scan as quickly as the Commanded Packet Rate, but Spectre will not exceed this rate. This rate is per Scanning Interface, this interface may be shared by more than one Collector
Device	As far as Asset Manager is concerned, a Device is one or more IP addresses that we’ve decided belong together. Typically we think they belong together due to our getting SNMP data that says they’re all interface addresses for the same thing. It’s an attempt to represent a physical thing that’s attached to the network, but it’s not always a complete match (we don’t have all the information that someone sitting in front of a physical device might have).
Eligible List	A collection of CIDRs that dictate if further interrogation for a specified address should be performed. This is primarily used when a response is received from an address that is outside the target list and influences the decision to further interrogate this address. In other words, if we target 2.2.2.2 and hear about 1.1.1.1, we’ll target 1.1.1.1 for scanning if it’s covered by the eligible list (e.g. if we had 1.0.0.0/8 in the eligible list)
Event	Event is an action or occurrence detected by a program. It can be “published” so that other parts of the system can act on it. At this point, it will appear as a notification.
Explicit Target	A Target explicitly defined in a Collector’s configuration (under Discovery Spaces > Target List)
Fact	Something we know about a Device by receiving data directly from that Device. This would typically be via Active or Passive Discovery (eliding for the moment the idea that “Fact”s can be tricky things as we’re talking through the network to a Device so Facts can be altered in transit). This would also include cases where we explicitly ask another system (like DNS) about a Device
Forwarder	A Device is a “Forwarder” if it’s seen in a trace (generated by the Path scanner) as anything but the last hop. In other words, a device that generates an ICMP Time Exceeded message. This is a Fact rather than an Inference
Indirect Discovery	Discovery where the system gets information about an address from something other than that address (e.g., BGP, DNS, or OSPF). For example, Asset Manager learns about device 2.2.2.2 while interrogating 1.1.1.1 via SNMP and learning about 2.2.2.2 from 1.1.1.1’s ARP table.
Inference	Something we can say about a Device derived from Facts about a Device or by Indirect Discovery (or by things like MAC Vendor data etc.). Profiling data (for example) is a collection of Inferences
Learned CIDR	A CIDR learned about via SNMP (either a host or a CIDR representing a route), OSPF, or BGP.
Loose IP	
Notification	A message presented to the user as the result of an event.
Passive Discovery	Listening to traffic without putting any packets on the network. (e.g., Broadcast). This could also be a Scanner listening to traffic on a trunk or SPAN port.
Primary Target	A Target that’s explicitly specified in a Collector configuration or learned about via an SNMP routing table, BGP, or OSPF. This is effectively a Host or Path target (these are the scan types that scan across entire CIDRs). Responses to a Primary Target can create Secondary Targets. That is to say, a response to Host can create targets for scan types like Port, or SNMP.
Qualified Address	An address that’s explicitly targeted, or learned and covered by the Eligible List. An address in the Avoid List cannot be Qualified.

Reference IP	For a Device with more than one IP address, we pick one address to refer to it by. We pick the reference IP by the following criteria (subject to change): 1) Prefer IPv4 over IPv6 2) Prefer public (non RFC 1918) addresses 3) Prefer internal addresses 4) Prefer known addresses 5) Highest IP address
Scanner	A specific bit of code (like SnmpHunter) that runs as part of a Collector on a Scout somewhere
Scanning Interface	A network interface associated with a Scout. This interface can be used by one or more Collectors. This interface can be given a Commanded Packet Rate.
Scout	A collection of Scanners and Scanning Interfaces running on a particular (virtual) machine. These scanners could be associated with any number of Zones or Command Centers. It could be a VM built and licensed as a Scout or an “Onboard Scout,” which is the Scout code running on a Command Center.
Scout Interface	A specific network interface on a Scout. This interface can be configured to throttle some discovery traffic (at least Host, Port, Path, and SNMP)
Secondary Target	A Target (/32 or /128) generated for a non-Host/Path scan(discovery) type as a result of Spectre learning about an address. These Targets can be generated by being discovered via Host or Path, being Indirectly or Passively discovered, or by having a device added via API. These are the Targets the system generates itself (governed by discovered addresses, Eligible List, and Avoid List).
snmpAccessible	A device that we were able to talk to and get responses with a set of SNMP credentials. Receiving SysDescr, routes, or interfaces will be examples of a SNMP Accessible device. If we just get an error message (an SNMPv3 credential error or a OID not found for v2) we will not be snmpAccessible though we will be an snmpResponder
SNMP Details	This is a Tertiary Target type. If configured to do so, we will gather data from various SNMP OIDs and determine things like Interface or Route information
SNMP Discovery	This is a Secondary Target type. When we do SNMP Discovery we try all the SNMP Credentials configured for a collector and report on which ones were accessible. In SNMP Discovery we will gather things like sysObjectId, sysDescr, and potentially serial number information.
snmpResponder	A device that we got an SNMP response from even if we can’t fetch data from it with our SNMP credentials. This could happen if we attempt to communicate with a device using SNMPv3, it can respond with an authentication error of some sort, this is different from SNMPv1/2c where the device usually doesn’t send anything back in the case of an authentication failure (though ACLs can cause SNMPv2 errors).
Spool File	On a Asset Manager command center, the data we ingest from scanning is contained under /var/spool/esi. The files that a queued up for ingestion are at /var/spool/esi/preprocessing. These files are commonly referred to as “Spool Files” and if we’re trying to debug why the system is behaving the way it does we’ll commonly start by looking at them.
Target	A combination of a CIDR, Scan Type, and Collector ID. This can be a Primary, Secondary, or Tertiary Target.
Tertiary Target	Once a device has been scanned using a primary scan type, it is determined to be alive. After a secondary scan type, the target has been determined to have the potential of responding to a particular protocol. The tertiary scan type asks for heavier weight responses, such as SNMP Details, HTTP banners, CIFS, or WMI.
Time of Discovery	The time a Scout discovers a Device (or information about a Device)
Time of Record	The time a discovered Device is actually available in the database for reporting (the time it’s actually visible to a client).
Zone	A set of Collectors and the data associated with them. For the most part, data is not propagated across zones.

Adversary	An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.
Baseline	A network's steady state; equilibrium

Broadcast Domain	Any computer connected to the same Ethernet repeater or switch is a member of the same broadcast domain. • Logical division of a computer network • Routers and the like border the domain • Essentially, the LAN, or "what is connected to a switch"
Command Center	• Houses end-user display (web GUI) • Allows monitoring, administration, and reporting • Configures and initiate scans via onboard collector • Distributes configuration to distributed Asset Manager Collectors •
Continuous Monitoring	The concept of monitoring information system security has long been recognized as sound management practice. Organizations review their information systems' security controls to ensure that system changes do not have a significant negative impact on security, security plans remain effective after a change, and security controls continue to perform as intended. Continuous monitoring goes further than a traditional periodic assessment or "snapshot" audit by continuously monitoring transactions and controls, so that weak, poorly designed, or poorly implemented controls can be corrected or replaced sooner rather than later, thus enhancing an organization's risk profile. • Initially a NIST term; subsequently adopted commercially • Indicates whether a defined set of planned, required, and deployed security controls within an information system continue to be effective over time in light of the inevitable changes that occur
Dynamic Mapping	A dynamic map depicts discovered devices and their network connectivity and can be updated and/or refreshed to show changes as they occur on the associated network.
File Hash	A process of applying a mathematical algorithm against a set of data to produce a numeric value (a 'hash value') that represents the data
Foundational Intelligence	• Intended to underscore the importance of Asset Manager information as a critical underpinning to a robust security practice • The information gathered and analyzed by Asset Manager
Hybrid Discovery	• Passive, active and targeted system inquires • Discovery processes iteratively fueled by their own output • Subtlety of results and breadth of coverage increase incrementally
Indicator of Compromise	An artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion. Typical IOCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs or domain names of botnet command and control servers. After IOCs have been identified in a process of incident response and computer forensics, they can be used for early detection of future attack attempts using intrusion detection systems and antivirus software.
Infrastructure	Individual networked computers to routers, cables, wireless access points, switches, backbones, network protocols, and network access methodologies.
Integration	Exchanging data between systems to improve information in each Manually or programmatically initiated
IOPS	Input-output operations per second. A measure of the disk performance that Asset Manager requires of a disk or storage array.
Link	The link state of a particular router. What's in the LSDs. The link is NOT the hop bwn routers/nodes. It's a statement about the link between the two hops. Is it healthy and other attributes.
Link Occupancy	A measure of congestion on a communications link is (e.g., how much of the bandwidth is being utilized). Highly occupied/congested links between a Command Center and Scout (or links in which there is an excessive round trip delay) can become a problem. To avoid issues, Asset Manager recommends no more than a 70% link occupancy on a 10Mb/s link, which implies that 7Mb/s (on average) is being consumed by traffic. Asset Manager also recommends a less-than 100 msec round-trip communications delay to ensure satisfactory performance.
Malicious Domain	When a domain is used in malware in place of an IP address to allow for rapid IP address rotation
Malware	Software that compromises the operation of a system by performing an unauthorized function or process.

Mental Model & Conceptual Model	This is a map of your network that can be shifted and molded, expressed in tiers or hierarchical layers of a canvas, and adapted over time to reflect your enterprise's increased understanding of its infrastructure assets under management. The conceptual model, which is a core feature in active development, will enable people to view one network segment from the perspective they find most useful. Each segment may be viewed from however many perspectives have been assembled. You may create your own conceptual models, or work from ones created by other Asset Manager users in your company. • An enterprise's conceptual model of their network • Refers to the display of Asset Manager maps • Maps align with your conceptual understanding of your network and enterprise • Your mental model perspective may be shaped by your clearance level, enclave, mission, or geography, among others.
MIB	A **management information base** (**MIB**) is a virtual database used for managing the entities in a communications network.The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. The top-level MIB OIDs belong to different standards organizations, while lower-level object IDs are allocated by associated organizations. This model permits management across all layers of the OSI reference model.
Non-Accessible SNMP Routers	Those routers that didn't respond to an SNMP test, yet indicated the capability to speak SNMP.
Non-Responding Network	CIDR blocks in the configured list of Target CIDRs, or discovered through router discovery, scanned that did not respond from any sensor. A CIDR block may respond from some locations and may not respond from others. There are several possible reasons these networks were not seen during a network scan. Some reasons include (a) the CIDR blocks may not be in use in the network (b) they may be part of a firewalled network.
Operational Discovery	• Signature quality that distinguishes Asset Manager from Classic IPsonar • Discovery embedded in the fabric of normal business operations
Organization	• In place to support data separation within Asset Manager • Zones are assigned to Organizations • Will support company-driven data separation as well as the managed service version of Asset Manager
OSPF	Open shortest path first protocol. OSPF functions in both broadcast network and non-broadcast, multiple-access networks (NBMA), in which end-to-end points are established. OSPF needs to run on virtual circuits (PVCs) when it runs in a NBMA network. Asset Manager traces to routes discovered in OSPF, unless those routes are in an Avoid list.
OSPF Area	• "Open Shortest Path First" • Most widely used internal routing protocol • Areas are logical groupings of networks • Contains link state information for the domain
Point-in-time-Scan	A Asset Manager IPsonar scan of an enterprise network that is performed in a single sweep. Point-in-time scans are often scheduled to run on a repeat basis and serve to provide a historical record or audit trail for use by oversight agencies.
Real-time Monitoring	Notification of network events-of-interest as they occur • Enables organizations to respond more quickly • Enables a system administrator to watch the current health, risk, processes, and vulnerabilities of a network through graphical charts and bars on a central interface/dashboard. • Visual insights into the data are conveyed. Instant notifications/alerts into specific data-driven, administrator-specified events, such as when a data value goes out of range are provided.
Router ID	One of the IP addresses on the router. From OSPF perspective, it's an identifier.

Router /Routing	The router's primary functions are to learn and propagate route information, and ultimately to forward packets via the most appropriate paths. Successful attacks against routers are those able affect or disrupt one or more of those primary functions by compromising the router itself, its peering sessions, and/or the routing information. Routers are subject to the same sort of attacks designed to compromise hosts and servers, such as password cracking, privilege escalation, buffer overflows, and even social engineering. Most of the best practices in this document help mitigate and even prevent some of those threats. Peering relationships are also target of attacks. For most routing protocols routers cannot exchange route information unless they establish a peering relationship, also called neighbor adjacency. Some attacks attempt to break established sessions by sending the router malformed packets, resetting TCP connections, consuming the router resources, etc. Attacks may also prevent neighbor adjacencies from being formed by saturating queues, memory, CPU and other router resources. This section of the document presents a series of best practices to protect neighbor adjacencies from those threats. Finally, routing can also be compromised by the injection of false route information, and by the modification or removal of legitimate route information. Route information can be injected or altered by many means, ranging from the insertion of individual false route updates to the installation of bogus routers into the routing infrastructure. Potential denial of service conditions may result from intentional loops or black-holes for particular destinations. Attackers may also attempt to redirect traffic along insecure paths to intercept and modify user's data, or simply to circumvent security controls. This section also includes a collection of best practices designed to prevent the compromising of routing information.
Scout	Your business has zones, each of which typically has one Asset Manager Scout • Houses collection agents • Collects information on the state of the network
Security Automation	• Automated set of rules or instructions that performs a task or process that would at one time have been done by a person • Generally includes some form of integration
Security Intelligence	• Real-time collection, normalization, and analysis of the data generated by users, applications, and infrastructure that impacts the IT security and risk posture of an enterprise • The goal of security intelligence is to provide actionable and comprehensive insight that reduces risk and operational effort
SNMP-Accessible	Asset Manager/IPsonar had appropriate credentials that enabled it to access SNMP tables on a network.
SNMP-Reflexive	Asset Manager/IPsonar was able to generate a response from a particular port (thereby demonstrating that the port exists), but unable to illicit a response from the port.
Threat Intelligence / Feed	Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.
Zombie / Bot	A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under the command and control of a remote administrator.
Zone	A ***Zone*** is any set of devices you want to monitor as a unit, for example, a subnet, an enclave, or a business unit. Typically, an organization contains multiple zones. Zones delimit the scope of information that can be displayed on an Asset Manager map. To map a particular network view, all elements belonging to that view must be contained in a single zone. When planning a zone definition, be sure to include elements you want to see on a one map as members of a single zone. Your enterprise sets the criteria that defines which devices should belong to a particular zone.